

Administrator's Handbook

iPlanet Partner Agent for ECXpert Server

*Addendum to the ECXpert 3.5 Administrator's
Handbook*

Version 1.0 for Solaris 2.6 and 2.7

806-4604-01
December 2000

Copyright © 2000 Sun Microsystems, Inc. Some preexisting portions Copyright © 1999 Netscape Communications Corp. All rights reserved.

Sun, Sun Microsystems, the Sun Logo and all other Sun trademarks, service marks, slogans, and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Netscape and the Netscape N logo are registered trademarks of Netscape Communications Corporation in the U.S. and other countries. Other Netscape logos, product names, and service names are also trademarks of Netscape Communications Corporation, which may be registered in other countries. Other product and brand names are trademarks of their respective owners.

Portions of this product are based upon copyrighted materials of Oracle Corporation, Inc. and Netscape Communications Corporation, RSA Data Security, Inc. copyright © 1994, 1995 RSA Data Security, Inc. Portions copyright © 1996 BMC Software, Inc. All rights reserved. Portions copyright © 1996 TSI International, Inc. Portions copyright © 1996-1997 Actuate Software Corporation. All rights reserved.

This file drive contains licensed technology from Receipt.com, formerly known as Differential. More information on Receipt.com products and services can be found at www.receipt.com. The following Third Party Encumbrances have been incorporated into this application: SSLeay SSL toolkit received from Eric Young; Perl5 for the sever administration scripts received from Free Software Foundation; gzip utility for decompression agent for the server received from Free Software Foundation (free and provided upon request); FTP server software received from University of California, Berkeley; wu FTP extensions to server software (FileDrive is a derivative work), received from University of Washington, Saint Louis; Apache Web server for server admin system received from Apache Group; and Apache SSL enhancements received from Ben Laurie.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of the product or this document may be reproduced in any form by any means without prior written authorization of the Sun-Netscape Alliance and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Contents

About this Book	11
Before You Begin	12
Downloading Updated Documentation	12
Suggested Supplementary Reading	13
The ECXpert Documentation Set	13
Release Note	14
Getting Started Guide	14
Administrator's Handbook	14
Developer's Handbook	15
Operations Reference Manual	15
Audience and Roles	15
Organization	15
Conventions Used in This Guide	17
Generic Names	17
Typographic Conventions	17
Part 1 The Partner Agent Server	19
Chapter 1 Introducing the iPlanet Partner Agent for ECXpert Server	21
The Partner Agent for ECXpert Client/Server System	22
Partner Agent Server	22
Partner Agent Client	23
Partner Agent Server Features	23
Partner Agent Server Distribution	24
Partner Agent Server Programs and Scripts	24
ECXpert Wrapper	24
ECXpert ActiveAgents	24
Partner Agent Server Libraries	26

Partner Agent Server Section of the ecx.ini File	27
New MSGFORMATS Messages in Database	31
ECXpert Member Directories	31
Pre-configured Settings for Interaction with ECXpert	32
Default Administrator Username and Password	32
Default Signing Certificate Password	32
Default ActiveAgents	32
Default Security Settings	33
Starting Partner Agent Server	35
Stopping Partner Agent Server	39
Chapter 2 Command Line Utilities	41
gencerts—Generating Self-issued Certificates	42
mkpasswd—Changing the Default Administrator Password	44
mkpasswd	44
addpasswd—Adding an Administrator Password	44
importcert—Importing User Certificates	45
fdx—Command Line FTP Client	45

Part 2 (Optional) Using the Server Administration System **47**

Chapter 3 (Optional) Using the Administration System	49
The Administration System	50
Issuer Certificate	50
Starting the Administration System	51
Accessing the Administration System	51
Navigating the Administration System	51
Changing System Configurations	53
Chapter 4 (Optional) Using the Master Server Controls	55
Server Status	56
Server Shutdown Options	57
Shutting Down the Server Now	57
Scheduling a Shutdown	58
Stopping a Standalone Server	59
Server Control	59
Server Bounce Options	60
Setting Bounce Options	60
Manually Bouncing the Server	61
FTP Server Modes of Operation	61
Changing the FTP Server Mode	61

HTTP Server	62
Server License	62
User Classes	64
User Types	64
Real Users	64
Anonymous Users	64
Virtual Users	65
Default User Classes	65
Adding a New Class Definition	66
Enabling or Disabling a Class Definition	67
Editing a Class Definition	67
Deleting a Class Definition	67
Examples of User Classes	68
Server Messages	69
Server Startup Messages	71
Run-time Messages	71
Cookies	72
Adding a Server Run-Time Message	72
Enabling or Disabling a Run-Time Message Entry	73
Editing a Run-Time Message Entry	73
Deleting a Run-Time Message Entry	73
Command Logging	73
Adding a Command Logging Entry	74
Disabling or Enabling a Command Logging Entry	75
Editing a Command Logging Entry	75
Deleting a Command Logging Entry	75
Transfer Logging	75
Adding a Transfer Logging Entry	76
Enabling or Disabling a Transfer Logging Entry	77
Editing a Transfer Logging Entry	77
Delete a Transfer Logging Entry	77
Passive Mode	77
Specifying a Base Port and Range for Passive Mode	78
Mirror Servers	79
Adding a Mirror Server Entry	80
Enabling or Disabling a Mirror Server Entry	80
Editing a Mirror Server Entry	80
Deleting a Mirror Entry	81
Example Mirror Entry	81
Miscellaneous Options	81
Setting the Administrator Email Address	82
Setting Usage Monitor Options	83
Enabling or Disabling Reverse DNS Lookups	83

Enabling or Disabling Valid User Shell Checks	84
Setting the Session Timeout	84
Version Control	84
Enabling or Disabling Version Control	85
Taking a Snapshot of the Current Version	86
Creating a New Baseline	86
Incremental Version Display	86
Deleting a Version Entry	87
Reverting to a Previous Version	87
Recommended Usage	87
Chapter 5 (Optional) Using the Server Access Controls	89
Admin System Host Access	90
Reordering Rules	91
Adding a New Admin System Access Rule Entry	91
Enabling or Disabling an Admin System Access Rule Entry	91
Editing an Admin System Access Rule Entry	92
Deleting an Admin System Access Rule Entry	92
Example of Admin System Access Rule Entry	92
Partner Agent Server Host Access	93
Reordering Partner Agent Server Host Access Rule Entries	94
Adding a New Partner Agent Server Host Access Rule Entry	94
Enabling or Disabling a Partner Agent Server Host Access Rule	94
Editing a Partner Agent Server Host Access Rule	95
Deleting a Partner Agent Server Host Access Rule	95
Example of Partner Agent Server Host Access Rules	95
Password Files	96
Virtual Users	96
Adding a New Password File Entry	97
Enabling or Disabling a Password File Entry	98
Editing a Password File Entry	98
Deleting a Password File Entry	98
Editing a Password File	99
Adding a New Password File Entry	100
Enabling or Disabling a Password File Entry	100
Editing a Password File Entry	100
Deleting a Password File Entry	100
Editing Permissions for Virtual Users	101
Rules	102
Rule Order and Conflict Policy	102
Virtual Shared Directories	102
Adding a Virtual Permission Entry	102
Enabling or Disabling a Virtual Permission Entry	103

Moving Virtual Permission Entries	103
Editing a Virtual Permission Entry	103
Deleting a Virtual Permission Entry	103
Changing the Conflict Policy	103
Example of Virtual Permission Entries	104
Master Virtual User	105
Virtual Groups	106
Adding a New Virtual Group Entry	106
Disabling or Enabling a Virtual Group Entry	106
Deleting a Virtual Group Entry	106
Limiting User Access	107
Adding a New User Limit Entry	108
Enabling or Disabling a User Limit Entry	109
Editing a User Limit Entry	109
Deleting a User Limit Entry	109
Denying User Access	110
Denying Access to Users	111
Allowing Access to Users	111
Denying Group Access	112
Denying Access to Groups	113
Allowing Access to Groups	113
Anonymous Logins	113
Enabling or Disabling Anonymous Users	114
Setting Criteria for Anonymous Passwords	115
Filesystem Restrictions	115
Adding a New Filesystem Restriction Entry	117
Enabling or Disabling a Filesystem Restriction Entry	117
Editing a Filesystem Restriction Entry	117
Deleting a Filesystem Restriction Entry	117
Upload Restrictions	118
Adding a New Upload Restriction Entry	119
Enabling or Disabling an Upload Restriction Entry	120
Editing an Upload Restriction Entry	120
Deleting an Upload Restriction Entry	120
Download Restrictions	121
Adding a New Download Restriction Entry	121
Enabling or Disabling a Download Restriction Entry	122
Editing a Download Restriction Entry	122
Deleting a Download Restriction Entry	122
Chapter 6 (Optional) Using the Server Security Controls	123
Secure Sockets Layer	124
Enabling or Disabling SSL	126

Modifying the Requirement for Client Certificates	126
Enabling or Disabling Client Certificate Verification	126
Adding a New SSL Users Encryption Entry	127
Enabling or Disabling an Encryption Entry	127
Editing an Encryption Entry	127
Deleting an Encryption Entry	127
User Authentication	128
Setting User Authentication Options	129
A Few Things to Know about User Authentication	129
Login Failures	130
Changing the Failed Login Threshold	130
FTP Commands	131
Setting FTP Command Options	132
Editing an FTP Command Entry	132
Deleting an FTP Command Entry	132
Entrust Configuration	133
Security Audit	133
EnGuard Features	133
Running EnGuard as a Cron Job	134
Security Audit Control Panel	134
Browsing Previously Generated Security Audit Reports	135
Configuring Archival and Distribution of Reports	136
Archival and Distribution of Security Reports Options	137
Customizing Reports	138
Enabling or Disabling Security Checks	139
Enabling or Disabling Report Settings	140
Configuring Security Checking Of Anonymous FTP Hierarchy	141
Excluding a Directory	142
Removing a Directory from the Excluded List	143
Excluding a File	143
Removing a File from the Excluded List	143
Performing a Security Audit	143
Chapter 7 (Optional) Using the Server Statistics Controls	145
Server Usage Monitor	146
Server Usage Snapshot by User Class	147
Server Usage Snapshot by Connection	147
Server Usage Statistics Control Panel	147
Server Usage Statistics Viewer	148
Server Usage Statistics Configuration Manager	148
Server Usage Statistics Generator	150

Chapter 8 (Optional) Using the Server ActiveAgents	153
Introducing ActiveAgents	154
ActiveAgent Server	155
Environment Variables	155
Notes on Agent Supplied Cookies	158
Bundled ActiveAgents	158
Agent Access	159
Reordering the Rules	160
Adding a New Agent Server Host Access Rule Entry	160
Enabling or Disabling an Agent Server Host Access Rule Entry	161
Editing an Agent Server Host Access Rule	161
Deleting an Agent Server Host Access Rule	161
Agent Server Port	162
ActiveAgents	162
Chaining ActiveAgents	164
Adding a New ActiveAgent Entry	164
Enabling or Disabling an ActiveAgent entry	166
Editing an ActiveAgent entry	166
Deleting an ActiveAgent entry	166
ActiveAgent Descriptions	166
Certificate Agent (cert)	166
User Configuration Agent (config)	167
Password Authentication Agent (auth)	168
Login and Logout Agents	169
Login Agent	169
Logout Agent	169
Incoming and Outgoing Agents	169
Incoming Agents	170
Outgoing Agents	170
FTP and HTTP Command Agents	171

Part 3 Appendices **173**

Appendix A (Optional) Installing a Stand-alone FileDrive Server	175
FileDrive Server	176
Hardware Requirements for a Stand-alone Instance of FileDrive Server	176
Server Distribution	177
Obtaining a License File	178
Installing a Stand-alone FileDrive Server	178
Installing a License File After Installation	187
Uninstalling a Stand-alone Instance of FileDrive Server	187
FileDrive Server FAQs	188

Appendix B (Optional) Using the Partner Agent Server Command Line Client	191
The Partner Agent Server Command Line Client	192
Installing the Command Line Client from CD	192
Starting Partner Agent Server Command Line Client Interactively	193
Starting the Command Interpreter	193
Establishing a Connection Automatically	193
Changing Transfer Protocol Schemes	196
Operating in Tunnel Mode	196
Environment Variables	196
Aborting a File Transfer	197
Transferring Files	197
Uploading or Downloading Files Using Shell Scripts	197
Uploading Files from the Command Line	198
Uploading Files Interactively	199
Uploading Files to ECXpert from the Command Line	200
Uploading Files to ECXpert Interactively	201
Downloading Files from the Command Line	203
Downloading Files Interactively	204
Downloading Files to ECXpert from the Command Line	205
Downloading Files to ECXpert Interactively	207
Deleting Files Interactively	208
Listing Files Interactively	209
Command Line Options	210
FTP Command Line Options	210
HTTP(S) Command Line Options	211
Interactive Commands	212
File Naming Conventions	212
File Transfer Parameters	213
FTP Interactive Commands	213
HTTP or HTTPS Interactive Commands	219
Tracking File Transfers in ECXpert	222
For more information on using the ECXpert Tracking feature, see the <i>ECXpert Site Administrator's Handbook</i> .	
Browser Client	223
Navigate	224
Download or Delete File	225
Upload a File	226
Index	227

About this Book

This handbook documents the conceptual, structural, and operational components of the iPlanet Partner Agent for ECXpert Server. It also provides a description of the functionality and guidelines for administering the system.

The following topics are discussed in this section:

- Before You Begin
- The ECXpert Documentation Set
- Audience and Roles
- Organization
- Conventions Used in This Guide

Before You Begin

This Handbook is written with the assumption that you understand the basics of TCP/IP communications and operating system on which you are running this software.

It is not necessary to be an expert concerning the technical intricacies of HTML or the World Wide Web, but it is helpful to understand the basic concepts of both.

Downloading Updated Documentation

We continuously update ECXpert documentation. Follow these steps to:

- Determine whether you have the latest version of any ECXpert document
- Download a copy of any ECXpert document
- 1. Obtain a user ID and password for ProductTracker by SubscribNet.

If you do not know where to start, display the ProductTracker by SubscribNet home page at the URL below:

<http://home.netscape.com/support/producttracker/index.html>

The information provided on this page should let you determine the contact person at your company who can provide you with the user ID and password. If that person is you, and you have not received this information, call the Netscape Customer Support phone number that is provided.

- 2. Display the ProductTracker by SubscribNet web page.

The URL is...

<http://subscribnet.netscape.com/>

- 3. Enter your Subscribnet user ID and password.

The main Subscribnet page is displayed.

- 4. Click the link in “Click here to access your software.”

An index of the Netscape and iPlanet software registered for your user ID is displayed.

- 5. Click the “iPlanet ECXpert” link.

A page is displayed that asks you to select the version and platform.

6. Locate the link for your version, platform, and domestic vs. export combination.

First locate Version Beta, and then find Solaris, for Export or Domestic (US/CAN) sale, as appropriate.

7. Click the link you have located.

A list of all the downloads available for ECXpert, including documentation, is displayed.

8. Locate the title in the ECXpert document set that you want.

9. Compare dates.

Compare the date for that title with the date in the footers in your copy of the same document.

If these dates are the same, you already have the latest version of the documentation.

10. If your documentation is outdated, click the download link.

If the date in the footers of the documentation you have is earlier than the date for the same document on the screen, you should download the updated version.

Suggested Supplementary Reading

The following documents may be helpful as supplements to this handbook:

- The *iPlanet Partner Agent for ECXpert Windows Client User's Guide*, for information about installing and using the Partner Agent Windows Client
- For ECXpert technical support, always visit the iPlanet Online Support website at <http://www.iplanet.com/support/online>
- Your operating system manuals, particularly any pertaining to system security

The ECXpert Documentation Set

You may wish to refer to other ECXpert books for additional information. This section discusses each book in the ECXpert documentation set.

Release Note

After you receive the ECXpert software, before you do anything else, you should download the *ECXpert Release Note*. See “Downloading Updated Documentation,” on page 12 for instructions on downloading the latest release note.

The Release Note contains:

- A 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 *Release Note* is platform-specific, so make sure you have the right version for the platform you’re using.

Getting Started Guide

The *ECXpert Getting Started Guide* is the book you use to install ECXpert. It includes preinstallation tasks—including basic instructions for installing or upgrading to the required version of Oracle—ECXpert installation steps, and information on additional tasks you may wish to perform after you install ECXpert. The *Getting Started Guide* is platform-specific, so make sure you have the right version for the platform you’re using.

Administrator’s Handbook

The *ECXpert Administrator’s Handbook* is written for the ECXpert System’s site administrator. This book provides an overview of the ECXpert system and 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. It also covers the ECXpert Server Administrative Interface in depth, discusses the ECXpert command line utilities, and explains how to integrate ECXpert with SAP and MQSeries.

Developer's Handbook

The *ECXpert Developer Handbook* book is written for C++ developers who want to customize ECXpert. It primarily documents the ECXpert APIs which 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.

Operations Reference Manual

If you ever have difficulty using ECXpert, the *ECXpert Operations Reference Manual* more than likely documents a quick resolution. This book contains basic troubleshooting guidelines for ECXpert, other Netscape products, and third-party products. It also includes a complete error message reference.

Audience and Roles

This handbook is written for the Partner Agent Server's site administrator. All documentation needed by Partner Agent Windows Client users is supplied in the *Partner Agent for ECXpert Windows Client User's Guide*.

Organization

This handbook is structured as follows:

Part 1: The Partner Agent Server

Chapter 1: Introducing the iPlanet Partner Agent for ECXpert Server

This chapter introduces the iPlanet Partner Agent for ECXpert family of applications and describes the major features and concepts of the Partner Agent Server.

Chapter 2: Command Line Utilities

This chapter describes Partner Agent Server's command line utilities.

Part 2: (Optional) Using the Server Administration System

Chapter 3: (Optional) Using the Administration System

This chapter describes the administration system that is used to configure and maintain Partner Agent Server.

Chapter 4: (Optional) Using the Master Server Controls

This chapter explains how to turn the Partner Agent Server on and off, control the display of messages to users, revert the Server configuration to a previous version, and control access to users by their account type.

Chapter 5: (Optional) Using the Server Access Controls

This chapter explains how to control access to the Partner Agent Server and the Partner Agent Server administration system.

Chapter 6: (Optional) Using the Server Security Controls

This chapter describes how to configure security settings for Partner Agent Server, enable or disable FTP commands, and perform audits.

Chapter 7: (Optional) Using the Server Statistics Controls

This chapter explains how to view server traffic, configure which statistics are logged, generate statistics, and view previously generated statistics.

Chapter 8: (Optional) Using the Server Active Agents

This chapter explains how to set up server side programs that are triggered by user activity on the Server.

Part 3: Appendices

Appendix A: (Optional) Installing a Stand-alone File Drive Server

This chapter describes how to install the stand-alone File Drive Server, which optionally can be used to exchange files with the Partner Agent Server, and consequently with ECXpert, through a firewall.

Appendix B: (Optional) Using the Partner Agent Server Command Line Client

This appendix explains how to install the Partner Agent Server Command Line Client, how to start the client, and the commands and options available.

Index

The index lists important terms and page numbers where information about those terms appears in the text.

Conventions Used in This Guide

The Partner Agent Server administration system is a series of HTML pages that are referred to as pages, for example the Active Agents page. Within each page are sections, where the various controls for setting up and configuring Partner Agent Server are located.

This guide is meant to be used as a reference, so there is some repetition of similar tasks. For example editing and deleting list entries is identical in many pages, but is described in each page's description.

The following conventions are used in this guide.

Generic Names

The Partner Agent Server and the Partner Agent Client are sometimes referred to as Partner Agent. The Partner Agent Server administration system is sometimes referred to as the admin system.

The base directory that houses all of the components of Partner Agent Server is, by default, `$NSBASE/NS-apps/paserver`, where the environment variable `$NSBASE` is the full path to the ECXpert installation directory. This location will be different if you install Partner Agent Server on a different machine than ECXpert.

Typographic Conventions

A number of typographic conventions are used throughout this manual to help you recognize special terms and instructions. These conventions are summarized in the table below.

Convention	Meaning	Example
numbered steps	higher level descriptions of tasks you perform (more detailed instructions follow)	<p>1. Enter the group information.</p> <p>Enter the name in the Group Name field, and a short description in the Description field.</p>

Convention	Meaning	Example
<i>italics</i>	key words, such as terms that are defined in the text names of books variables In command syntax, items in italics are <i>not</i> literals.	The notices posted on an electronic BBS are called <i>articles</i> . For more information, refer to the <i>ECXpert Getting Started Guide</i> . usrlogin=login You must substitute valid values for italicized items.
courier font	file names text file content (HTML templates, config files) code samples and command line output	The associated data is stored in the Dispatcher section of the <code>bdg.ini</code> file. <TITLE>Password Check</TITLE> Syntax <code>const char* getName() const</code>
courier bold	command line input, to be entered by the user	Enter the following command: ls *.mle
# or <code>fdx></code>	command line prompt	fdx>sslmode tun
square brackets, [...]	In command syntax, items within square brackets are <i>optional</i> .	In the following example: <code>nsusrgrp [-v] insert [-l] -k <i>key arguments</i> -r act=<i>relation action</i>, usrid=<i>ID</i> usrlogin=<i>login</i></code>
vertical line ()	In command syntax, items on either side are valid <i>alternatives</i> .	<ul style="list-style-type: none"> • <code>-v</code> and <code>-l</code> are optional. • You may specify either <i>usrid</i> or <i>usrlogin</i>. • You must substitute valid values for italicized items.
em dash (—)	“none” or “nothing”	Arguments —

The Partner Agent Server

Chapter 1, “Introducing the iPlanet Partner Agent for ECXpert Server”

Chapter 2, “Command Line Utilities”

Introducing the iPlanet Partner Agent for ECXpert Server

This chapter describes the iPlanet Partner Agent for ECXpert client/server system and the features of the Partner Agent Server in particular.

The following topics are discussed in this section:

- The Partner Agent for ECXpert Client/Server System
- Partner Agent Server Features
- Partner Agent Server Distribution
- Pre-configured Settings for Interaction with ECXpert
- Starting Partner Agent Server
- Stopping Partner Agent Server

The Partner Agent for ECXpert Client/Server System

Partner Agent for ECXpert is a client/server solution for secure file transfer and automated document processing. Partner Agent products work with the ECXpert system to provide high performance file transfer capabilities as well as state of the art security, reliability, and automation. Partner Agent is fully compatible with FTP and HTTP(S) standards.

Partner Agent is made up of the Partner Agent Server and the Partner Agent Client. Partner Agent Server is integrated with ECXpert, turning ECXpert into a secure file transfer site. Partner Agent Client runs as a stand-alone application that turns your PC into a powerful, secure, and reliable download and upload manager for exchanging files with ECXpert, as well as with other machines.

Partner Agent Server allows Client users to exchange files directly with ECXpert. Partner Agent Server uses the ECXpert submit utility to upload files from the Client to ECXpert, where they are processed further as required. It uses the ECXpert poll utility to retrieve files downloaded from ECXpert; these files can be viewed and processed using the Client.

Partner Agent is scalable, making it an ideal building block for industrial-strength extranet applications.

Partner Agent Server

Partner Agent for ECXpert Server is a customized, pre-configured system that allows you to turn ECXpert into a secure file transfer site.

In addition to integrating state-of-the-art security standards, such as Secure Socket Layer (SSL) and digital certificates (X.509), Partner Agent Server contains a sophisticated access control system as well as EnGuard™ security auditing software that automatically warns of potential security issues.

Partner Agent Server also guarantees Extranet data delivery and data integrity while protecting corporate bandwidth.

Partner Agent Server's functionality is extended through a plug-in architecture that uses *ActiveAgents*. ActiveAgents are transactional software agents that call ECXpert APIs to initiate events based on file transfers and to also feed information into back-end applications, such as databases, enterprise scheduling software, and network printing operations. ActiveAgents also make it easy to add third-party functionality to Partner Agent Server, such as virus scanning, file format conversion, or additional security mechanisms as required.

Partner Agent Server comes with a browser-based administration system, which can optionally be used to reconfigure the Server in special circumstances; it is not needed in most cases since the Server is already preconfigured for optimal, secure performance with ECXpert. It also comes with a secure command line client, which can optionally be used for testing the system.

Partner Agent Client

Partner Agent Client software for Windows 98/95 and NT provides high-performance, reliable, and secure file transfer of critical business documents between your Windows desktop and ECXpert or other machines—over your intranet, business extranet, or the Internet.

You can also use a standard browser as a client for file transfers to non-ECXpert machines.

Partner Agent Server Features

- Pre-configured settings for interaction with ECXpert
- Full compatibility with the FTP standard (RFC 959).
- Secure Sockets Layer (SSL) encryption.
- Logging of all server activity.
- Graphical and tabular server activity analysis.
- Extended FTP commands support mirror servers.
- Optional web-based server administration GUI.
- Real-time server activity monitor.
- Server access restrictions.
- ActiveAgents architecture for dynamic server applications.
- Virtual user capabilities for secure virtual accounts.
- EnGuard™ security auditing system with heuristic break-in analysis.

Partner Agent Server Distribution

The Partner Agent Server distribution is installed under the `$NSBASE/NS-apps/paserver` directory.

Partner Agent Server Programs and Scripts

The following programs are provided in the `$NSBASE/NS-apps/ECXpert/bin` directory.

ECXpert Wrapper

ecxpa-m-server. This is an ECXpert administrative wrapper around the Partner Agent servers. The Partner Agent Server has an entry (*ecxpa-server*) in the ECXpert `ecx.ini` file just like any other ECXpert server, which means it can be stopped and started via the ECXpert administrative user interface just like any other ECXpert server. When this server is started, it in turn starts all the Partner Agent servers. When the ECXPA server is stopped, it in turn stops the Partner Agent servers. This feature means that a uniform administrative interface is provided for all ECXpert servers.

ECXpert ActiveAgents

The following scripts and programs, invoked via Partner Agent Server file transfers, provide interaction between Partner Agent Server and ECXpert.

ecxpa-welcome. This is a shell script invoked when a user attempts to login to the Partner Agent Server. A welcome message is relayed to the client program and displayed to the user.

ecxpa-bye. This is a shell script invoked when a user logs out of the Partner Agent Server. A message is relayed to the client program and displayed to the user.

ecxpa-fd-certify. This is a shell script invoked when a user presents a certificate to the Partner Agent Server, which has been configured to expect one, for authentication.

ecxpa. This is a shell script wrapper around an ECXpert ActiveAgent. The wrapper establishes an environment that will allow the subsequent program invocation to execute in a well-defined manner. The program to be invoked, together with any arguments it may take, is passed to the shell script wrapper on the command line. The remaining programs listed below are all invoked by the `ecxpa` script. Each of these wrapped programs follows the standard ECXpert

convention of taking the location of the ECXpert `ecx.ini` file and the server section name as command-line arguments. This mechanism provides an extensible and consistent way to pass parameters into these programs. The `ecx.ini` file section name is `[excpa-server]`. For example, for this release the value of `debug_flag` is examined by each of these programs and an ECXpert debug log is produced (under the `$NSBASE/NS-apps/ECXpert/data/logs` directory, as usual) if it is enabled.

excpa-config. This program returns information about the ECX member that is essential for correct subsequent file transfer. It includes the ECXpert member's home directory location as well as the UNIX userid and groupid by which to execute the ActiveAgent programs.

excpa-login. This program authenticates the ECXpert member name and password supplied against the ECXpert member database/directory.

excpa-submit. This program is invoked at the completion of a file upload from the Partner Agent client. It uses ECXpert APIs to submit the uploaded file to ECXpert. From the client user's perspective, this is an atomic one-step process. A file upload from the remote client is essentially a direct submission to a remote ECXpert system.

excpa-retrieve. This program is invoked at the beginning of a file download from the Partner Agent client. It uses ECXpert APIs to retrieve the specified file from ECXpert. From the client user's perspective, this is an atomic one-step process. A file download request from the remote client is essentially a direct poll of a file from the remote ECXpert system. It uses the poll interface and is therefore subject to the same limitations that poll has.

excpa-cleanup. This program is triggered at the end of a file download. Depending on the outcome of the file download, it will report back to the ECXpert tracking log whether or not the file download was successful. It also removes any temporary files created during the file download.

Partner Agent Server Libraries

To support these executables, the following shared libraries are supplied in the *\$NSBASE/NS-apps/ECXpert/lib* directory:

- `libecxpacleanup10.so`
- `libecxpaconfig10.so`
- `libecxpalogin10.so`
- `libecxpaplugin10.so`
- `libecxpapretrieve10.so`
- `libecxpaserver10.so`
- `libecxpasubmit10.so`
- `libecxpauti110.so`

Partner Agent Server Section of the ecx.ini File

The Partner Agent Server installation script automatically adds a new section, *[expa-server]*, to the ECXpert *ecx.ini* file in the *\$NSBASE/NS-apps/ECXpert/config/* directory. Table 1 outlines the parameters in this section.

Table 1-1 [expa-server] section of the ecx.ini file

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. <i>Default:</i> 19; do not change.
snmp_trap_flag	Trap information for SNMP service? <i>Restrictions</i> —valid values: yes, no <i>Default:</i> yes
snmp_trap_level	SNMP event level to trap. <i>Restrictions</i> —valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only <i>Default:</i> 10
section_type	Type of section. <i>Default:</i> server; do not change.
protocol_id	Protocol identifier. <i>Default:</i> 775
port_location	Location to pick up the port. <i>Default:</i> mmap
listener_level	Listener level. Number of listener threads to launch on startup. <i>Default:</i> 1; do not change.
listener_type	Listener type. <i>Restrictions</i> —valid values: - dynamic = Administrative Server assigns - manual = always use value in listener_port <i>Default:</i> thread

Table 1-1 [ecxpa-server] section of the ecx.ini file (*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. <i>Restrictions:</i> Total number of threads you specify must be supported by your hardware. <i>Default:</i> 4
runnable_flag	Can executable be run? <i>Restrictions</i> —valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation) <i>Default:</i> yes
thread_mode	Thread operational mode <i>Restrictions</i> —valid values: - threaded = run threaded - serialized = run serialized <i>Default:</i> 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. <i>Default:</i> 10
admin_time_out	Admin server time out period, in seconds. <i>Default:</i> 10
start_mode	Server start mode. <i>Restrictions</i> —valid values: commandline, background <i>Default:</i> background
type	Type of executable. <i>Restrictions</i> —valid values: none, daemon, process <i>Default:</i> daemon
Machine independent information	
host_name	IP address of host machine where instances of executable are run. <i>Restrictions:</i> Must be a valid IP address in your domain. <i>Default:</i> set during installation
File and directory information	
exec_path	Executable path. Full path to the executable. <i>Default:</i> %NSBASE%\NS-apps\ECXpert\bin\ecxpa-m-server

Table 1-1 [ecxpa-server] section of the ecx.ini file (*Continued*)

Entry	Description
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system? <i>Restrictions</i> —valid values: yes, no <i>Default</i> : yes; do not change.
worker_max_threads	Number of worker threads to run in parallel. <i>Default</i> : 4; do not change.
master_max_threads	Number of master threads to run in parallel. <i>Default</i> : 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads? <i>Restrictions</i> —valid values: yes, no <i>Default</i> : yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue. <i>Default</i> : 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack. <i>Default</i> : 500; do not change.
Port information	
listener_port	Listener port number. <i>Restrictions</i> : Ports used by ECXpert must not be used by other applications. <i>Default</i> : set during installation
admin_port_type	Administrative port type. <i>Restrictions</i> —valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port <i>Default</i> : dynamic
listener_port_type	Listener port type. Only set when adding your own network_id. <i>Restrictions</i> —valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port <i>Default</i> : dynamic
admin_port	Administrative port number. <i>Restrictions</i> : Ports used by ECXpert must not be used by other applications. <i>Default</i> : set during installation

Table 1-1 [ecxpa-server] section of the ecx.ini file (*Continued*)

Entry	Description
Start and stop scripts	
pa_server_start_admin	Program that starts the HTTPS admin server, which provides a browser-based user interface to configure the installation, from the command line. Spawned when the server is started. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/start_admin
pa_server_start_agentd	Program that starts the agent server, which runs the ActiveAgent programs that perform the back-end ECXpert interactions, from the command line. Spawned when the server is started. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/start_agentd
pa_server_start_httpd	Program that starts the HTTP server from the command line. Spawned when the server is started. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/start_httpd
pa_server_start_ftpd	Program that starts the ftp server from the command line. Spawned when the server is started. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/start_ftpd
pa_server_stop_admin	Program that stops the HTTPS admin server, which provides a browser-based user interface to configure the installation, from the command line. Spawned when the server is shut down. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/stop_admin
pa_server_stop_agentd	Program that stops the agent server, which runs the ActiveAgent programs that perform the back-end ECXpert interactions, from the command line. Spawned when the server is shut down. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/stop_agentd
pa_server_stop_httpd	Program that stops the HTTP server from the command line. Spawned when the server is shut down. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/stop_httpd
pa_server_stop_ftpd	Program that stops the ftp server from the command line. Spawned when the server is shut down. <i>Default:</i> \$NSBASE/NS-apps/paserver/bin/stop_ftpd
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started? <i>Restrictions</i> —valid values: yes, no <i>Default:</i> no

Table 1-1 [ecxpa-server] section of the ecx.ini file (*Continued*)

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit? <i>Restrictions</i> —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 may be required) <i>Default:</i> no
Debug output configuration	
stderr_path	Fully specified path for log file to receive standard output from low level trace. <i>Default:</i> \$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. <i>Default:</i> \$NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.ecxpa-server.dat
debug_flag	Turn on low level tracing information? <i>Restrictions</i> —valid values: yes, no <i>Default:</i> no

New MSGFORMATS Messages in Database

The Partner Agent Server installation process updates the MSGFORMATS table in the database to include seven new messages.

ECXpert Member Directories

The Partner Agent Server installation process creates new home directories for each existing ECXpert member under the \$NSBASE/NS-apps/ECXpert/data/pas directory.

Pre-configured Settings for Interaction with ECXpert

Partner Agent Server is installed with default configuration settings that ensure optimal, secure performance with ECXpert. These defaults enable fast ramping and deployment. Use of the browser-based Administration System to modify the settings is, in most cases, neither required nor recommended.

Some of the default configuration settings are outlined in this section.

Default Administrator Username and Password

The default username and password for accessing the optional browser-based Administration System are *ECX* and *ECX*.

For more information about the browser-based Administration System, see Part 2, “(Optional) Using the Server Administration System,” on page 47.

Default Signing Certificate Password

The default password for signing certificates, for which you are prompted whenever you run the *gencerts* utility, is *ECXpert*.

For more information about the *gencerts* utility, see “*gencerts*—Generating Self-issued Certificates,” on page 42.

Default ActiveAgents

ActiveAgents are programs, triggered by user activity on the Partner Agent Server, that interact with the ECXpert server. They handle ECXpert member authentication programs as well as file submission and retrieval.

Figure 1-1 shows the default ActiveAgents.

Figure 1-1 Default ActiveAgents

The screenshot shows the iPlanet Partner Agent Server interface. The left sidebar contains navigation links: [Agent Server Host Access](#), [Agent Server Port](#), [ActiveAgents](#), and [Help](#). The main content area is titled "ActiveAgents" and features a section for "Add New ActiveAgent Entry". This section includes a form with the following fields:

- Agent Type: Certificate Verification
- User: *
- Execution: User/Group
- Exec As User: -
- Exec As Group: -
- Target: (empty text box)
- Agent: (empty text box)
- Arguments: (empty text box)
- Server Address: (empty text box)
- Server Port: (empty text box)
- Action: Add Agent

Below the form is a table titled "Current ActiveAgents Entries":

Agent Type	User	Exec As	Target	Agent	S
Certificate Verification	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa-fd-certify	lo
Password Authentication	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa	lo
User Configuration	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa	lo
Login	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa-welcome	lo
Logout	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa-bye	lo
Incoming End	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa	lo
Outgoing End	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa	lo
Outgoing Error	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa	lo
Outgoing Start	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/eczpa	lo

Default Security Settings

By default, Partner Agent Server has been pre-configured for maximum security. Data passing over the connection between the Partner Agent Client and the Partner Agent Server is encrypted via Secure Socket Layer (SSL). Client users also must present a valid certificate to the server for authentication.

After a user's certificate has been authenticated, Partner Agent Server extracts the username from the Distinguished Name (DN) string and prompts for a password. This username/password combination must correspond to a valid ECXpert member. As pre-configured, the Server authenticates users only via the ActiveAgent for ECXpert authentication, `ecxpas-login`, which calls ECXpert APIs to perform this authentication against the ECXpert member directory/database.

Figure 1-2 shows the default SSL settings. The default user authentication settings are shown in Figure 1-3.

Figure 1-2 Default Secure Socket Layer Settings

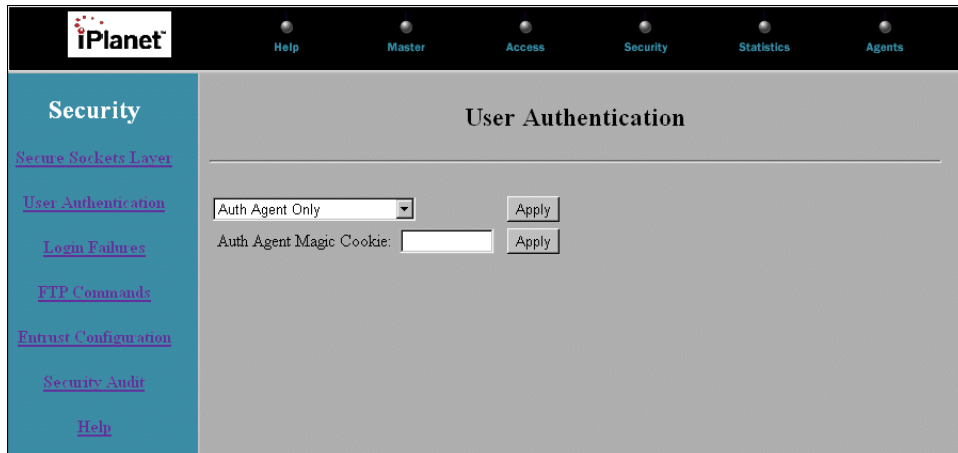
The screenshot displays the iPlanet Partner Agent Security configuration interface. The main content area is titled "Secure Sockets Layer" and contains the following sections:

- SSL Options:** Three configuration rows, each with a dropdown menu and an "Apply" button.
 - Secure Sockets Layer Enabled (dropdown)
 - Client Certificate Mandatory (dropdown)
 - Client Certificate Verification Enabled (dropdown)
- Add New SSL Users Encryption Entry:** A table with columns for User Class, Encryption, and Action.

User Class	Encryption	Action
*	Optional	Add Entry
- Current SSL Users Encryption Entries:** A table showing the current configuration.

User Class	Encryption	Status	Action
*	Optional	Enabled	Disable Edit Delete

Figure 1-3 Default User Authentication Settings



Starting Partner Agent Server

To start the Partner Agent Server:

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 1-4) is displayed.

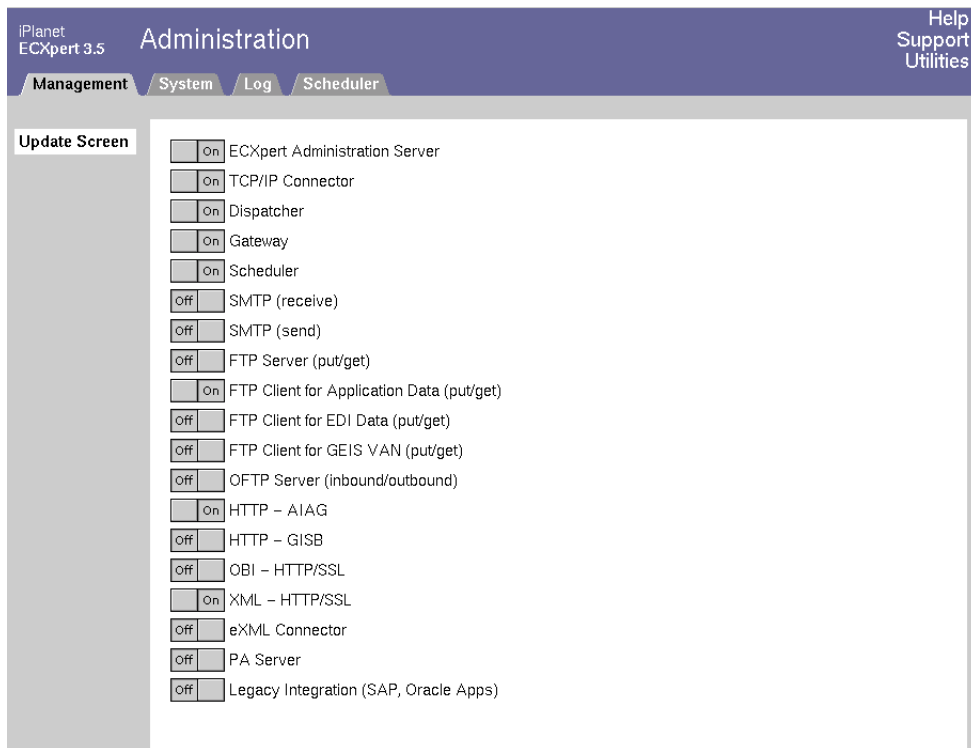
Figure 1-4 ECXpert home page



- **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. Click the Admin link. The initial screen for the Server Administrative Interface is displayed. If the ECXpert Administrative Server is running, the Management tab appears as shown in Figure 1-5.

Figure 1-5 Initial Server Administrative Interface screen (ECXpert Administration Server is On)



3. Toggle the PA Server switch to the On position.

4. Click the Update Screen button after ten seconds has passed.

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

When the Partner Agent Server is started, the following servers are started:

admin. This is the Partner Agent administrative HTTPS server that provides a browser-based user interface to configure the Partner Agent Server installation. The ECXpert user is provided with a pre-configured package that minimizes use of this administrative interface (see “(Optional) Using the Administration System,” on page 49). The Partner Agent Server system can be configured and administered from a remote browser where the communication between the browser and the admin server is over secure HTTP.

This server can also be started manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/start_admin`.

agentd. This is the Partner Agent server that runs the ActiveAgent programs that perform the back-end ECXpert interactions. Partner Agent Server offers a decoupled architecture that separates the incoming communications-handling processing from the business logic processing. The agentd daemon executes the business logic. This architecture offers valuable security benefits such as the ability to partition the servers in a demilitarized (DMZ) firewall configuration.

This server can also be started manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/start_agentd`.

ftpd. This is the Partner Agent FTP server. It can be configured to accept either plain incoming FTP sessions or SSL-encrypted FTP sessions.

This server can also be started manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/start_ftpd`.

httpd. This is the Partner Agent HTTP server. It can be configured to accept either plain HTTP sessions or secure HTTP sessions.

This server can also be started manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/start_httpd`.

Stopping Partner Agent Server

To shut down the Partner Agent Server:

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 is displayed, as shown in Figure 1-4.

2. Click the Admin link. The initial screen for the Server Administrative Interface is displayed. If the ECXpert Administrative Server is running, the Management tab appears as shown in Figure 1-5.
3. Toggle the PA Server switch to the Off position.
4. Click the Update Screen button after ten seconds has passed.

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

When the Partner Agent Server is stopped, the following servers are shut down:

admin. This is the Partner Agent administrative HTTPS server that provides a browser-based user interface to configure the Partner Agent Server installation.

This server can also be shut down manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/stop_admin`.

agentd. This is the Partner Agent server that runs the ActiveAgent programs that perform the back-end ECXpert interactions.

This server can also be shut down manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/stop_agentd`.

ftpd. This server can also be shut down manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/stop_ftpd`.

This is the Partner Agent FTP server.

httpd. This is the Partner Agent HTTP server.

This server can also be shut down manually from the command line by running the script `$NSBASE/NS-apps/paserver/bin/stop_httpd`.

Stopping Partner Agent Server

Command Line Utilities

This chapter describe each of the Partner Agent Server command line utilities, which are located in the `$NSBASE/NS-apps/paserver/bin` directory.

The following topics are discussed in this section:

- `gencerts`—Generating Self-issued Certificates
- `mkpasswd`—Changing the Default Administrator Password
- `addpasswd`—Adding an Administrator Password
- `importcert`—Importing User Certificates
- `fdx`—Command Line FTP Client

gencerts—Generating Self-issued Certificates

The gencerts utility generates self-issued, base-64 encoded certificates in PEM format for each of the Partner Agent servers, which include agentd, admin, ftpd, and httpsd. The utility adds the certificates to the Partner Agent Server database and uses them to authenticate incoming certificate-based login attempts made by the user.

Syntax

The syntax of the submit command is as follows:

```
gencerts <parameter_list>
```

where <parameter_list> consists of options selected from Table 2-1.

Table 2-1 Parameters for the gencerts utility

Parameter	Usage
-s	To generate certificates for the Agent, FTP, and HTTP(S) Servers.
-u <User ID>	To generate a certificate for the specified ECXpert user.
-a	To generate a certificate for the Agent Server.
-f	To generate a certificate for the FTP Server.
-w	To generate a certificate for the HTTP(S) Server.
-h	To display usage help.

NOTE You will be prompted to specify two pass phrases. The first is associated with the private key, and is used to decrypt the certificate; enter a password of your choice. The second is the administrator's password to sign the certificate; this has been pre-configured to default to "ECXpert."

Example

```
gencerts -u PartnerA
```

Figure 2-1 Example output of the gencerts utility script

```

$ ../../paserver/bin/gencerts -u johndoe
==> Generating certificate request for johndoe
==> Encrypt private key? [y]
==> Enter key password when prompted for PEM pass phrase
Using configuration from
/export/disk2/usr/actraadm/NS-apps/paserver/conf/ssl.client.conf
Generating a 1024 bit RSA private key
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
Country Name          (2 letter code)  []:US
State/Province Name  (full name)     []:CA
Locality Name        (eg, city)      []:MV
Organization Name    (eg, company)   []:Company
Organizational Unit  (eg, section)   []:APD
Common Name          (eg, first last) []:John Doe
Email Address        (eg, name@fqdn) []:john_doe@company.com
==> Signing certificate for johndoe
==> Enter signing password when prompted for PEM pass phrase
Using configuration from
/export/disk2/usr/actraadm/NS-apps/paserver/conf/ssl.ca.conf
Enter PEM pass phrase:
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName          :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'CA'
localityName         :PRINTABLE:'MV'
organizationName     :PRINTABLE:'Company'
organizationalUnitName:PRINTABLE:'APD'
commonName           :PRINTABLE:'John Doe'
emailAddress          :IA5STRING:'john_doe@company.com'
Certificate is to be certified until Oct  7 23:46:57 2000 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
$

```

mkpasswd—Changing the Default Administrator Password

mkpasswd

By default, the administrator username and password, which are used to log into the browser-based Administration System, are *ECX/ECX*. The username and encrypted password are stored in a data file,

`$NSBASE/NS-apps/paserver/var/db/http/admin_users.db`.

The `mkpasswd` utility allows you to change the default password, overwriting the user data in the `$NSBASE/NS-apps/paserver/var/db/http/admin_users.db` file.

Syntax

The syntax of the `mkpasswd` command is as follows:

```
mkpasswd
```

When prompted, enter the administrator account name and the password.

addpasswd—Adding an Administrator Password

Use the `addpasswd` utility to add another administrator user account, or to change the password of an existing administrator user. The utility adds the new data to the `$NSBASE/NS-apps/paserver/var/db/http/admin_users.db` file.

Syntax

The syntax of the `submit` command is as follows:

```
addpasswd
```

When prompted, enter the administrator account name and password

importcert—Importing User Certificates

The `importcert` utility imports a user's public certificate file to the Partner Agent Server and creates a one-to-one mapping between the certificate's subdirect and the ECXpert member.

Syntax

The syntax of the submit command is as follows:

```
importcert <parameter_list>
```

where *<parameter_list>* consists of options selected from Table 2-2.

Table 2-2 Parameters for the gencerts utility

Parameter	Usage
<code>-u <ECXpert Member ID></code>	Specifies the ECXpert user for whom the certificate is imported.
<code>-f <Certificate File></code>	Specifies the path and filename of the certificate to be imported.

Example

```
importcert -u PartnerA -f
$NSBASE/NS-apps/paserver/lib/certs/private/agentd-crt.pem
```

fdx—Command Line FTP Client

`fdx` is a command-line driven, SSL-enabled FTP client. It is detailed in the appendix on “(Optional) Using the Partner Agent Server Command Line Client.”

(Optional) Using the Server Administration System

Chapter 3, “(Optional) Using the Administration System”

Chapter 4, “(Optional) Using the Master Server Controls”

Chapter 5, “(Optional) Using the Server Access Controls”

Chapter 6, “(Optional) Using the Server Security Controls”

Chapter 7, “(Optional) Using the Server Statistics Controls”

Chapter 8, “(Optional) Using the Server ActiveAgents”

NOTE As installed, Partner Agent Server is pre-configured with defaults that ensure optimal, secure performance with ECXpert. These defaults enable fast ramping and deployment and should satisfy the majority of users' needs. Minimal use of the separate administration system described in this part of the manual is required.

(Optional) Using the Administration System

This chapter describes the browser-based administration system that is used to configure and maintain Partner Agent Server. It describes how to access the administration system, how to set your browser to recognize the signing certificate, how to navigate the administration system, and how to make changes in the system.

The following topics are discussed in this section:

- The Administration System
- Navigating the Administration System
- Changing System Configurations

NOTE As installed, Partner Agent Server is pre-configured with defaults that ensure optimal, secure performance with ECXpert. These defaults enable fast ramping and deployment and should satisfy the majority of users' needs. Minimal use of the separate administration system described in this part of the manual is required.

The Administration System

The Partner Agent Server administration system is a series of HTML pages that are referred to as pages, for example the Active Agents page. Within each page are sections, where the various controls for setting up and configuring Partner Agent Server are located.

This guide is meant to be used as a reference, so it includes some repetition of similar tasks. For example, editing and deleting list entries is identical in many pages but is described in each page's description.

Your Partner Agent Server server is administered and configured through its web-based administration system. The administration system runs over a secure HTTPS connection. This allows system administrators to manage the server from any remote console that has a standard browser that supports SSL, such as Netscape Navigator or Microsoft Internet Explorer. If you do not have a web browser available, you can download the latest version for your operating system from Netscape or Microsoft.

Issuer Certificate

As part of the installation process, you are asked for information that is used to create a CA signing certificate for all certificates that are subsequently created during the installation. This certificate is not recognized by either Netscape Navigator or Microsoft Internet Explorer. To address this issue, we have provided a web application that updates your browser with your CA signing certificate. To add your certificate to your browser's database:

1. Open your browser.
2. In the location or address window type:

```
http://[hostname]:[port]/addcert.cgi
```

The host name and port are entered during the installation process (see *Chapter 2: Installation*) for the non-secure admin.

3. Follow the instructions provided by your browser.

NOTE You need to do this only once.

NOTE The default certificate signing password is *ECXpert*.

Starting the Administration System

The administration system runs as an HTTPS process listening on port 444 by default. You are given the option of changing this port at system installation time. When you start the Partner Agent Server from the ECXpert Admin screen, the Administration System is automatically started (see “Starting Partner Agent Server,” on page 35).

To start the administration system from the command line:

- Run the `$NSBASE/NS-apps/paserver/bin/start_admin` program.

Accessing the Administration System

To access the administration system:

1. Open your browser.
2. In the location or address window, type:

```
https://[hostname]:[port]/admin
```

where the host name and port are those specified during the installation process (see the *iPlanet Release Note for ECXpert Version 3.5 for Solaris*).

3. Enter the administrator’s User Name and Password.

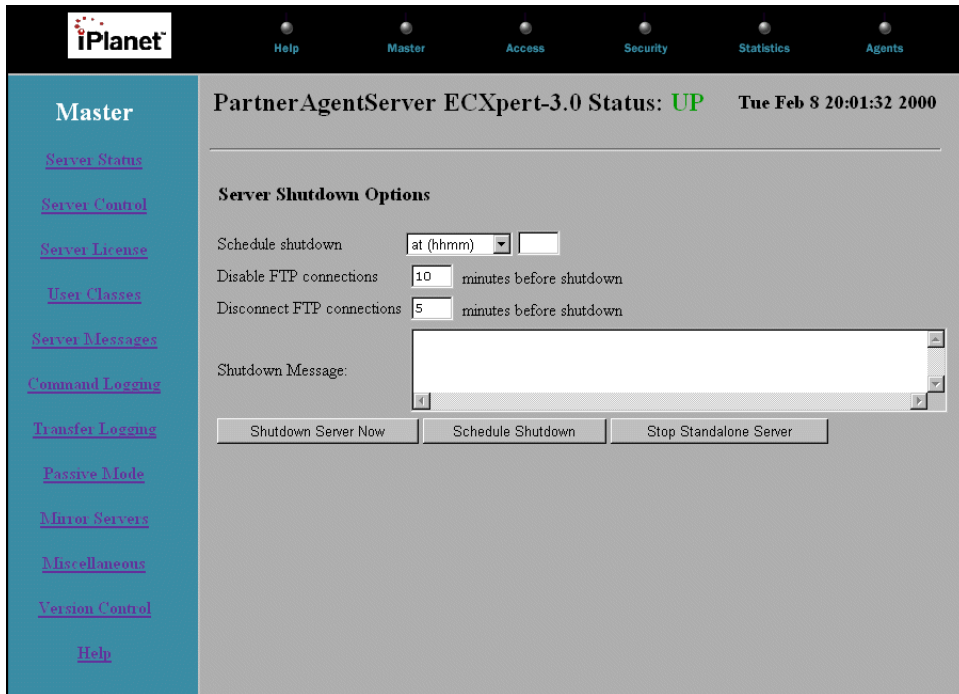
By default, these are *ECX/ECX*.

Navigating the Administration System

The administration system screen is divided into three parts, or frames. At the top of the screen are the buttons for accessing the six main sections of the system:

- Help
- Master
- Access
- Security
- Statistics
- Agents

Figure 3-1 Partner Agent Server Administration System, initial screen



To access a section, click on the appropriate button in the top menu bar of the administration system.

NOTE Clicking on the iPlanet logo takes you to the iPlanet web site, (www.iplanet.com).

Each section consists of multiple pages that contain the controls for the administration system. When you select a section, the left vertical frame displays links for that section's pages. For example, clicking on Master displays the links to the Master pages in the left vertical frame. At the bottom of each list is a link to the online Help file.

The large central frame displays the controls for the currently selected administration page.

When you select a section from the top frame, the first page in the list in the left frame, becomes the currently selected page. Its controls are displayed in the central frame. So, for example, when you select the Master section, the central frame displays the controls for the Server Status page.

Changing System Configurations

The central frame displays the pages for altering the system configurations. The current values for the settings are displayed in the frame.

In general, to change these values:

1. Make the desired change(s) to the relevant field(s).
2. To submit your changes, click the appropriately labeled button.

The form makes the desired changes to the server configuration.

NOTE Your changes do not take effect if you do not click the button to submit the form. If you change fields in the form and then decide that you do not want to submit your changes, do not click the button.

Instructions to change specific system configurations are contained in the following chapters.

(Optional) Using the Master Server Controls

This chapter describes how to use the Master Server Control section of the administration system to turn the Partner Agent Server on and off, control the display of messages to users, revert the Server configuration to a previous version, and control access to users by their account type.

This chapter covers the pages for viewing and changing the Master Server Controls. These pages, which are displayed by clicking the corresponding header in the left frame of the Master screen, include:

- Server Status
- Server Control
- Server License
- User Classes
- Server Messages
- Command Logging
- Transfer Logging
- Passive Mode
- Mirror Servers
- Miscellaneous Options
- Version Control

NOTE For information about ECXpert system settings specific to the Partner Agent Server, which are added to the ECXpert *ecx.ini* file during the Partner Agent Server installation, see the *iPlanet Release Note for ECXpert Version 3.0 SP1 for Solaris* or the *ECXpert Site Administrator's Handbook*.

Server Status

At the top of the Server Status page, the software version, Server status, date, and time are displayed.

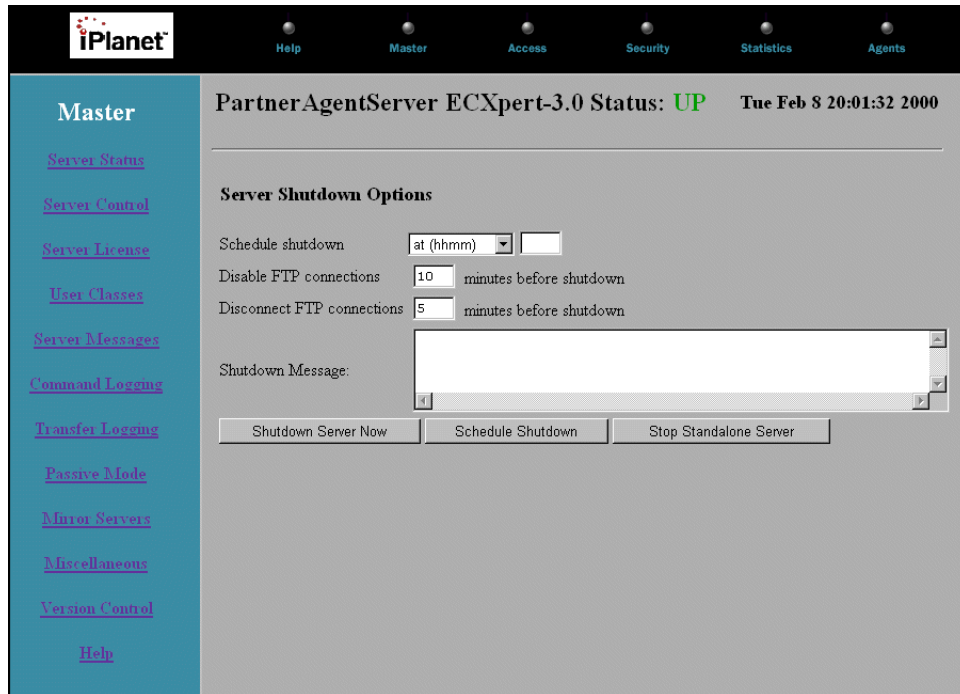
If a Server shutdown is pending the time that the Server is scheduled to shut down is displayed next to the words Shutdown Pending in blue.

If the Server is not running, the word Down is displayed in red.

- To start the Server, click Start the Server

If the Server is running, the word UP is displayed in green. Below that are controls for shutting down the Server.

Figure 4-1 Master pages, Server Status screen



Server Shutdown Options

The Server shut down options are to shut down the Server now, schedule a shut down, or stop the standalone Server.

Shutting Down the Server Now

You have the option of performing an instant shut down of the Server at any time. When you shut down the Server in this manner, it automatically disconnects all users to the Server and disables any FTP connections. This option does not display a warning to connected users. The administration Server and the ActiveAgents Server continue to run.

- To shut down the Server immediately, click Shutdown Server Now.

Scheduling a Shutdown

The Schedule shutdown option allows you to determine at what time the Server will shut down and how much time you want to give connections and users before disabling or disconnecting.

To schedule a Server shutdown for some time in the future:

1. Choose an absolute time or a number of minutes from the current time. To do this, in the schedule drop-down list select:
 - At (hhmm).
 - In (minutes).OR
 - In (hours).
2. In the field next to the drop-down list, either enter the number of minutes or hours from the current time that the Server will stop, or enter the absolute time at which you want the Server to stop.

NOTE For an absolute time, enter the time in the HHMM format, (a two-digit hour followed by two-digit minutes, based on a 24-hour clock), with no spaces or separators. If you specify a shutdown time that is before the current time, Partner Agent Server assumes that you mean to shut the Server down tomorrow. For example, if it is currently 1400 and you specify a HHMM shutdown time of 1330, the Server is scheduled to shutdown in 23 hours and 30 minutes (1:30 P.M. tomorrow).

3. In the Disable FTP connections field, enter the number of minutes prior to shut down that you want the Server to stop allowing new connections.
4. In the Disconnect FTP connections field, enter the number of minutes prior to shut down that you want the Server to stop and disconnect the current users.
5. In the Shutdown Message field, enter a short text message concerning the shutdown, which will be displayed for users currently connected to the Server.
6. Click Schedule Shutdown.

The page displays the status of shutdown pending and the time that the Server will shut down. To return to the main Server Status page, click Reschedule Shutdown.

Figure 4-2 Master pages, Server Status screen with Shutdown Pending



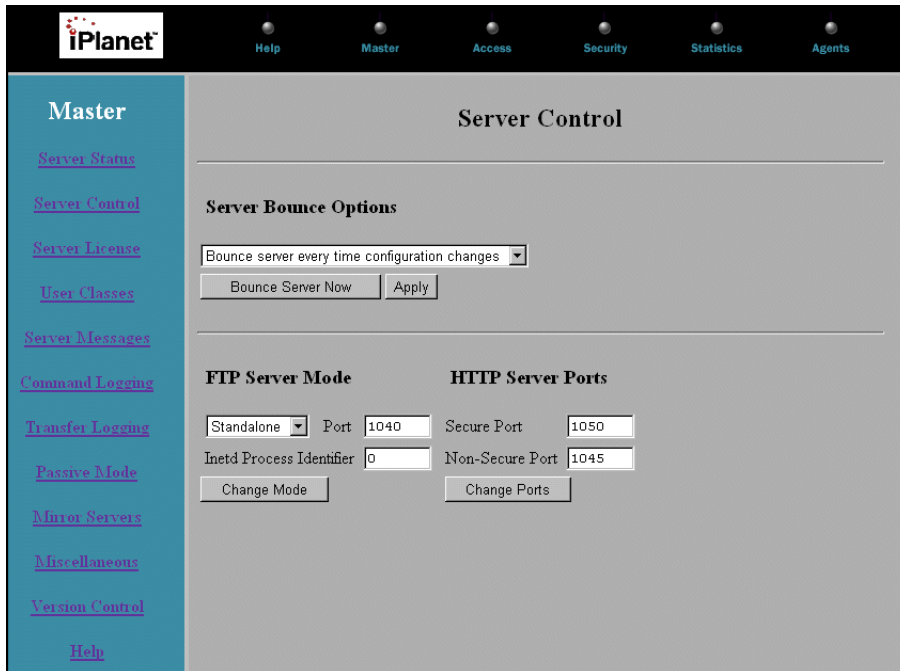
Stopping a Standalone Server

If the Server is running in standalone mode, you can shut it down.

- To shut down the Server, click Stop Standalone Server.
- To restart the Server, click Start the Server.

Server Control

The Server Control page allows you to set the bounce options and select the mode of operation for the FTP Server.

Figure 4-3 Master pages, Server Control screen

Server Bounce Options

Bouncing the Partner Agent Server is required for the standalone mode of operation. This tells Partner Agent Server to re-read all of its configuration files. Since the standalone master Server reads its configuration files only at startup, any changes made through the administration system will not take effect immediately. The Server bounce feature works as a refresh for the Server when changes are made to the configuration files. A bounce does not affect any existing connections, but only new connections following the bounce.

The Server can be set to bounce whenever the configuration files are changed, or it can be bounced manually.

Setting Bounce Options

To set the bounce options:

1. Select whether to “Bounce server only when requested” or to “Bounce server every time configuration changes.” Choose from the Server Bounce Options drop-down list.
2. Click Apply.

Manually Bouncing the Server

To manually bounce the Server, click Bounce Server Now.

FTP Server Modes of Operation

There are two modes of FTP Server operation, inetd and standalone. In inetd mode, a Partner Agent Server is started each time a request comes in for an FTP connection. All config files are read each time the Server starts.

In standalone mode, there is a master Partner Agent Server running, with the sole purpose of handling incoming FTP requests. The Server is started once, reads all its config files and then waits for connections. This is a higher performance mode of operation, since all the disk I/O required to read the Partner Agent Server configuration files is done only once at master startup. Each connection request then gets its own Server started preconfigured, speeding up startup time.

Changing the FTP Server Mode

To change the FTP Server mode:

1. Select the desired mode, inetd or standalone. Choose from the Server Mode drop-down list.

In standalone mode:

- m Enter a port that the Server listens to for connections, in the Port field.

In inetd mode:

- m Enter the process number that starts the Server, in the Inetd Process Identifier field.

2. Click Change Mode.

Your changes are applied. In inetd mode, the Port field displays *ftp*, to indicate that Partner Agent Server is listening to the port specified in the FTP entry in `/etc/services`.

HTTP Server

The HTTP Server runs in standalone mode only. Each time a change is made to the configuration files, you need to bounce the Server. The port that the HTTP Server listens on can be changed for secure and non-secure modes.

- m To change the port that the HTTPS Server listens to for connections, enter a number in the Secure Port field.
- m To change the port that the HTTP Server listens to for connections, enter a number in the Non-Secure Port field.
- m Click Change Ports to apply any changes.
- m If necessary, bounce the Server, (“Server Bounce Options,” on page 60).

Server License

The Server License page shows you information about your current Partner Agent Server license. The license is non-expiring and should not need to be updated.

If, for some reason, you need to update your Partner Agent Server license:

1. Contact iPlanet Technical Support to get a text file that contains a Server license.

To contact ECXpert Technical Support in the United States, call Expert Alliance at:

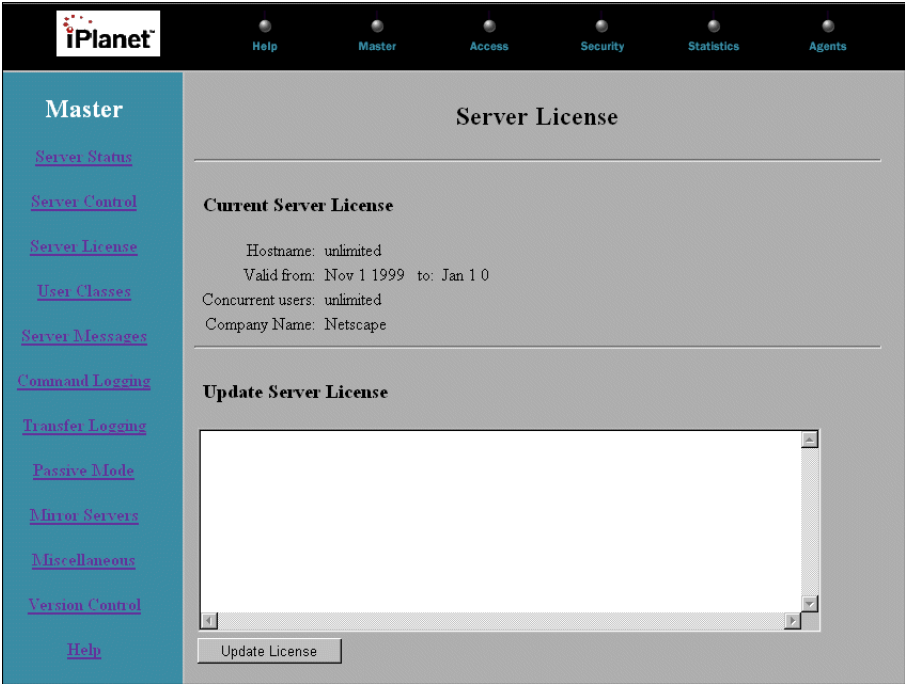
800-560-5749

To contact ECXpert Technical Support outside of the United States, call Technical Support International at:

650-937-6688

2. Copy the contents of the text file.
3. Paste the contents into the Update Server License window.
4. Click Update License.

Figure 4-4 Master pages, Server License screen



User Classes

User Classes are the fundamental unit of access control in Partner Agent Server. A user class consists of a combination of user type, user name, user group, and address. The user type is either real, anonymous, or virtual (see User Types below). The user name is the user's UNIX login name. The user group is the user's UNIX group, and the address is the IP address or hostname to which this user class applies.

User classes are a way of classifying Partner Agent Server users. Create user classes to apply access rules, for example, to force certain user classes to have SSL-enabled Clients.

User Types

There are three types of users in Partner Agent Server: real, anonymous, and virtual. User types are pre-defined in Partner Agent Server. By default, all ECXpert members are configured as virtual users.

Real Users

Real users have access to the entire file system on the machine hosting the Partner Agent Server. Real users typically have a shell account permitting them to log into the machine using telnet or rlogin, in addition to FTP access. Real users are listed in the operating system password file (`/etc/passwd`).

Anonymous Users

Anonymous users are those logging in through a shared FTP account. One anonymous user per Server is allowed, with the user defined as `ftp` in `/etc/passwd`. When a user logs in on the FTP account, the virtual root of the file system, `/`, is actually the home directory of the FTP account. This means that the user cannot access files or directories outside of the FTP account.

NOTE For Solaris, in order for directory listings to work correctly you must configure the `dev` and `etc` directories with certain files. To perform this configuration, run the `$NSBASE/NS-apps/paserver/bin/ftpsetup` script.

Anonymous user access is useful for publishing public content that does not require user authentication to access it. You can disable anonymous logins, even if the FTP user account is present (“Anonymous Logins,” on page 113).

Virtual Users

Virtual users are a special type of users, unique to Partner Agent Server. A virtual user has the authentication requirements of a real user with the limited file system access of an anonymous user. A virtual user is limited to browsing only those portions of the file system that are rooted in their home directory. The only exception to this is when a virtual user has access to virtual shared directories. Virtual users exist only in the context of Partner Agent Server and are unknown to the UNIX system. This prevents virtual users from logging in to the Server machine with telnet or rlogin, even if they have a valid shell, since they are not in the set of system users.

All ECXpert members are configured to be virtual users; new members are added to this user class automatically.

Default User Classes

By default, Partner Agent Server defines three classes of users that correspond to the three types of users:

- *real*—users of type *real* connecting from any host address (*).
- *anon*—users of type *anonymous* connecting from any host address (*).
- *virt*—users of type *virtual* connecting from any host address (*).

The User Classes page is where you create new class definitions or disable or remove any of the default class definitions.

Figure 4-5 Master pages, User Classes screen

The screenshot shows the iPlanet User Classes management interface. On the left is a navigation menu with links: Master, Server Status, Server Control, Server License, User Classes, Server Messages, Command Logging, Transfer Logging, Passive Mode, Mirror Servers, Miscellaneous, Version Control, and Help. The main content area is titled 'User Classes' and features a form to 'Add New User Class Entry' and a table of 'Current User Class Entries'.

Add New User Class Entry

Class Name	User Type	User Name	User Group	From Address	Action
<input type="text"/>	<input type="text" value="real"/> <input type="text" value="anonymous"/> <input type="text" value="virtual"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text"/>	<input type="button" value="Add Class"/>

Current User Class Entries

Class Name	User Type	User Name	User Group	From Address	Status	Action		
local	*	*	*	127/8	Enabled	Disable	Edit	Delete
real	real	*	*	*	Enabled	Disable	Edit	Delete
anon	anonymous	*	*	*	Enabled	Disable	Edit	Delete
virt	virtual	*	*	*	Enabled	Disable	Edit	Delete

NOTE If a user falls into multiple classes, Partner Agent Server categorizes them as belonging to the first matching class in the list of Current User Class Entries.

Adding a New Class Definition

To add a new class definition:

1. Define a class name, using any unique word.
2. Select the pre-defined user type from the User Type drop-down list.
3. Select the user name (UNIX login name), from the User Name drop-down list.
4. Select the user group (UNIX group name), from the User Group drop-down list.

5. Enter a host name address or IP address in the From Address field. You can use UNIX-style wildcards, such as *, to define classes by subnet.
6. To add your class definition, click Add Class.
The definition is added to the list of Current User Class Entries with a status of Disabled.

Enabling or Disabling a Class Definition

To enable or disable a class definition, click Enable or Disable next to the desired class definition.

Editing a Class Definition

To edit a class definition from the list of Current User Class Entries:

1. In the Action column next to the desired class definition, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit User Class section above the list of Current User Class Entries.
3. Click Apply.

Your changes are reflected in the list of Current User Class Entries.

Deleting a Class Definition

To delete a class definition, in the Action column next to the desired class definition, click Delete.

NOTE Deleting a class definition does not delete any rules that reference that class.

Examples of User Classes

Figure 4-6 Example of user class entries

Class Name	User Type	User Name	User Group	From Address	Status	Action		
local	*	*	*	127/8	Enabled	Disable	Edit	Delete
real	real	*	*	*	Enabled	Disable	Edit	Delete
anon	anonymous	*	*	*	Enabled	Disable	Edit	Delete
virt	virtual	*	*	*	Enabled	Disable	Edit	Delete

Table 4-1 User ClassDefinition

local	Defines a user class named <i>local</i> in which users of any type, name, or group, from the localhost (<i>127.8</i>) address would become members.
real	Defines a user class named <i>real</i> in which all users of type <i>real</i> , from any name, group, or address would become a member.
anon	Defines a user class named <i>anon</i> in which all users of type <i>anonymous</i> , from any name, group, or address would become a member.
virt	Defines a user class named <i>virtual</i> in which all users of type <i>virtual</i> , from any name, group, or address would become a member..

NOTE Any user is classified in the first class in the list to which they apply.

Wildcards are supported in all fields, but they are most useful for specifying the from address. Addresses of the following form are all valid:

```
tnt.acme.com
*.acme.com
192.168.1.*
192.168.1/8
127.0.*
127.0/16
```

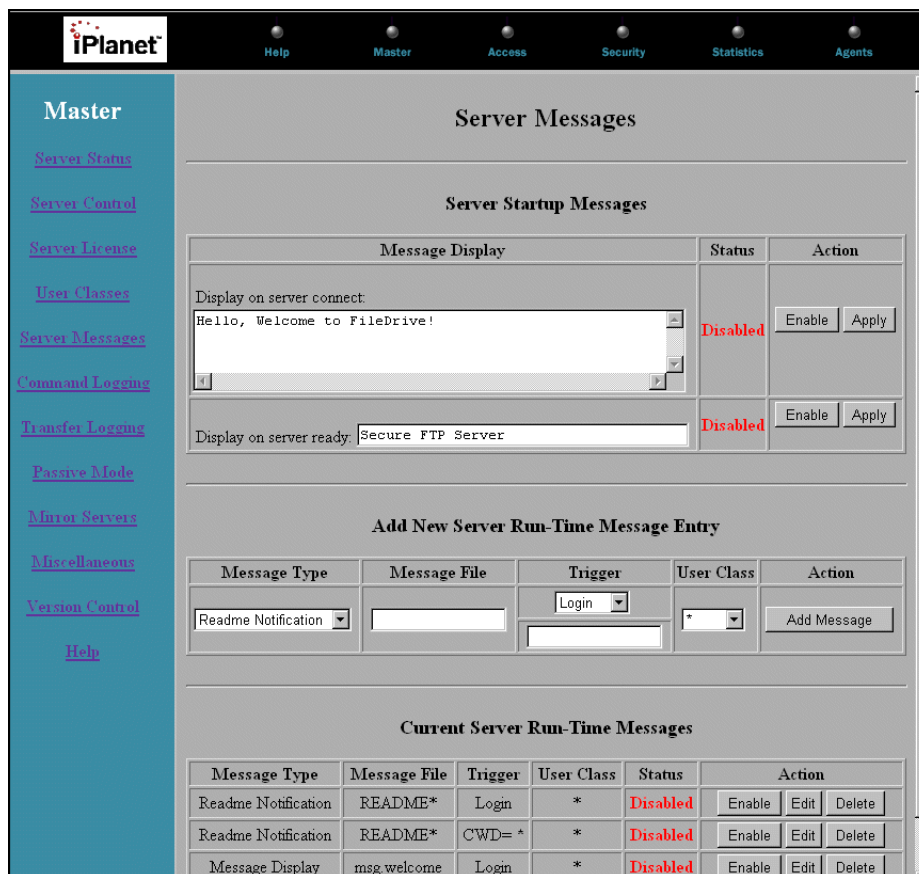
Server Messages

Server Messages are messages that display to users at various points in an FTP connection. Server messages do not display for HTTP Clients.

NOTE Users may or may not see these messages, depending on the software they are using to connect to your Partner Agent Server. Most FTP Client software will display these messages. Users browsing your FTP site with a Web browser will see these messages. Users downloading a single file by URL from a Web browser may not see these messages.

The Server Messages page allows you to enable and disable the sending of message files to users.

Figure 4-7 Master pages, Server Messages screen



Two types of Server messages are available: startup and run-time.

Server Startup Messages

Startup messages display during the initial connection to the Server, prior to any login prompt being displayed. One message displays to the user when the connection has been established; another displays when the Partner Agent Server is ready to accept a login. The default is to display the hostname of the Server and the Server version, but this default can be overridden.

To create or edit the Server connect message:

1. Enter the message you want displayed in the Display on server connect field.
2. Click Apply.
3. Make sure it is enabled (if not, click Enable).

To create or edit the Display on server ready message:

1. Enter the message you want displayed in the Display on server ready field.
2. Click Apply.
3. Make sure it is enabled (if not, click Enable).

NOTE If no message is enabled, the default message, (the hostname of the Server and the Server version), displays.

Run-time Messages

Run-time messages are displayed to the user during the course of an FTP session. There are two types of run-time messages, README notifications and message displays. A README notification informs the user of the presence of a message file and asks them to read it. A message display message displays the contents of a message file.

- When a user changes into a directory, Partner Agent Server scans the directory for filenames that start with “README.” If any such files exist, the Server notifies the users that they should look at those files. This is useful for users who may be browsing software or document archives. You can specify that the user is notified of the presence of a README file on login as well as when changing a directory into a directory that contains a README file.
- Message Display files, located in the file system, can be displayed to the user when they change directories.

Cookies

Partner Agent Server allows you to have magic cookies in message and README files. The cookies are replaced by Server-generated strings when the files are sent to users. The specifications of these cookies are similar to those supported by several University FTP Servers:

Cookie	What the Server replaces it with.
%T	Local time in the form: Thu Dec 19 14:15:18 1996
%F	Free space in partition of CWD (kbytes)
%C	Current working directory
%E	The Server administrator's email address
%R	Remote host name
%L	Local host name
%u	User name as determined via RFC931 authentication
%U	User name given at login time
%M	Maximum allowed number of users

Adding a Server Run-Time Message

To add a Server run-time message:

1. Select a message type from the Message Type drop-down list—either Readme Notification or Message Display.
2. In the Message File field, enter the message's file name.
3. Select a trigger type from the Trigger drop-down list. Two events trigger run-time messages—a user login (login) or the first time a user changes directories (cwd=).
4. For triggers of type cwd=, enter the directory name in the field below.
5. Select a user class from the User Class drop-down list.
6. Click Add Messages.

The message is added to the list of Current Server Run-Time Messages, with a status of Disabled.

Enabling or Disabling a Run-Time Message Entry

To enable or disable a run-time message entry, click Enable or Disable next to the desired entry.

Editing a Run-Time Message Entry

To edit an entry from the list of Current Server Run-Time Message Entries:

1. In the Action column next to the desired class definition, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Server Run-Time Message Entry section above the list of Current Run-Time Message Entries.
3. Click Apply.

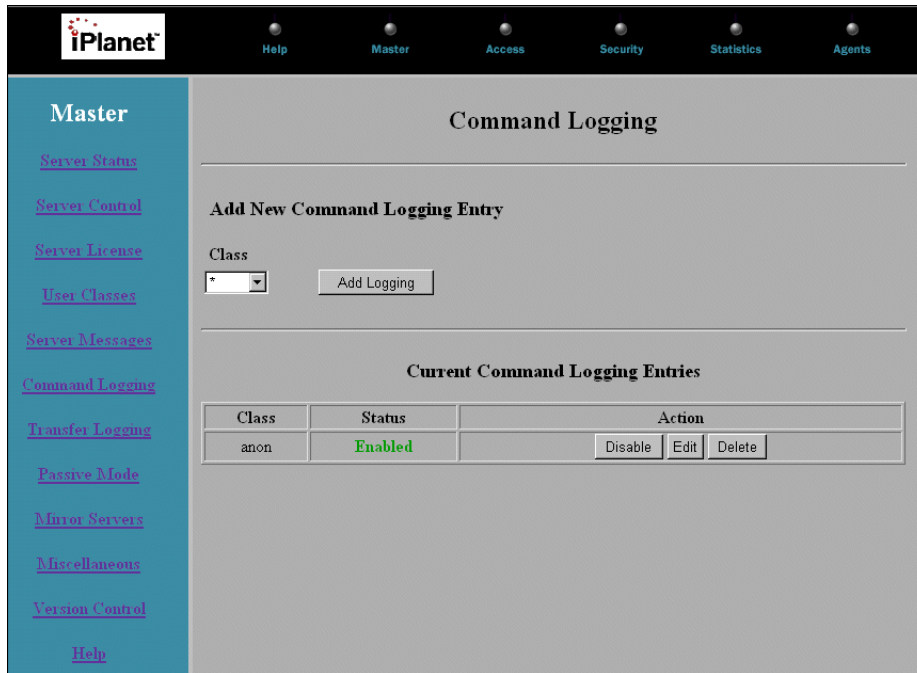
Your changes are reflected in the list of Server Run-Time Message Entries.

Deleting a Run-Time Message Entry

To delete a message entry, in the Action column next to the desired message entry, click Delete.

Command Logging

Partner Agent Server's Command Logging feature works as a tracking system. When users are on the system, typing commands, the Command Logging feature records their commands in a log. Command logging is available only for the FTP Server.

Figure 4-8 Master pages, Command Logging screen

The Command Logging page is where you view and determine which user classes will have their commands logged. You can restrict this feature by user class so that only certain user classes are logged.

Adding a Command Logging Entry

To add a new command logging entry:

1. Select a user class from the Class drop-down list.
2. Click Add Logging.

Your entry is added to the list of Current Command Logging Entries, with a status of Enabled.

Disabling or Enabling a Command Logging Entry

To disable or enable a logging entry, click **Disable** or **Enable** next to the desired entry.

Editing a Command Logging Entry

To edit an entry from the list of **Current Command Logging Entries**:

1. In the **Action** column next to the desired command logging entry, click **Edit**.
2. Make the desired changes in the fields and drop-down lists in the **Edit Command Logging Entry** section, above the list of **Current Command Logging Entries**.
3. Click **Apply**.

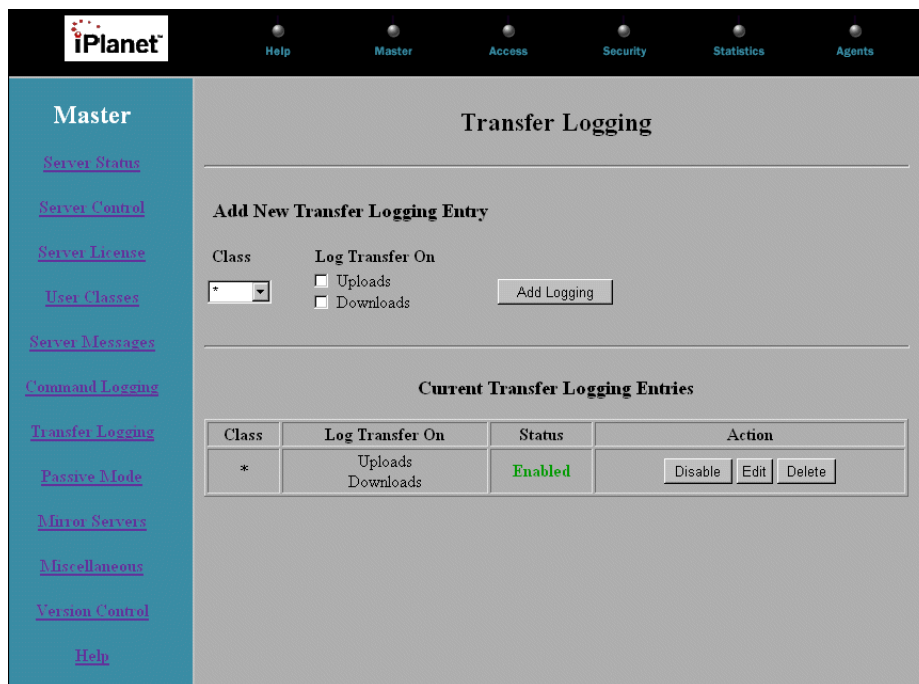
Your changes are reflected in the list of **Current Command Logging Entries**.

Deleting a Command Logging Entry

To delete a logging entry, in the **Action** column next to the desired entry, click **Delete**.

Transfer Logging

Transfer Logging tracks what uploads and downloads have occurred on the system. The tracking information is kept in a log file on the system. This feature may also be enabled by user class.

Figure 4-9 Master pages, Transfer Logging screen

The Transfer Logging page is where you add and edit logging entries to determine which transfers get logged.

Adding a Transfer Logging Entry

To add a new Transfer logging entry:

1. Select a user class from the Class drop-down list.
2. Check in the desired Log Transfer On checkboxes to determine whether to log uploads, downloads, or both.
3. Click Add Logging.

Your entry is added to the list of Current Transfer Logging Entries, with a status of Disabled.

Enabling or Disabling a Transfer Logging Entry

To enable or disable a transfer logging entry, click Enable or Disable next to the desired entry.

Editing a Transfer Logging Entry

To edit an entry from the list of Current Transfer Logging Entries:

1. In the Action column next to the desired command logging entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Transfer Logging Entry section, above the list of Current Transfer Logging Entries.
3. Click Apply.

Your changes are reflected in the list of Transfer Logging Entries.

Delete a Transfer Logging Entry

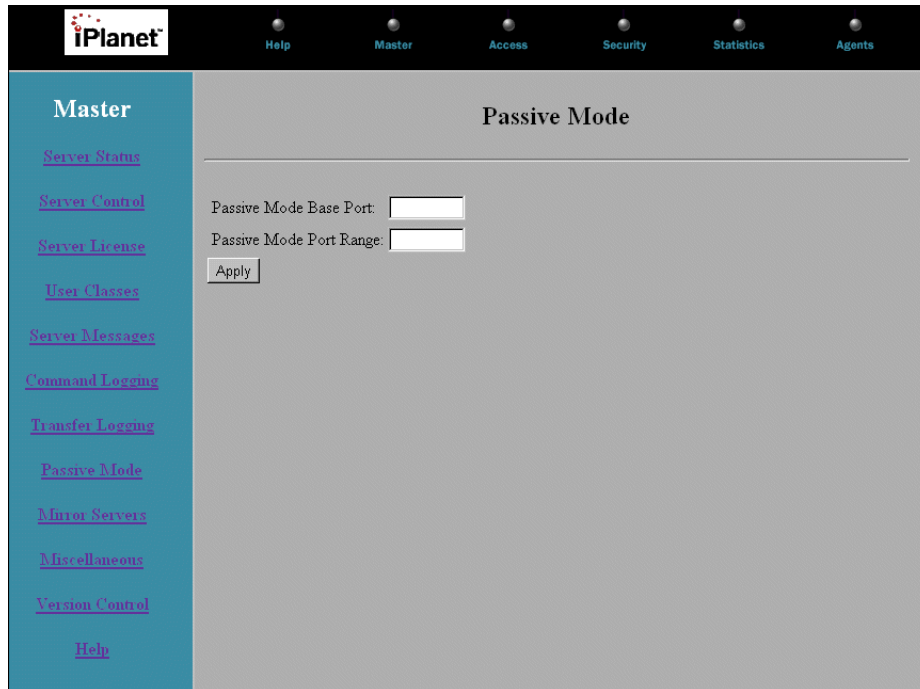
To delete a logging entry, in the Action column next to the desired message entry, click Delete.

Passive Mode

Passive mode requests the FTP Server to listen on a data port, other than the default data port, and to wait for a connection rather than initiate one upon receipt of a transfer command. The response to this command includes the host and port address on which this FTP Server is listening.

The passive mode options in the administration system allow the administrator to specify a passive mode base port and a range of ports that can be used for passive mode. If, for example, the base port is set to 10000 and the port range is 1024, passive mode connections will use only the ports from 10000 to 11023.

Figure 4-10 Master pages, Passive Mode screen



The Passive Mode page is where you specify a base port or a base port and range for passive mode.

Specifying a Base Port and Range for Passive Mode

To specify a passive mode base port and range:

1. In the Passive Mode Base Port field, enter the desired port. Enter 0 to clear the field. Clearing the Passive Mode Base Port field also clears the Passive Mode Port Range field.
2. If desired, in the Passive Mode Port Range field, enter a port range.
3. Click Apply.

Mirror Servers

You can improve the reliability and performance of wide area network access to large file repositories by mirroring the file repositories onto multiple Partner Agent Servers. Partner Agent Clients for Windows 95, 98, and NT can query a Partner Agent Server for a list of mirror Servers and route to mirror Servers if a file Server is unavailable.

The Mirror Servers page allows you to control how mirrored Servers are advertised by your Partner Agent Server. The base level Server allows you to list the URL of mirrored Servers to FTP Clients that support the `SITE MIRR` extended command.

Figure 4-11 Master pages, Mirror Servers screen

The screenshot shows the iPlanet web interface for managing mirror servers. The top navigation bar includes links for Help, Master, Access, Security, Statistics, and Agents. The left sidebar is titled 'Master' and lists various administrative functions. The main content area is titled 'Mirror Servers: paradise' and features a section for 'Add New Mirror Server Entry'. This section includes a dropdown menu for selecting the mirror entry type, a text input field for the 'Path to mirror', another text input field for the 'Mirror URL' (currently containing 'ftp://'), and an 'Add Mirror' button.

Adding a Mirror Server Entry

A mirror Server entry consists of the pathname for the file or directory that is mirrored (or the keyword “default,” which indicates that the entire Server file system is mirrored) and the URL of where the mirrored file or directory is located.

To add a new mirror Server entry:

1. Select whether you want the mirror to reflect the entire site or a specific path from the drop-down list.
2. In the Path to mirror field, enter the absolute pathname of the file or directory on your Partner Agent Server that is mirrored on a remote Server. If you are mirroring the entire site, you can leave this field blank.
3. In the Mirror URL field, enter the URL of the Server where your file system, directory or file is mirrored. The URL should be of the form:

ftp:// Servername/ pathname

4. Click Add Mirror.

The new mirror Server entry is added to the list of Current Mirror Server Entries, with a status of Disabled.

Enabling or Disabling a Mirror Server Entry

To enable or disable a mirror Server entry, click Enable or Disable next to the desired entry.

Editing a Mirror Server Entry

To edit an entry in the list of Current Mirror Server Entries:

1. In the Action column next to the desired mirror Server entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Mirror Server Entry section, above the list of Current Mirror Server Entries.
3. Click Apply.

Your changes are reflected in the list of Current Mirror Server Entries.

Deleting a Mirror Entry

To delete a mirror entry, in the Action column next to the desired entry, click Delete.

Example Mirror Entry

If the file `/home/ftp/testfile` is mirrored on the Server

`ftp://newServer/home/ftp/testfile`, you must create the following two mirror entries for the mirror entry to be accessible to real and anonymous and virtual FTP users:

Figure 4-12 Example of mirror server entries

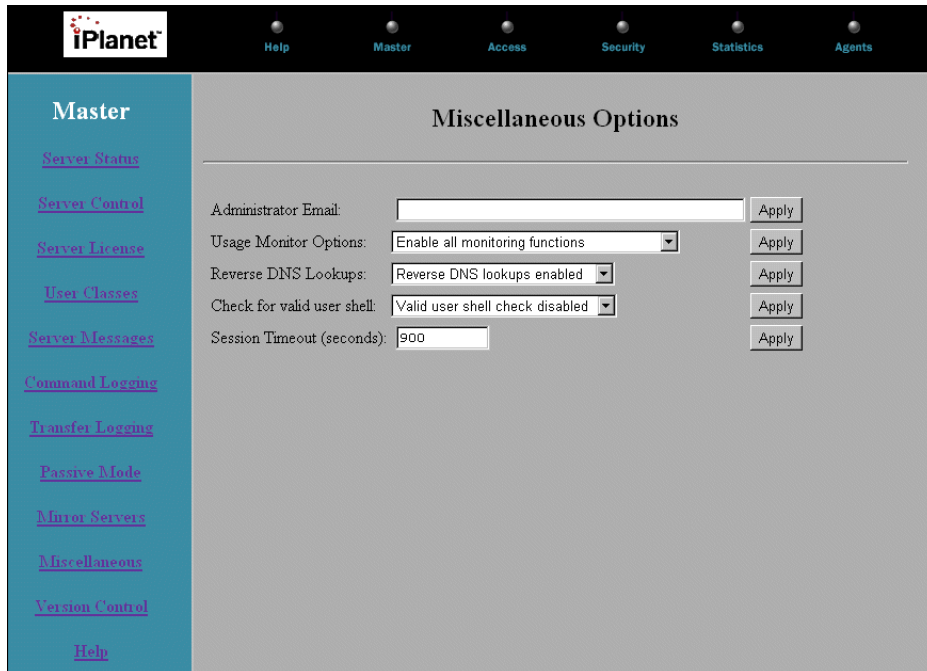
Mirror Target	Mirror URL	Status	Action		
<code>/testfile</code>	<code>ftp://newserver/testfile</code>	Enabled	Disable	Edit	Delete
<code>/home/ftp/testfile</code>	<code>ftp://newserver/home/ftp/testfile</code>	Enabled	Disable	Edit	Delete

NOTE The first entry defines the pathname from the root of the anonymous FTP account or a virtual users virtual root (home directory). Anonymous FTP users use this entry.

The second entry defines an absolute pathname for the file. This entry is used by real users.

Miscellaneous Options

The Miscellaneous page is where you enter the administrator's email address, set usage monitor options, enable reverse DNS lookups and valid user shell checks, and set session timeout limits.

Figure 4-13 Master pages, Miscellaneous Options screen

Setting the Administrator Email Address

The administrator email is the email address of the system administrator of the FTP Server. This address, if specified, is used in several Server response messages and is available for runtime messages via the magic cookie *%E*.

To set the administrator's email:

1. Enter an email address in the Administrator Email field.
2. Click Apply.

Setting Usage Monitor Options

The Server Usage Monitor (STATISTICS/Monitor) can be configured to monitor different aspects of the Server, or it can be turned off entirely. The possible option settings are:

- Enable all monitoring functions.

- Enable monitor-Measure bandwidth—keeps track of the instantaneous transfer rate of each Server process running.
- Enable monitor-Display user commands—keeps track of which command a user is currently executing.
- Enable monitor-No bandwidth/commands—displays process information per Server connection.

NOTE Each of these options requires additional CPU resources per Server process to compute and track the enabled measurements. If monitoring is not needed or you want to increase the performance of the Server, disable all monitoring functions.

- Disable monitor.

To set usage monitor options:

1. Select the desired option from the Usage Monitor Options drop-down list.
2. Click Apply.

Enabling or Disabling Reverse DNS Lookups

Reverse DNS lookups are used to resolve an IP address into a fully qualified domain name for logging purposes. When the DNS Server is under heavy load, the startup time of an FTP session can be significantly affected. If the domain name is not needed in the log files, it is recommended that you turn off this feature.

To enable or disable reverse DNS lookups:

1. Select the desired option from the Reverse DNS Lookups drop-down list.
2. Click Apply.

Enabling or Disabling Valid User Shell Checks

Valid user shell checks are used to determine if a user has a valid shell as listed in the `/etc/shells` file. This option can be disabled.

To disable or enable valid user shell checks:

1. Select the desired option from the Check for valid user shell drop-down list.
2. Click Apply.

Setting the Session Timeout

Set session timeout so Partner Agent Server automatically logs users out if they are inactive for a given time period.

To set the session timeout threshold:

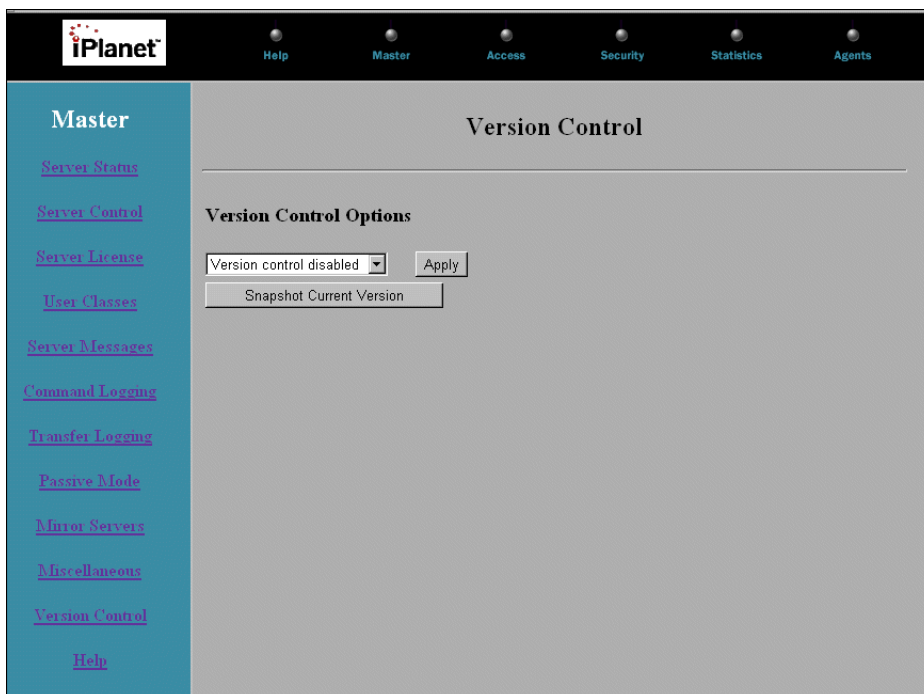
1. Enter a number of seconds in the Session Timeout (seconds) field.
2. Click Apply.

Version Control

Version Control allows Partner Agent Server to store a record of each change made to the administration system's configuration through the administration system; these files are stored on the server in the `$NSBASE/NS-apps/paserver/var/db/hist/conf` directory. Version control is disabled by default.

The Version Control page is where you enable and disable version control, take snapshots of the current system configuration, and revert to an old configuration.

Figure 4-14 Master pages, Version Control screen



The first time you access the Version Control page after you install Partner Agent Server, the following two options are available:

- Enable version control.
- Snapshot current version.

Enabling or Disabling Version Control

When version control is enabled, every change made to the administration system configuration through the administration system is recorded. Each incremental version is stored as the change from the most recent snapshot (version). If no current snapshot exists when a change is made to system configuration with version control enabled, one is taken automatically prior to recording the change.

To enable or disable Version control:

1. Select the desired option from the Version Control drop-down list.

2. Click Apply.

NOTE Version control significantly slows down the system; it is disabled by default.

Taking a Snapshot of the Current Version

A version snapshot copies the administration system configuration files and stores them as a baseline snapshot tagged with the date and time the snapshot was taken. This baseline snapshot is then used as a reference point for any subsequent incremental versions. Once a set of versions are available, you can revert to any incremental version off the current snapshot, or you can revert to a particular snapshot. When you create a new snapshot, you establish a new baseline, and you can revert only to versions of this current baseline.

Versions are never deleted unless you explicitly request it. You can delete any version or snapshot. Deleting a baseline snapshot also deletes all incremental versions based on this snapshot. If you delete the current baseline, the incremental versions of the previous baseline become available again.

Creating a New Baseline

To take a snapshot of the system configuration and create a new baseline, click Snapshot Current Version.

The Current Snapshot list displays a list of the current baseline and any incremental versions of the baseline. Below that is the Previous Snapshots list, which displays any other baseline snapshots.

Incremental Version Display

The first line of an incremental version shows the actual configuration file that has been changed, along with the date and time the version was recorded. The rest of the display shows what has actually changed. The changes are shown as the difference between that version and the baseline. A + indicates something that has been added since the snapshot, and a - indicates something that has been removed since the snapshot. There is no limit to the number of snapshots or incremental versions that can be stored.

Deleting a Version Entry

To Delete a version entry, click Delete next to the desired entry in the list.

Reverting to a Previous Version

To revert to a version, click Revert next to the desired entry.

Recommended Usage

The recommended usage of version control is:

- Get your Partner Agent Server configuration to a stable state with version control enabled.
- Perform a snapshot.
- Disable version control.

This allows you to make subsequent changes to the configuration and also have the ability to revert to a stable version if required.

(Optional) Using the Server Access Controls

This chapter describes how to use the Access Control pages to control access to the Partner Agent Server and the Partner Agent Server administration system. Using Access Controls, you can control the number of simultaneous users that are allowed to connect to the Server, restrict access by user type, user account and host address, lock users into specific directories, define alternate password files for users, and specify file system and upload restrictions.

This chapter covers the main pages for viewing and changing the Access Controls:

- Admin System Host Access
- Partner Agent Server Host Access
- Password Files
- Virtual Groups
- Limiting User Access
- Denying User Access
- Denying Group Access
- Anonymous Logins
- Filesystem Restrictions
- Upload Restrictions
- Download Restrictions

Admin System Host Access

The Admin System Host Access page allows you to control access to the Partner Agent Server administration system. Access is controlled through the use of access rules. The rules define which computer host names or IP addresses that are either allowed or denied to use the administration system. You can specify any number of allow and deny rules, and you can use UNIX-style wildcards such as * to restrict access from subnets.

The Admin System Host Access page has a section for adding new rules and a list of any current access rules.

Figure 5-1 Access pages, Admin System Host Access screen

The screenshot shows the iPlanet Admin System Host Access interface. At the top, there is a navigation bar with the iPlanet logo and several menu items: Help, Master, Access, Security, Statistics, and Agents. On the left side, there is a vertical menu with the following items: Access (highlighted), Admin System Host Access, Partner Agent Server Host Access, Password Files, Virtual Groups, Limit User Access, Deny User Access, Deny Group Access, Anonymous Logins, Filesystem Restrictions, Upload Restrictions, Download Restrictions, and Help.

The main content area is titled "Admin System Host Access". Below the title, there is a section for "Add New Admin System Host Access Entry". This section contains a table with three columns: Rule, Address, and Action. The "Rule" column has a dropdown menu with "Allow access from" selected. The "Address" column has an empty text input field. The "Action" column has a button labeled "Add Entry".

Below the "Add New Admin System Host Access Entry" section, there is a section for "Current Admin System Host Access Entries". This section contains a table with three columns: Rule Order, a dropdown menu with "Deny then Allow" selected, and a button labeled "Change Order".

Reordering Rules

When a browser attempts to connect to the Partner Agent Server administration system, the administration Server looks up the address and host name that the browser is connecting from, and applies the access rules to see if that browser should be allowed to connect. The default setting is for allow rules to be applied first, then for deny rules to be applied. You can change the order that rules are applied.

NOTE Be careful not to lock your own host out of the administration system. If you change the order of rules to Allow then Deny, when there are no rules, you are locked out. If you do get locked out, you must edit the file `NSBASE/NS-apps/paserver/share/.htaccess`.

To change the order that rules are applied:

1. Select the order from the Rule Order drop-down list.
2. Click Apply.

Adding a New Admin System Access Rule Entry

To add a new administration access rule:

1. Select if the rule is a allow or deny rule from the drop-down list.
2. Enter the IP address or host name to which the rule is to apply.
3. Click Add Entry.

The rule is added to the list of Current Admin System Host Access Entries, with a status of Disabled.

Enabling or Disabling an Admin System Access Rule Entry

To enable or disable an administration access rule, click Enable or Disable, next to the desired rule.

Editing an Admin System Access Rule Entry

To edit an administration access rule from the list of Current Administration Access Rules:

1. In the Action column next to the desired class definition, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Admin System Host Access Entry section, above the list of Current Admin System Host Access Entries.
3. Click Apply.

Your changes are reflected in the list of Current Admin System Host Access Entries.

Deleting an Admin System Access Rule Entry

To delete an administration access rule, in the Action column next to the desired rule, click Delete.

Example of Admin System Access Rule Entry

You can use UNIX-style wildcards such as * to manage access from subnets. For example, the following two rules allow access to the administration system only from hosts in the mydomain.com domain:

Figure 5-2 Example of admin system access rule entries

Access Rule	Address	Status	Action
allow from	mydomain.com	Enabled	<input type="button" value="Disable"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Partner Agent Server Host Access

The Partner Agent Server Host Access page allows you to manage access to the Partner Agent Server. This is useful for restricting user account access to known hosts, thereby reducing the potential for hacker access from outside computers. Access is controlled through the use of access rules, which define computer host names or IP addresses that are either allowed or denied access to the administration system. You can specify any number of allow and deny rules, and you can use UNIX-style wildcards such as * to restrict access from subnets.

Figure 5-3 Access pages, Partner Agent Host Access screen

Partner Agent Server Host Access

Add New Partner Agent Server Host Access Entry

Rule	Address	User Class	Action
Allow access from ▾	<input type="text"/>	* ▾	Add Entry

Current Partner Agent Server Host Access Entries

Rule Order:	Deny then Allow ▾	Change Order
-------------	-------------------	--------------

Reordering Partner Agent Server Host Access Rule Entries

When a client attempts to connect to the Partner Agent Server, the Server looks up the user class and address/host name that the client is connecting from, and applies the access rules to see if that client should be allowed to connect. The default setting is for allow rules to be applied first, then for deny rules to be applied. You can change the order that rules are applied.

To change the order that rules are applied:

1. Select the order from the Rule Order drop-down list.
2. Click Apply.

Adding a New Partner Agent Server Host Access Rule Entry

Server access rules allow you to limit access to the Partner Agent Server.

To add a new access rule:

1. Select if the rule is an allow or a deny rule from the Rule drop-down list.
2. Select the user account from the User list. Selecting account * applies the rule to all user accounts.
3. Enter the IP address or host name to which the rule is to apply.
4. Click Add Entry.

The rule is added to the list of Current Partner Agent Server Host Access Entries, with a status of Disabled.

Enabling or Disabling a Partner Agent Server Host Access Rule

To enable or disable a Server access rule, click Enable or Disable, next to the desired rule.

Editing a Partner Agent Server Host Access Rule

To edit an access rule from the list of Server Host Access Rules:

1. In the Action column next to the desired class definition, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Server Host Access Entry section above the list of Server Host Access Entries.
3. Click Apply.

Your changes are reflected in the list of Current Server Host Access Entries.

Deleting a Partner Agent Server Host Access Rule

To delete an access rule, in the Action column next to the desired rule, click Delete.

Example of Partner Agent Server Host Access Rules

You can use UNIX-style wildcards such as * to manage access from subnets. For example, the following two rules only allow access from hosts in the mydomain.com domain:

Figure 5-4 Example of Partner Agent Server host access entries

Access Rule	User Class	Address	Status	Action
deny	*	*	Enabled	Disable Edit Delete
deny	*	198.178.123.*	Disabled	Enable Edit Delete
allow	*	198.160.123.*	Enabled	Disable Edit Delete

A user account or host address can appear in several access restriction rules. This allows you to create very secure access rules, by denying access to all hosts (*), and then adding specific allow rules for the hosts that you want to grant access. For example, denying access to user class * from address *198.178.123.** would mean that nobody is allowed to connect to the Partner Agent Server from the subnet *198.178.123*.

Mixing allow and deny rules can be very powerful. For example, deny access to user class * from address *, then allow access to account * from address *198.160.123.** means that only hosts from the *198.160.123* subnet can access your Partner Agent Server.

Password Files

Partner Agent Server allows you to specify and create additional or alternate password files to the operating system's password file (typically */etc/passwd*).

The default setting is for Partner Agent Server to use the system's default password file to control user logins.

NOTE You can remove or disable the system's default password file and have the Server operate entirely from an alternate password file or from a Virtual Users password file. Also, if all password file entries are removed or disabled, the system password file is used.

The Password Files page is where you add, enable, disable, or remove the password file entries that Partner Agent Server examines. You can also access the pages for setting up a Virtual User password file and virtual permissions.

Virtual Users

Partner Agent Server allows you to define Virtual Users. Virtual Users are listed in a separate password file of type *virtual*, and are virtually locked into their home directories with a chroot-style operation.

The Virtual Users functionality is useful if you are using Partner Agent Server to implement your own file transfer site, where you dynamically add new user accounts to Partner Agent Server and do not want to create real system user accounts for those users. Your application can manage its own password file, which is identical in format to the UNIX system's */etc/passwd* file, and Partner Agent Server allows the users specified in your virtual password file to make connections. Users specified in your virtual password files are virtually chrooted into their home directories.

Figure 5-5 Access pages, Password Files screen

Access

[Admin System Host Access](#)

[Partner Agent Server Host Access](#)

Password Files

[Virtual Groups](#)

[Limit User Access](#)

[Deny User Access](#)

[Deny Group Access](#)

[Anonymous Logins](#)

[Filesystem Restrictions](#)

[Upload Restrictions](#)

[Download Restrictions](#)

[Help](#)

Password Files

Add New Password File Entry

User Type	Password File	Action
Real Users	Specify	<input type="text"/> <input type="button" value="Add File"/>

Current Password File Entries

User Types	Password File	Status	Action			
Real Users	/etc/passwd	Disabled	<input type="button" value="Enable"/>	<input type="button" value="Edit Entry"/>	<input type="button" value="Delete"/>	N/A

Adding a New Password File Entry

To add a new password file entry:

1. Select whether the users in the password file are Real or Virtual. Select from the User Type drop-down list.
2. In the next drop-down list, select either the system's password file (typically `/etc/passwd`) or Specify, to indicate a password file other than your system's default password file.

3. If you chose Specify in the previous field, enter the absolute pathname to a new password file. If you do not enter an absolute pathname, such as `/etc/alt.passwd`, then Partner Agent Server looks for your new password file in the directory `$NSBASE/NS-apps/paserver/etc`. If you specify a file that does not exist, Partner Agent Server creates the file.
4. Click Add File.

The entry is added to the list of Current Password File Entries, with a status of Disabled. If you specified a virtual password file, two buttons display next to the entry, Edit File and Edit Perms. These buttons are used to access the pages to edit the password file and its permissions.

Enabling or Disabling a Password File Entry

To enable or disable a password file entry, click Enable or Disable, next to the desired entry.

Editing a Password File Entry

To edit an password entry from the list of Password File Entries:

1. In the Action column next to the desired password file entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Password File Entry section above the list of Current Password File Entries.
3. Click Apply.

Your changes are reflected in the list of Current Password File Entries.

Deleting a Password File Entry

To delete a password entry, in the Action column next to the desired entry, click Delete.

Editing a Password File

When you specify an additional password file in the Password Files page, you can create or edit entries to the file in the Editing Password File page.

To access the Editing Password File page, click Edit File next to the desired entry in the list of Current Password File Entries.

Figure 5-6 Access pages, Password Files, Editing Password File screen

The screenshot shows the iPlanet web interface for editing a password file. The page title is "Editing Password File: /etc/virtualpasswords". The interface includes a navigation sidebar on the left with links such as "Access", "Admin System Host Access", "Partner Agent Server Host Access", "Password Files", "Virtual Groups", "Limit User Access", "Deny User Access", "Deny Group Access", "Anonymous Logins", "Filesystem Restrictions", "Upload Restrictions", "Download Restrictions", and "Help". The main content area is divided into two sections: "Add New User Entry" and "Current Password File Entries".

The "Add New User Entry" section contains the following form fields:

- Login Name:
- Password:
- Retype Password:
- Uid/Gid:
- Full Name:
- Home Directory:
- Shell:
-

The "Current Password File Entries" section displays a table with the following data:

Login Name	UID	GID	Full Name	Home Directory	Shell	Action
Hal	90000	90000	Hal Ninethousand	/users/psychcomputers	etc/peanutshell	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
virtual1	20001	20001	Virtual User 1	public	etc/noshell	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

At the top of the page is the name of the selected Password file. Below that is a section for adding entries. At the bottom of the page is a list of any Current Password File Entries.

Adding a New Password File Entry

To add a new password entry:

1. Enter a user name in the Login Name field.
2. Enter a password, in the Password field.
3. Retype the password in the Retype Password field.
4. Enter a user ID in the Uid field.
5. Enter a group ID in the adjacent Gid field.
6. Enter the user's full name in the Full Name field.
7. Enter the user's home directory in the Home Directory field.
8. Enter the user's shell pathname in the Shell field.

NOTE This field is optional and is not used by Partner Agent Server

9. Click Add User.

The entry is added to the list of Current Password File Entries with a status of Disabled.

Enabling or Disabling a Password File Entry

To enable or disable a Password File Entry, click Enable or Disable next to the desired entry.

Editing a Password File Entry

To edit a password entry from the list of Password File Entries:

1. In the Action column next to the desired password file entry, click Edit.

Make the desired changes in the fields and drop-down lists in the Edit Password File Entry section above the list of Current Password File Entries.

Click Apply.

Your changes are reflected in the list of Current Password File Entries.

Deleting a Password File Entry

To delete a password entry, in the Action column next to the desired entry, click Delete.

Editing Permissions for Virtual Users

You can control the visibility and access to specified files in the virtual users environment. Files and directories can be allowed or denied. Allow and Deny rules provide a flexible and versatile set of access controls to virtual content.

When you specify an additional password file of type virtual in the Password Files page, you can control permissions for files and directories in the Editing Virtual Permissions page.

To access the Editing Virtual Permissions page, click Edit Perms next to the desired entry in the list of Current Password File Entries.

Figure 5-7 Access pages, Password Files, Editing Virtual Permissions screen

Access

[Admin System Host Access](#)

[Partner Agent Server Host Access](#)

[Password Files](#)

[Virtual Groups](#)

[Limit User Access](#)

[Deny User Access](#)

[Deny Group Access](#)

[Anonymous Logins](#)

[Filesystem Restrictions](#)

[Upload Restrictions](#)

[Download Restrictions](#)

[Help](#)

Editing Virtual Permissions: /etc/virtualpasswords.perms

Add New Virtual Permission Entry

Permission Type	User Class	Select Permission		Action
Shared Directory	*	Rule Order:	Allow then Deny	Add Entry
		Path:		
		Shared As:		

Current Virtual Permission Entries

Conflict Policy: Conflict policy is to Allow Access

Type	User Class	Path	Shared As/Order	Status	Action
Deny Access	virt	*/message.welcome	N/A	Enabled	Disable Edit Delete
Deny Access	virt	*/.message	N/A	Enabled	Disable Edit Delete
Allow/Deny Order	N/A	N/A	Deny then Allow	Enabled	Disable Edit Delete

Virtual permission entries are allow and deny rules, rule order, shared directories, and the rule conflict policy.

Rules

You determine which files and directories can be accessed or not, with Allow or Deny rules. A rule consists of rule type (allow or deny), user class, and the path to which access is allowed or denied.

Rule Order and Conflict Policy

Rule order can be changed at any time, with a Virtual Permission entry. Any allow or deny rules that follow the new order entry, use that order to determine access. If a conflict in rule matching causes an allow and a deny rule to become active, the Conflict Policy determines whether to allow or deny.

Virtual Shared Directories

Virtual Users are limited to browsing only the parts of the file system rooted in their home directory unless a shared directory is specified for that user. A shared directory may be located at any point in the real file system and is defined as a pair of values, the file system mount point and the share name. The share name appears as a directory under the user's home directory. For example to share the directory `/usr/local` with the name *public*, when the virtual user logs in to Partner Agent Server, there is a directory called `public` in the home directory, which refers to the directory `/usr/local`. The virtual user has access to the content of `/usr/local` and below, but not anything higher than `/usr/local` in the real file system.

Adding a Virtual Permission Entry

To add a virtual permission entry:

1. Select a type of permission entry from the Permission Type drop-down list.
2. Select a user class from the User Class drop-down list.
3. For Allow/Deny permissions only, select the rule order from the Rule Order drop-down list.
4. For Allow or Deny rules or for Shared Directories only, enter a path name for the file or directory in the Path field.
5. For Shared Directories only, enter the name to share the directory as in the Shared As field. This is the name that appears in the virtual user's home directory.
6. Click Add Entry.

The entry is added to the list of Current Virtual Permission Entries with a status of Disabled.

Enabling or Disabling a Virtual Permission Entry

To enable or disable a Virtual Permission Entry, click **Enable** or **Disable** next to the desired entry.

Moving Virtual Permission Entries

Once an entry has been added to the list of **Current Virtual Permission Entries**, it can be moved up or down in the list using the arrows to the left of the entry. For example you may want to move an allow or deny entry above or below a rule order entry.

- To move an entry down, click on the down pointing arrow, to the left of the entry.
- To move an entry up, click on the up pointing arrow, to the left of the entry.

NOTE If an entry is at the top of the list, it has no up arrow and if it is at the bottom of the list if it has no down arrow.

Editing a Virtual Permission Entry

To edit a virtual permission entry from the list of **Virtual Permission Entries**:

1. In the **Action** column next to the desired **Virtual Permission** entry, click **Edit**.
2. Make the desired changes in the fields and drop-down lists in the **Edit Virtual Permission Entry** section above the list of **Current Virtual Permission Entries**.
3. Click **Apply**.

Your changes are reflected in the list of **Current Virtual Permission Entries**.

Deleting a Virtual Permission Entry

To delete a virtual permission entry, in the **Action** column next to the desired entry, click **Delete**.

Changing the Conflict Policy

To change the conflict policy:

1. Select a policy from the **Conflict Policy** drop-down list.
2. Click **Change Policy**.

Example of Virtual Permission Entries

To allow access to everything but hide the `msg.welcome` file and any `.message` files, you would define the following rules:

Figure 5-8 Example of virtual permission entries (Part 1)

Current Virtual Permission Entries						
Conflict Policy:		Conflict policy is to Allow Access ▾			Change Policy	
Type	User Class	Path	Shared As/Order	Status	Action	
↓	Allow Access	virt	*	N/A	Enabled	Disable Edit Delete
↑	Deny Access	virt	*/message.welcome	N/A	Enabled	Disable Edit Delete
↑	Deny Access	virt	*/message	N/A	Enabled	Disable Edit Delete

To then deny access to everything in the `beep` directory except a file called `README.txt`, you specify a rule to deny access to everything in `beep`. Then specify a rule that allows access to

`/beep/README.txt`. Since the rule order is still the default, Allow then Deny, the deny rule overrides the allow rule. Therefore you must first specify a new rule order. The Allow `*` rule, (from the previous example), allows access to any file and the Deny `/beep/*` denies access to everything in `/beep`. This results in a conflict. If the conflict policy is to Allow access, then the Allow `*` rule takes precedence. To get the desired result, make sure the conflict policy is to Deny access.

The updated list of Current Virtual Permission Entries looks like:

Figure 5-9 Example of virtual permission entries (Part 2)

Current Virtual Permission Entries						
Conflict Policy:		Conflict policy is to Deny Access ▾			Change Policy	
	Type	User Class	Path	Shared As/Order	Status	Action
↓	Allow Access	virt	*	N/A	Enabled	Disable Edit Delete
↑	Deny Access	virt	*/message.welcome	N/A	Enabled	Disable Edit Delete
↑	Deny Access	virt	*/message	N/A	Enabled	Disable Edit Delete
↑	Allow/Deny Order	N/A	N/A	Deny then Allow	Enabled	Disable Edit Delete
↑	Deny Access	virt	/beep/*	N/A	Enabled	Disable Edit Delete
↑	Allow Access	virt	/beep/README.txt	N/A	Enabled	Disable Edit Delete

NOTE Virtual Permissions apply to real and shared directories.

Master Virtual User

A very powerful way to use the Virtual User functionality is to create a real user in your system's password file. We will call this user *master*. Underneath the master user's account you create a directory for each of your virtual users. Create a virtual password file with an `/etc/passwd` style entry for each of these virtual users. List their user ID and group ID as being the same as your master user's. This way, all files that your virtual users upload are owned by the master. Yet, each virtual user is virtually chrooted into their own account.

To make this even more secure, use the Password Files controls to disable use of the system password file. This way, only your virtual users are able to use the Partner Agent Server Server. For increased security, you can define the master user's shell to be `/etc/noshell`, which effectively stops this user from logging into the system with telnet.

Virtual Groups

Every user on a UNIX system has a user ID and a group ID. UNIX systems use these to set process and file permissions. The Virtual Groups page allows you to specify certain UNIX groups as virtual groups. Any user who is a member of a virtual group becomes a Virtual User whether or not they are members of a Virtual Password file. This is a quick way to make any user virtual based solely on their group membership.

Figure 5-10 Access pages, Virtual Groups screen

The Virtual Groups page contains a section to add new virtual group entries and a list of any current virtual group entries.

Adding a New Virtual Group Entry

To add a new Virtual Group entry:

1. Select the Group you want to add from the Groups drop-down list.
2. Click Add Group.

The entry is added to the list of Current Virtual Group Entries, with a status of Enabled.

Disabling or Enabling a Virtual Group Entry

To disable or enable a virtual group entry, click Disable or Enable, next to the desired entry.

Deleting a Virtual Group Entry

To delete a virtual group entry, in the Action column next to the desired entry, click Delete.

Limiting User Access

Limit rules allow you to limit the number of simultaneous users that Partner Agent FTP Server allows to be connected at one time. Partner Agent Server allows you to define limits on a per user class basis. You can also limit access for different days of the week and even for different times during the day.

NOTE If you do not specify a limit rule for a class, Partner Agent Server assumes that you do not want to limit the maximum number of simultaneous FTP connections of users of that class. You are limited only by the capacity of your Server hardware and the bandwidth of your network (and by the number of licenses).

The Limit User Access page is where you view, create and edit limit rules. A limit rule consists of the name of the user class, the maximum number of users of that class that are allowed to connect to the FTP Server simultaneously, the days and times when the rule is in effect, and whether the rule is enabled or disabled. This allows you to create rules that are not enabled, but remain in the system so that you can quickly enable them.

Figure 5-11 Access pages, Limit User Access screen

Limit User Access

Add New User Limit Entry

User Class	Max Users	Restrictions	Action
<input type="text"/>	<input type="text"/>	<input type="text" value="No Restrictions"/> <input type="text" value="Sunday"/> <input type="text" value="Monday"/> <input type="text" value="Tuesday"/> From (hhmm): <input type="text"/> To (hhmm): <input type="text"/>	<input type="button" value="Add Limit"/>
Message displayed when limit enforced: <input type="text"/>			

Adding a New User Limit Entry

To add a new user limit entry:

1. Select a user class from the User Class drop-down list.
2. Enter the maximum number of simultaneous users for that class in the Max Users field.
3. Select if you want to add day and time restrictions or no restrictions from the next drop-down list.
4. If you chose to add day/time restrictions in the prior field, select which days of the week for which you want the rule to apply. To select a day, click on it in the drop-down list. To select more than one day, hold down your control, (Ctrl), key and click on the desired days.

5. To specify a time range for the rule to be in effect, enter times in the From and To fields. Enter times in the HHMM format, (2-digit hour and 2-digit minute for a 24 hour clock).
6. Enter a message in the Message displayed when limit enforced field. This message is sent to users who try to connect and are refused during the active time of the limit rule.
7. Click Add Limit.

The rule is added to the list of Current User Limit Entries, with a status of Disabled.

NOTE If multiple limit rules are defined for a given time and day period, the first rule in the list of Current User Limit Entries is used.

Enabling or Disabling a User Limit Entry

To enable or disable a user limit entry, click Enable or Disable, next to the desired entry.

Editing a User Limit Entry

To edit a user limit entry from the list of User Limit Entries:

1. In the Action column next to the desired user limit entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit User Limit Entry section above the list of Current User Limit Entries.
3. Click Apply.

Your changes are reflected in the list of Current User Limit Entries.

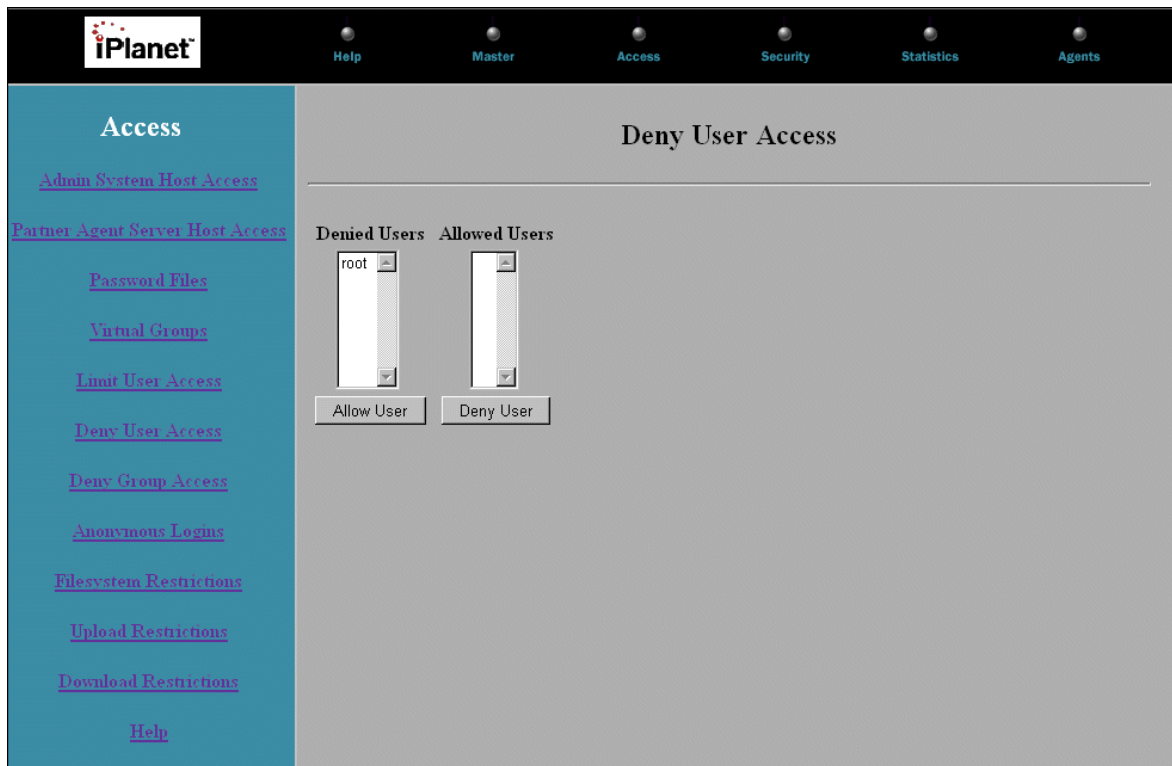
Deleting a User Limit Entry

To delete a user limit entry, in the Action column next to the desired entry, click Delete.

Denying User Access

The Deny User Access page lists the names of user accounts, (login names), that are not allowed to login to the Partner Agent Server, Denied Users, and the names of user accounts that are allowed to login, Allowed Users. You can move names back and forth between the Denied Users and the Allowed Users lists. For maximum security, the Denied Users list should include users like root, bin, boot, daemon, news, nobody, operator, sys and uucp.

Figure 5-12 Access pages, Deny User Access screen



Denying Access to Users

To add a user to the list of Denied Users:

1. Select the user name in the Allowed Users drop-down list.
2. Click Deny User, below the Allowed Users list.

The user is added to the Denied Users list.

Allowing Access to Users

To add a user to the list of Allowed Users:

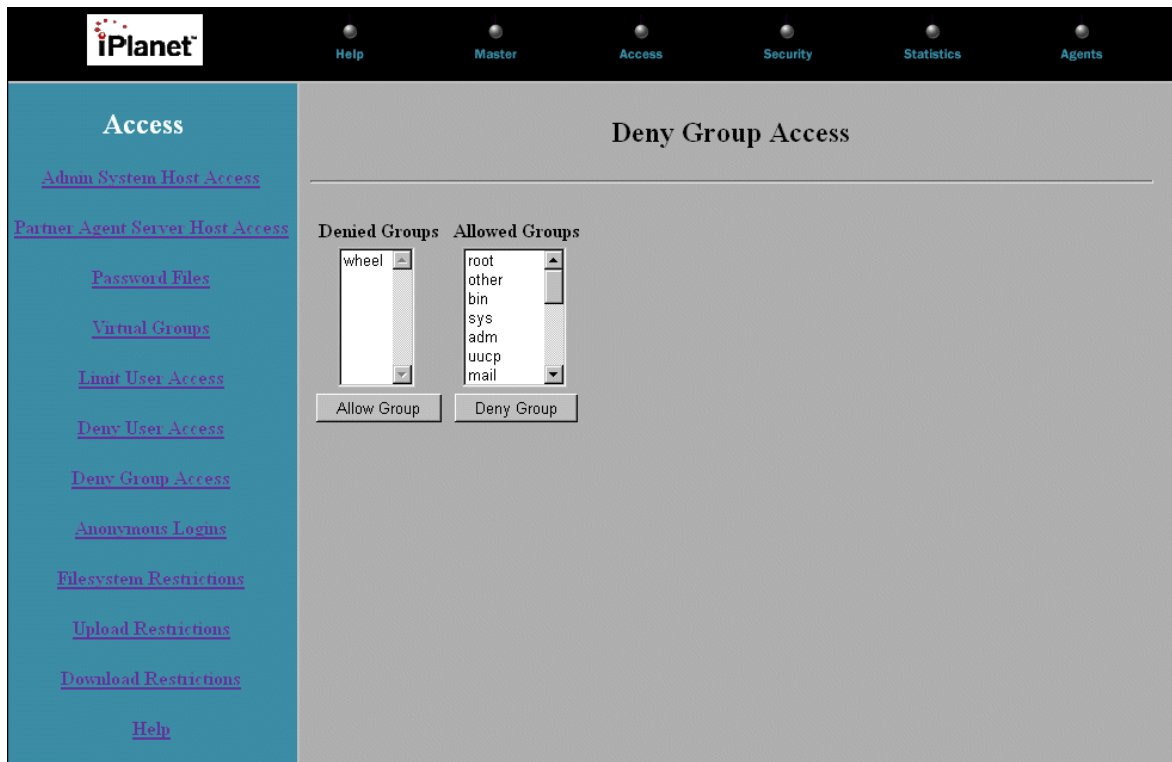
1. Select the user name in the Denied Users drop-down list.
2. Click Deny User, below the Denied Users list.

The user is added to the Allowed Users list.

Denying Group Access

The Deny Group Access page lists the names of Group accounts that are not allowed to login to the Partner Agent Server, Denied Groups. It also lists the names of Group accounts that are allowed to login, Allowed Groups. You can move names back and forth between the Denied Groups and the Allowed Groups lists.

Figure 5-13 Access pages, Deny Group Access screen



Denying Access to Groups

To add a Group to the list of Denied Groups:

1. Select the Group name in the Allowed Groups drop-down list.
2. Click Deny Group, below the Allowed Groups list.

The Group is added to the Denied Groups list.

Allowing Access to Groups

To add a Group to the list of Allowed Groups:

1. Select the Group name in the Denied Groups drop-down list.
2. Click Deny Group, below the Denied Groups list.

The Group is added to the Allowed Groups list.

Anonymous Logins

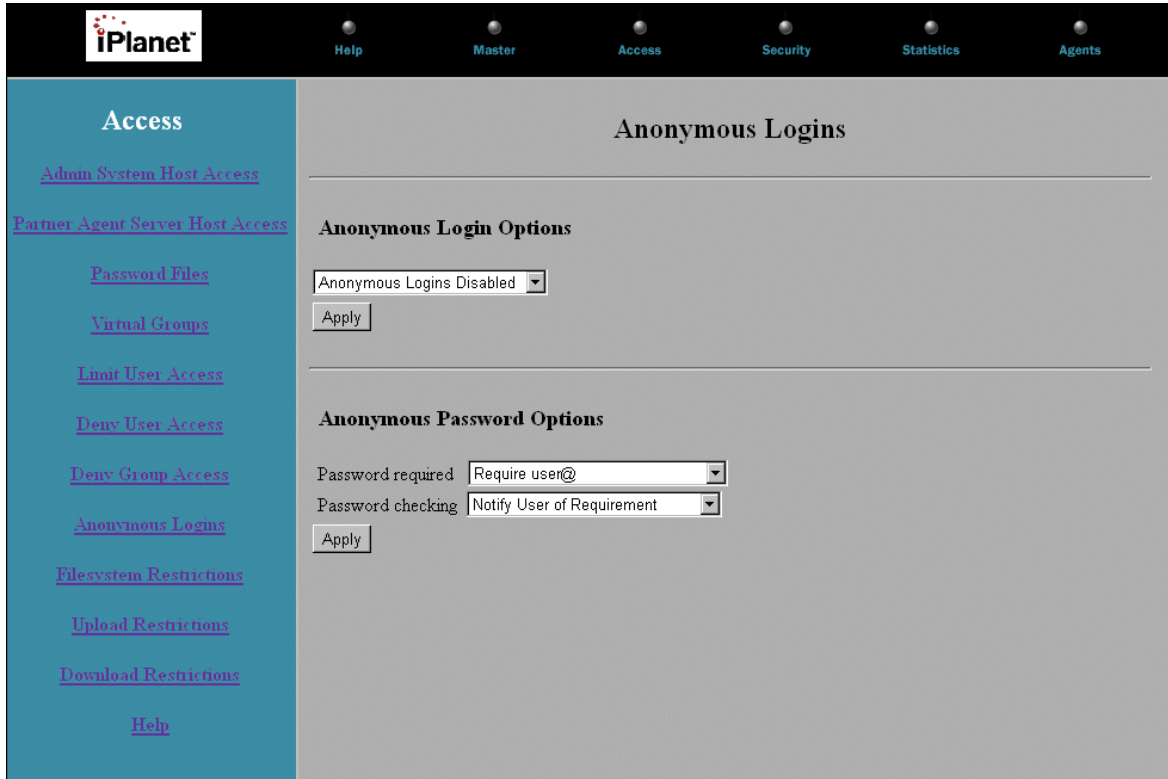
When you install Partner Agent Server, the Install program checks if an FTP account, (user name is ftp), exists. If you created this account at install time, (or if it already exists on your Server), then you can enable or disable anonymous user access. The Anonymous Logins page allows you to turn anonymous user access on and off without having to delete an anonymous FTP user account.

To create the anonymous FTP directory, as the super-user run:

```
$NSBASE/NS-apps/paserver/bin/ftpsetup
```

NOTE You still need to add an entry for user 'ftp' in the system's `etc/passwd` file. `ftpsetup` does not do this for you.

Figure 5-14 Access pages, Anonymous Logins screen



Enabling or Disabling Anonymous Users

To enable or disable anonymous user access:

1. Select the desired setting from the Anonymous Login Options drop-down list.
2. Click Apply.

Your change is applied.

Setting Criteria for Anonymous Passwords

If your Partner Agent Server is configured to allow anonymous users, you can use the Anonymous Password Options section to control the format of passwords that anonymous users must present when using your Server. Typically, anonymous users must supply their e-mail address as the password to the anonymous user account.

To choose the criteria for anonymous user passwords:

1. Select an option from the Password required drop-down list. The options are:
 - m None required—no password checking performed.
 - m Require user@—password must contain an @.
 - m Require user@host.domain.com—password must be an rfc822 compliant address, for example user@server.com.
2. The Server enforces or warns users of your password policy. Select the desired option from the Password checking drop-down list. The options are:
 - m Notify User of Requirement—warn the user, but allow them to log in.
 - m Enforce Password Requirement—warn the user, and then require them to re-authenticate.
3. Click Apply.

Your changes are applied.

Filesystem Restrictions

The Filesystem Restrictions page allows you to control the ability for specific user types to modify files and directories on the Partner Agent Server. You can specify restrictions that allow or deny the operations that users can perform on files and directories on the Server.

There are seven operations that can be allowed or denied. They are:

- Delete a file—determines whether or not a user class may delete files on the Server.
- Rename a file—determines whether or not a user class may rename files on the Server.

- Overwrite a file—determines whether or not a user class may overwrite existing files on the Server.
- Make a directory—determines whether or not a user class may create directories on the Server.
- Remove a directory—determines whether or not a user class may remove directories from the Server.
- Change file mode—determines whether or not a user class may change file access permissions on the Server.
- Change Umask—determines whether or not a user class may change the access permissions mask for new files being uploaded to the Server.

Figure 5-15 Access pages, Filesystem Restrictions screen

The screenshot shows the iPlanet Partner Agent Server Site Administrator's Handbook interface. The top navigation bar includes 'iPlanet' and several menu items: 'Help', 'Master', 'Access' (highlighted), 'Security', 'Statistics', and 'Agents'. The left sidebar contains a navigation menu with 'Access' highlighted and several sub-links: 'Admin System Host Access', 'Partner Agent Server Host Access', 'Password Files', 'Virtual Groups', 'Limit User Access', 'Deny User Access', 'Deny Group Access', 'Anonymous Logins', 'Filesystem Restrictions' (highlighted), 'Upload Restrictions', 'Download Restrictions', and 'Help'.

The main content area is titled 'Filesystem Restrictions'. It features a section for 'Add New Filesystem Restriction Entry' with a form containing the following fields:

Operation	Allowed	User Class	Path	Action
Delete a File	No	*		Add Entry

Below this is a section for 'Current Filesystem Restriction Entries' with a table listing various operations and their status:

Operation	Allowed	Class	Path	Status	Action
Delete a File	Yes	*	*	Enabled	Disable Edit Delete
Rename a File	Yes	*	*	Enabled	Disable Edit Delete
Overwrite a File	Yes	*	*	Enabled	Disable Edit Delete
Make a Directory	Yes	*	*	Enabled	Disable Edit Delete
Remove a Directory	Yes	*	*	Enabled	Disable Edit Delete
Change File Mode	Yes	*	*	Enabled	Disable Edit Delete
Change Umask	Yes	*	N/A	Enabled	Disable Edit Delete

Adding a New Filesystem Restriction Entry

To add a restriction entry that allows or denies an operation:

1. Select an operation from the Operations drop-down list.
2. Select Yes or No to allow or deny the operation. Select an option from the Allowed drop-down list.
3. Select the desired user class from the User Class drop-down list.
4. Enter the path name for which the restrictions apply, in the Path field.
5. Click Apply.

The rule is added to the list of Current Filesystem Restriction Entries, with a status of Disabled.

Enabling or Disabling a Filesystem Restriction Entry

To enable or disable a filesystem restriction entry, click Enable or Disable, next to the desired entry.

Editing a Filesystem Restriction Entry

To edit a filesystem restriction entry in the list of Filesystem Restriction Entries:

1. In the Action column next to the desired filesystem restriction entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Filesystem Restriction Entry section above the list of Current Filesystem Restriction Entries.
3. Click Apply.

Your changes are reflected in the list of Current Filesystem Restriction Entries.

Deleting a Filesystem Restriction Entry

To delete a filesystem restriction entry, in the Action column next to the desired entry, click Delete.

Upload Restrictions

You can grant or revoke permission for users to upload files and to create directories. Partner Agent Server gives you per user control of upload and directory creation permissions. You can also control the owner, group and access permissions of uploaded files. The Upload Restrictions page is where you view, create and edit upload and directory creation restriction rules.

Figure 5-16 Access pages, Upload Restrictions screen

The screenshot shows the iPlanet Partner Agent Server interface. The top navigation bar includes links for Help, Master, Access, Security, Statistics, and Agents. The left sidebar is titled 'Access' and contains several links. The main content area is titled 'Upload Restrictions' and features a form to 'Add New Upload Restriction' and a table of 'Current Upload Restriction Entries'.

Add New Upload Restriction Form:

Upload Directory	Allowed	User Class	Upload Owner	Upload Group	Mode	Action
<input type="text"/>	No	*	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add Entry

Current Upload Restriction Entries Table:

Directory	Allowed	User Class	Owner	Group	Mode	Status	Action
*	No	anon	-	-	-	Disabled	Enable Edit Delete
/incoming	Yes	anon	ftp	bin	0644	Disabled	Enable Edit Delete

Rules are applied in top-down order as they are displayed in the list of upload and directory creation restrictions. This allows you to deny upload permission for a user's account (directory would be *) and then have a following restriction that only enables uploads for a particular subdirectory.

Adding a New Upload Restriction Entry

To create a new upload restriction:

1. Enter the pathname of the directory to be affected by the restriction, in the Upload Directory field. UNIX wildcards such as * are allowed. All directories must be specified based on the file system root in use by the user. For anonymous FTP, this is the directory specified in the FTP user account. For example, if the FTP hierarchy is rooted in `/home/ftp`, and the directory is `/home/ftp/incoming`, you must only specify `/incoming` as the upload directory. Similarly, for virtual users, this is the virtual root directory specified in the virtual password file. For example, if the virtual root is `/home/ftp/virtual/user1` and you want to restrict uploads to this directory, specify `/` as the upload directory.
2. Select Yes or No to allow or deny uploads. Select from the Allowed drop-down list.
3. Select a user class from the User Class drop-down list.
4. If you want to specify the owner, regardless of who uploads a file, select an upload owner from the Upload Owner drop-down list.

NOTE The ownership of the uploaded file is established after the file is successfully uploaded to the Server.

5. If you want to specify the group membership of a file regardless of the group of whoever uploads a file, select an upload group from the Upload Group drop-down list.
6. If you want to have the file mode of uploaded files be other than the default umask mode of the user doing the uploading, change the file mode. Enter the file mode in the File Mode field.

NOTE The file mode is set when the file is opened for writing at the start of an upload.

7. Click Add Entry.

The restriction is added to the list of Current Upload Restriction Entries, with a status of Disabled.

NOTE Rules are applied in top-down order as they appear in the list. Therefore if you are listing multiple rules for a single user class you should list the broadest rules first (e.g. deny uploads for subdirectory *) followed by the narrower rules (e.g. allow uploads for subdirectory /incoming).

Enabling or Disabling an Upload Restriction Entry

To enable or disable an upload restriction entry, click Enable or Disable, next to the desired entry.

Editing an Upload Restriction Entry

To edit an upload restriction entry from the list of Upload Restriction Entries:

1. In the Action column next to the desired upload restriction entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Upload Restriction Entry section above the list of Current Upload Restriction Entries.
3. Click Apply.

Your changes are reflected in the list of Current Upload Restriction Entries.

Deleting an Upload Restriction Entry

To delete an upload restriction entry, in the Action column next to the desired entry, click Delete.

Download Restrictions

You can allow or deny access to specific directories for downloading files by user class. The Download Restrictions page is where you create, view and edit Download restrictions.

Figure 5-17 Access pages, Download Restrictions screen

The screenshot shows the iPlanet Access interface. The top navigation bar includes links for Help, Master, Access, Security, Statistics, and Agents. The left sidebar contains a menu with the following items: Access, Admin System Host Access, Partner Agent Server Host Access, Password Files, Virtual Groups, Limit User Access, Deny User Access, Deny Group Access, Anonymous Logins, Filesystem Restrictions, Upload Restrictions, Download Restrictions, and Help.

The main content area is titled "Download Restrictions" and contains the following sections:

Add New Download Restriction

Download Directory	Allowed	User Class	Action
<input type="text"/>	No	*	<input type="button" value="Add Entry"/>

Current Download Restriction Entries

Directory	Allowed	User Class	Status	Action
*	No	anon	Disabled	<input type="button" value="Enable"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
/pub	Yes	anon	Disabled	<input type="button" value="Enable"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Adding a New Download Restriction Entry

To add a download restriction entry:

1. Enter the pathname of the directory to be affected by the restriction, in the Download Directory field. UNIX wildcards such as * are allowed. All directories must be specified based on the file system root in use by the user. For anonymous FTP, this is the directory specified in the FTP user account.

2. Select Yes or Now to allow or deny downloads. Select an option from the Allowed drop-down list.
3. Select the desired user class from the User Class drop-down list.
4. Click Add Entry.

The restriction is added to the list of Current Download Restriction Entries, with a status of Disabled.

Enabling or Disabling a Download Restriction Entry

To enable or disable a download restriction entry, click Enable or Disable, next to the desired entry.

Editing a Download Restriction Entry

To edit a download restriction entry from the list of Download Restriction Entries:

1. In the Action column next to the desired download restriction entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Download Restriction Entry section above the list of Current Download Restriction Entries.
3. Click Apply.

Your changes are reflected in the list of Current Download Restriction Entries.

Deleting a Download Restriction Entry

To delete a download restriction entry, in the Action column next to the desired entry, click Delete.

(Optional) Using the Server Security Controls

This chapter describes how to use the Security control pages to configure security settings for Partner Agent Server, enable or disable FTP commands, and perform audits.

This chapter covers the pages for viewing and changing the Security Controls:

- Secure Sockets Layer
- User Authentication
- Login Failures
- FTP Commands
- Entrust Configuration
- Security Audit

Secure Sockets Layer

The Secure Sockets Layer (SSL) is the security protocol that Partner Agent Server uses. SSL can be enabled or disabled globally. If SSL is enabled, then there are two client certificate options, plus any user class SSL requirements. Encryption (SSL) can be set as optional or mandatory on a user class basis.

When SSL is made mandatory, the Partner Agent Server allows only connections that are encrypted using SSL; if the client does not support SSL, it cannot connect. If SSL is optional, then it is up to the client to decide whether or not to use SSL. If the client requests an SSL connection, it is negotiated; if not, the Partner Agent Server allows the connection to proceed without encryption.

NOTE Even if SSL is optional, if the client requests SSL and then fails the Client Certificate Verification, the connection will be rejected.

By default, Partner Agent Server has been pre-configured for maximum security. This means that data passing over the connection between the Partner Agent Client and the Partner Agent Server is encrypted via SSL. It also means that client users must present a valid certificate to the server for authentication.

Figure 6-1 Security pages, Secure Sockets Layer screen

Secure Sockets Layer

SSL Options

Secure Sockets Layer Enabled

Client Certificate Mandatory

Client Certificate Verification Enabled

Add New SSL Users Encryption Entry

User Class	Encryption	Action
<input type="text" value="*"/>	<input type="text" value="Optional"/>	<input type="button" value="Add Entry"/>

Current SSL Users Encryption Entries

User Class	Encryption	Status	Action
*	Optional	Enabled	<input type="button" value="Disable"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

The Secure Sockets Layer page is where you set up the SSL options for Partner Agent Server. In the first section of the page, there are three drop-down lists for setting the SSL options. Below that there is a section for adding SSL User Encryption Entries and below that a list of any Current SSL Users Encryption Entries.

Enabling or Disabling SSL

To globally enable or disable SSL:

1. Select the desired option from the first drop-down list.
The default value is Secure Sockets Layer Enabled.
2. Click Apply.
Your change is applied.

Modifying the Requirement for Client Certificates

To require or make optional a client certificate:

1. Select the desired option from the second drop-down list.
The default value is Client Certificate Mandatory.
2. Click Apply.
Your change is applied.

Enabling or Disabling Client Certificate Verification

To enable or disable client certificate verification:

1. Select the desired option from the third drop-down menu.
The default value is Client Certificate Verification Enabled.
2. Click Apply.
Your change is applied.

Adding a New SSL Users Encryption Entry

To add a new SSL users encryption entry:

1. Select a user class from the User Class drop-down list.
2. Select whether encryption is Mandatory or Optional. Choose from the Encryption drop-down list.
3. Click Add Entry.

The definition is added to the list of Current SSL Users Encryption Entries, with a status of Disabled.

Enabling or Disabling an Encryption Entry

To enable or disable an encryption entry, click Enable or Disable next to the desired encryption entry.

Editing an Encryption Entry

To edit an encryption entry from the list of Current SSL Users Encryption Entries:

1. In the Action column, next to the desired encryption entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit SSL Users Encryption Entry section above the list of Current SSL Users Encryption Entries.
3. Click Apply.

Your changes are reflected in the list of Current SSL Users Encryption Entries.

Deleting an Encryption Entry

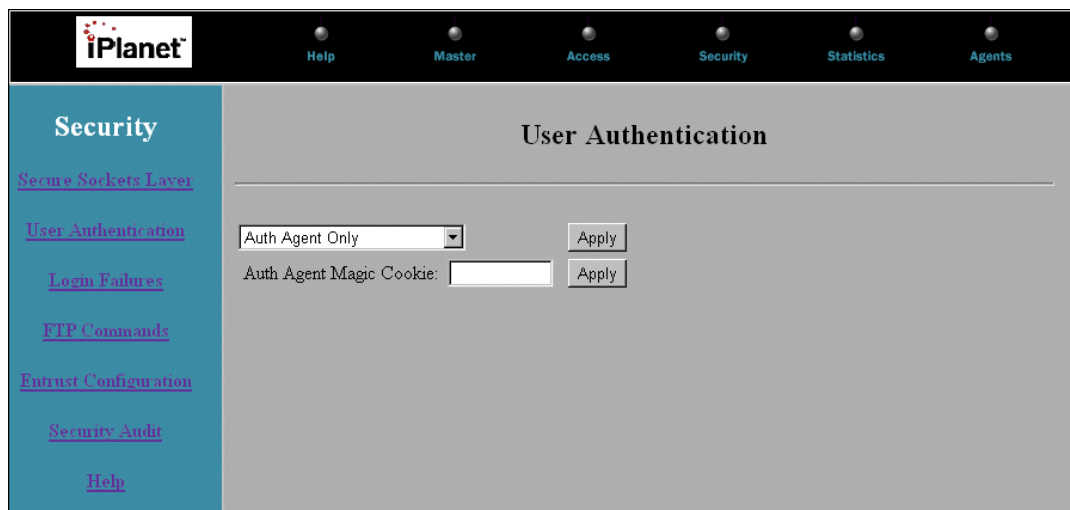
To delete an encryption entry, in the Action column, next to the desired entry, click Delete.

User Authentication

User authentication is the method by which a real or virtual user-supplied password is authenticated. This can be accomplished using the standard UNIX password based authentication or by invoking a defined Authentication ActiveAgent (auth agent) to perform the authentication. For more on ActiveAgents see *Chapter 8: ActiveAgents*.

Partner Agent Server has been pre-configured to extract the username from the Distinguished Name (DN) string and prompt for a password after a user's certificate has been authenticated. This username/password combination must correspond to a valid ECXpert member. As pre-configured, the Server authenticates users only via the ECXpert authentication ActiveAgent program (`ecxpas-login`), which calls ECXpert APIs to perform this authentication against the ECXpert member directory/database.

Figure 6-2 Security pages, User Authentication screen



The screenshot displays the iPlanet web interface for User Authentication. At the top, the iPlanet logo is on the left, and navigation tabs for Help, Master, Access, Security, Statistics, and Agents are on the right. The left sidebar is titled 'Security' and contains links for [Secure Sockets Layer](#), [User Authentication](#), [Login Failures](#), [FTP Commands](#), [Trust Configuration](#), [Security Audit](#), and [Help](#). The main content area is titled 'User Authentication' and features two configuration options:

- Auth Agent Only:** A dropdown menu with 'Auth Agent Only' selected and an 'Apply' button.
- Auth Agent Magic Cookie:** A text input field and an 'Apply' button.

Setting User Authentication Options

To set the options:

1. Select an authentication order from the first drop-down list.
The default value is Auth Agent Only.
2. Click Apply.
3. Enter a value for the Magic Cookie in the Auth Agent Magic Cookie field, (“A Few Things to Know about User Authentication,” on page 129.)
4. Click Apply.

A Few Things to Know about User Authentication

- If an auth agent magic cookie is defined, its value is used to check against the password field in the user’s password entry obtained from a password file or using a user configuration agent. If it matches, only call the auth agent. If it does not match, only standard password based authentication is performed.
- If an auth agent magic cookie is not defined, or it is set to off, the authentication order is checked.
- If the authentication order is password files only, only standard password based authentication is done.
- If the authentication order is auth agent only, only the auth agent is called. If the authentication order directive is password agent, standard password based authentication is done. If it fails, the auth agent is called as a second chance.
- If the authentication order directive is agent password, the auth agent is called. If it fails then standard password based authentication is done as a second chance.
- A non-existent auth agent is considered an authentication failure. So, for example, if auth-order is agent password, and there is no agent, the first round of authentication fails and the second round attempts standard password based authentication. If authentication order is auth agent only, the authentication always fails.
- If authentication order is not defined, only standard password based authentication is done.

Login Failures

For security reasons, we recommended you limit the number of consecutive failed logins before the Partner Agent FTP Server terminates the connection with a user. If you do not limit this, a hacker could connect once and keep trying multiple passwords on a user's account. Set the failed login threshold at three attempts, for example, so users have to reconnect after every three failed attempts. The Login Failures page is where you can change the failed login threshold.

Figure 6-3 Security pages, Login Failures screen



Changing the Failed Login Threshold

To change the failed login threshold:

1. Enter the desired value in the Disconnect after field.
2. Click Apply.

Your change is applied.

FTP Commands

Partner Agent FTP Server uses a number of standard and customized FTP commands. The FTP Commands page is where you enable and disable the available FTP commands in Partner Agent Server. You can also determine which user classes you want to allow or restrict FTP Command privileges.

Figure 6-4 Security pages, FTP Commands screen

The screenshot shows the IPlanet FTP Commands management interface. The main content area is titled "FTP Commands" and contains two sections:

Add New FTP Command Entry

FTP Command	Enable/Disable	User Class	Action
CWD	Enable FTP Command	*	Add Entry

Current FTP Command Entries

FTP Command	Enabled/Disabled	Class	Action
CWD	FTP Command Enabled	*	Edit Delete
DELE	FTP Command Enabled	*	Edit Delete
HELP	FTP Command Enabled	*	Edit Delete
IDLE	FTP Command Enabled	*	Edit Delete
LIST	FTP Command Enabled	*	Edit Delete
MDTM	FTP Command Enabled	*	Edit Delete
MKD	FTP Command Enabled	*	Edit Delete
MODE	FTP Command Enabled	*	Edit Delete
NLST	FTP Command Enabled	*	Edit Delete
PASV	FTP Command Enabled	*	Edit Delete
PORT	FTP Command Enabled	*	Edit Delete
PWD	FTP Command Enabled	*	Edit Delete
RETR	FTP Command Enabled	*	Edit Delete
REST	FTP Command Enabled	*	Edit Delete

Setting FTP Command Options

To set FTP command options:

1. Select a command from the FTP Command drop-down list.
2. Select either Enable FTP Command or Disable FTP Command from the Enable/Disable drop-down list.
3. Select the User Class you want to allow or deny use of the selected FTP command. Select from the User Class drop-down list.
4. Click Add Entry.

The entry is added to the list of Current FTP Command Entries.

Editing an FTP Command Entry

To edit an FTP Command entry from the list of Current FTP Command Entries:

1. In the Action column, next to the desired FTP Command entry, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit FTP Command Entry section above the list of Current FTP Command Entries.
3. Click Apply.

Your changes are reflected in the list of Current FTP Command Entries.

Deleting an FTP Command Entry

To delete an FTP Command entry, in the Action column next to the desired entry, click Delete.

Entrust Configuration

Entrust is an option available for some UNIX platforms. If it is not set up for your system, the Entrust page displays the message “Entrust not Available.”

Security Audit

Your Partner Agent Server has an integrated security auditing system, called EnGuard™, that can be enabled to automatically runs daily. EnGuard alerts you of potential security holes and possible break-ins. EnGuard uses pre-programmed security checks in combination with sophisticated historical inference algorithms to detect security weaknesses on your Server.

EnGuard Features

- Checks for security holes caused by interactions between Partner Agent Server and other programs such as Telnet.
- Analyzes anonymous FTP hierarchies for security holes.
- Analyzes Server configuration files and binaries for security holes.
- Historical inference engine for detecting breakins.
- Notifies system administrators through e-mail or logfiles.
- Generates textual or HTML security reports.
- Runs daily as a cron job, for continual monitoring.

Running EnGuard as a Cron Job

EnGuard is commented out by default, but can be enabled to run as part of the nightly Partner Agent Server cron job that is configured at install time. EnGuard maintains a historical database about your Partner Agent Server site. As it is run successively, it uses this database to spot anomalies in accesses to your site, and new security holes that may have appeared since the last time EnGuard was run

NOTE If you set the “reportformat email” control in your config file, you can have EnGuard send you an email whenever it detects new problems with your site. This way, it remains invisible unless problems are detected.

To enable EnGuard:

- Edit `$NSBASE/NS-apps/paserver/bin/rotate` and un-comment the EnGuard entry:

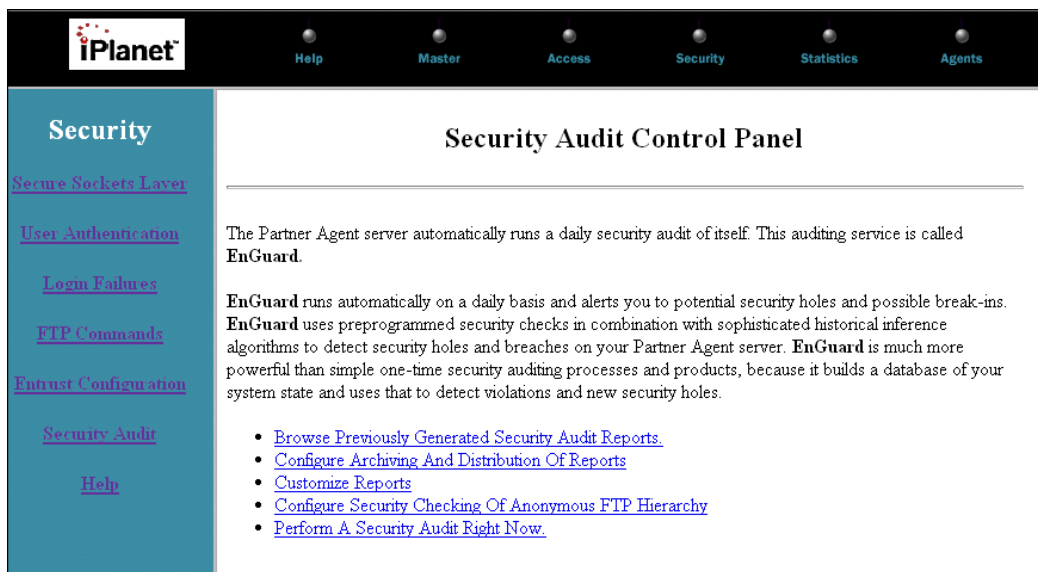
```
# $NSBASE/NS-apps/paserver/bin/enguard
```

Security Audit Control Panel

The Security Audit Control Panel page is where you browse reports, configure reports, perform an instantaneous security check and update the Enguard settings.

This page has links to other pages and controls. Each page contains a link back to the Security Audit Control Panel page.

Figure 6-5 Security pages, Security Audit Control Panel screen



Browsing Previously Generated Security Audit Reports

To go to the Browse Security Audit Reports Archive page, click Browse Previously Generated Security Audit Reports. If you enabled archiving of reports, (“Configuring Archival and Distribution of Reports,” on page 136). This page displays the historical archive of any Partner Agent Server security audit reports that your Server has run.

Reports are stored as date-stamped files in the `$NSBASE/NS-apps/paserver/var/db/audit/htmllogs` and `$NSBASE/NS-apps/paserver/var/db/audit/textlogs` directories. You can page through the archive, viewing links to twenty reports at a time, in most-recently-created order. Security audit reports are archived forever, so to get rid of old archived reports, delete them from their directories.

Configuring Archival and Distribution of Reports

The Archiving and Distribution of Security Reports page allows you to configure the archival and distribution of security reports. You can have security audits e-mailed to a list of users.

Reports are archived as date-stamped files in the `$NSBASE/NS-apps/paserver/var/db/audit/htmllogs` and `$NSBASE/NS-apps/paserver/var/db/audit/textlogs` directories. You can enable or disable the archiving of reports. If you disable the archiving of reports, a single report file is overwritten every time EnGuard is run. This avoids using a lot of disk space for archiving reports, but is not an advisable setting as it does not preserve reports which may have detected transient or new security weaknesses.

To access the Archiving and Distribution of Security Reports page, click Configure Archiving and Distribution of Reports. This page is where you enable or disable archiving of reports and sending of the daily security audit results.

Figure 6-6 Security pages, Security Audit Control Panel, Archiving and Distribution of Security Reports screen

The screenshot shows the iPlanet Security Audit Control Panel. The top navigation bar includes links for Help, Master, Access, Security, Statistics, and Agents. The left sidebar contains links for Security, Secure Sockets Layer, User Authentication, Login Failures, FTP Commands, Entrust Configuration, Security Audit, and Help. The main content area is titled 'Archiving And Distribution Of Security Reports' and contains the following text and form fields:

The Partner Agent server automatically runs a daily security audit of itself. This auditing service is called **EnGuard**. The results of the security audits are viewable in the [Browse Previously Generated Security Audit Reports](#) page.

If you would like the Partner Agent auditing system to send you the results of the daily security audits via e-mail, check the checkbox below and fill in the names of the users (separate names with a space) and the full pathname of the e-mail program to use.

Send E-Mail Report:

Recipient list:

E-Mail program to use:

EnGuard archives its reports so that you can browse them later. There is some value to keeping a historical archive of your security reports, as a shrewd systems administrator might find subtle security holes or anomalies when browsing the historical reports. Reports are run on a daily basis.

Archive Old Reports: Yes No

[Security Audit Control Panel](#)

Archival and Distribution of Security Reports Options

To set the options for archiving and distributing daily security audits:

1. Click the Send Email Report's checkbox to enable or disable sending of email reports.
2. List e-mail addresses in the Recipient list field. The user names in the recipient list should be separated with spaces. For example: `root admin dave@myserver.com`.
3. Enter the pathname to the mail application in the E-Mail program to use field. For example: `/bin/mailx`.

4. Choose Yes or No for whether or not Partner Agent Server should archive old reports.
5. To apply all your changes for this page, click Change Audit Settings.

Customizing Reports

The Customize Security Audit Reports page is where you set which security checks are performed and what gets reported. To access this screen, from the Security Audit Control Panel page, click Customize Reports.

Figure 6-7 Security pages, Security Audit Control Panel, Customize Security Audit Reports screen

iPlanet Help Master Access Security Statistics Agents

Security

[Secure Sockets Layer](#)

[User Authentication](#)

[Login Failures](#)

[FTP Commands](#)

[Entrust Configuration](#)

[Security Audit](#)

[Help](#)

Customize Security Audit Reports

The security auditing system performs a number of security checks. You can disable these checks by unchecking the items below.

- checking of /etc/passwd.
- checking of /etc/shadow (solaris only).
- checking of denied users.
- checking of user passwords.
- checking of the FTP daemon, inetd.conf and related binaries.
- checking of the anonymous FTP file hierarchy.
- checking for failed logins in syslog.
- checking for repeated failed logins in syslog.
- checking if files have been modified since the last run.
- checking if new files in the anonymous FTP file hierarchy are shared libraries.

The security auditing system will print a report of the configuration errors, security warnings and security violations every time it runs. Additionally, you can ask for a progress report. This is a verbose report that details all the actions of the security auditing process. If you are receiving e-mail reports, you will only receive a report if there is something to report. If you want to be notified every time that the security auditing system runs, regardless of whether there were security issues for you to investigate, then you should enable OK Reports or Progress Reports.

- Report Progress.
- Report OK.
- Report Errors.
- Report Warnings.
- Report Violations.

Change EnGuard Settings

On the Customize Security Audit Reports page there are a list of options that can be enabled or disabled. Each option has a checkbox. A checkmark in a item's checkbox means that item is enabled, no checkmark means it is disabled.

To Enable or Disable an item:

1. Click in the checkbox, to make a checkmark appear or disappear.
2. Click Change EnGuard Settings, to enact your changes.

Enabling or Disabling Security Checks

Partner Agent Server's security auditing system performs a number of security checks. You can enable or disable these checks. The security checks that you can enable or disable are:

- checking of `/etc/passwd`.
- checking of `/etc/shadow`.
- checking of denied users.
- checking of user passwords.
- checking of the FTP daemon, `inetd.conf` and related binaries.
- checking of the anonymous FTP file hierarchy.
- checking for failed logins in `syslog`.
- checking for repeated failed logins in `syslog`.
- checking if files have been modified since the last run.
- checking if new files in the anonymous FTP file hierarchy are shared libraries.

Enabling or Disabling Report Settings

The security auditing system prints a report of the configuration errors, security warnings and security violations every time it runs. Additionally, you can ask for a progress report. This is a verbose report that details all the actions of the security auditing process. If you are receiving E-mail reports, you only receive a report if there is something to report. If you want to be notified every time the security auditing system runs, regardless of whether there were security issues for you to investigate, then you should enable OK Reports or Progress Reports.

- **Report Progress**

The progress report is a report that details all the actions of the security auditing process. If you want to be notified every time that the security auditing system runs, regardless of whether there were security issues for you to investigate, then you should enable OK Reports or Progress Reports.

This disables or enables the printing of a report, even if no violations, warnings or errors were detected. The default is for an OK report to be printed every time a security audit is run. You can disable the printing of an OK report if you have scheduled EnGuard to run frequently and you do not want frequent notification that everything is OK. However, if you want to be notified that auditing is still running on an automatic basis, you should enable OK printing.

- **Report Errors**

This disables or enables the printing of errors in your reports. The default is for error printing to be enabled. Errors notify you of problems with the setup of the auditing system itself (very rare). It is advisable for you to enable the printing of errors.

- **Report Warnings**

This disables or enables the printing of security warnings in your reports. The default is for warning printing to be enabled. Warnings notify you of potential problems or failed Partner Agent Server logins. These may or may not be security holes. It is advisable for you to enable the printing of warnings. Warnings are displayed like this:

WARNING: /etc/ftpusers file does not exist.

- **Report Violations**

This disables or enables the printing of security violations in your reports. The default is for violation printing to be enabled. Violations notify you of serious security holes and hacker attacks on your Partner Agent Server. It is strongly advised that you enable the printing of violations. Violations are displayed like this:

VIOLATION: /home/ftp/pub/tmp/test has write permission for OWNER and GROUP and OTHERS.

This is a serious security problem, as it lets all FTP users write into the file. To correct this problem, execute the command `chmod 555 /home/ftp/pub/tmp/test` as root.

Configuring Security Checking Of Anonymous FTP Hierarchy

The security auditing system checks the anonymous FTP directory for security holes. There may be directories in the anonymous FTP directory hierarchy that you do not want EnGuard to check. You can exclude these directories by adding them to the excluded directory list. Doing this removes the directories and their child directories from the EnGuard audit list. For example, if you have a directory that is writable by all users, and you do not care if any of the subdirectories or files inside this hierarchy are writable. Be warned that not checking an entire directory hierarchy can open up some serious security holes on your Server.

To access the Auditing The Anonymous FTP Hierarchy page, click [Configure Security Checking Of Anonymous FTP Hierarchy](#).

Figure 6-8 Security pages, Security Audit Control Panel, Auditing the Anonymous FTP Hierarchy screen

Security

[Secure Sockets Layer](#)

[User Authentication](#)

[Login Failures](#)

[FTP Commands](#)

[Trust Configuration](#)

[Security Audit](#)

[Help](#)

Auditing The Anonymous FTP Hierarchy

The security auditing system checks the anonymous FTP directory for security holes. There may be directories in the anonymous FTP directory hierarchy that you do not want EnGuard to check. You can exclude these directories by adding them to the following list. Doing this removes the directories and their child directories from the EnGuard audit list.

Add Directory To Exclude List

There may be individual files in the anonymous FTP directory hierarchy that you do not want EnGuard to check. You can exclude these files by adding them to the following list.

List Of Excluded Files

~ftp/dev/zero	<input type="button" value="Remove File From Exclude List"/>
~ftp/dev/udp	<input type="button" value="Remove File From Exclude List"/>
~ftp/dev/ticotsord	<input type="button" value="Remove File From Exclude List"/>
~ftp/dev/tcp	<input type="button" value="Remove File From Exclude List"/>
~ftp/incoming	<input type="button" value="Remove File From Exclude List"/>

Add File To Exclude List

Excluding a Directory

To exclude a directory from the daily security check:

1. Enter a directory path name in the Add Directory to Exclude List field.
2. Click Add Directory to Exclude List.

The Directory is added to the list of any excluded directories.

Removing a Directory from the Excluded List

To remove a directory from the excluded list, next to the list entry, click Remove Directory from Exclude List.

The Directory is removed from the list of any excluded directories.

Excluding a File

To exclude a file from the daily security check:

1. Enter a file path name in the Add File To Exclude List field.
2. Click Add File To Exclude List.

The file is added to the list of any excluded files.

Removing a File from the Excluded List

To remove a file from the excluded list, next to the list entry, click Remove File from Exclude List.

The Directory is removed from the list of any excluded files.

Performing a Security Audit

To perform a real-time security audit of the Server, click Perform A Security Audit Right Now. This typically only takes a few seconds on a lightly used system. When the audit is complete you are presented with a link to view the security audit report.

To view the report, click [Click here to view security audit report](#).

To return to the Security Audit Control Panel page, click Security Audit Control Panel.

(Optional) Using the Server Statistics Controls

The Partner Agent Server logs all file transfers to and from the server. By default, when the Server is installed, a crontab entry is created that runs every night at midnight. This nightly job archives the transfer logs and then runs a statistics generation program on the logs.

The Statistics control pages are where you view server traffic, configure which statistics are logged, view previously generated statistics and generate statistics.

The main pages for viewing and changing the Statistics Controls are:

- Server Usage Monitor
- Server Usage Statistics Control Panel

Server Usage Monitor

The Server Usage Monitor page allows you to view traffic on the server in real time. The monitor lists all users currently logged into the server, (by user class and individually), the date and time of their login, user class, process ID of their login session, their transfer command and the bandwidth being consumed.

Figure 7-1 Statistics pages, Server Usage Monitor screen

Server Usage Monitor Tue Feb 8 22:36:54 PST 2000

Auto Refresh every seconds

Server Usage Snapshot by User Class

User Class	Logged In	Max Allowed	Bandwidth
local	0	unlimited	0 bytes/sec
real	0	unlimited	0 bytes/sec
anon	0	unlimited	0 bytes/sec
virt	0	unlimited	0 bytes/sec
Total Instantaneous Server Bandwidth			0 bytes/sec

This screen can be refreshed on a regular basis with the auto refresh feature or can be refreshed instantaneously with the Refresh button.

To generate an instant snapshot of server traffic, click Refresh.

To start repeated automatic updates:

1. Enter the number of seconds between updates in the Auto Refresh Every field.
2. Click Start Auto Refresh.

To disable auto-refresh mode, when it is enabled, click Stop Auto Refresh.

Server Usage Snapshot by User Class

This section lists, on a per user class basis, the number of users logged in, the maximum number of simultaneous users of that class that are allowed to be logged in, and bandwidth being used. It also displays the total network bandwidth being used.

Server Usage Snapshot by Connection

This section lists information about each connection. Next to each entry in the list of connections is a button to kill a connection.

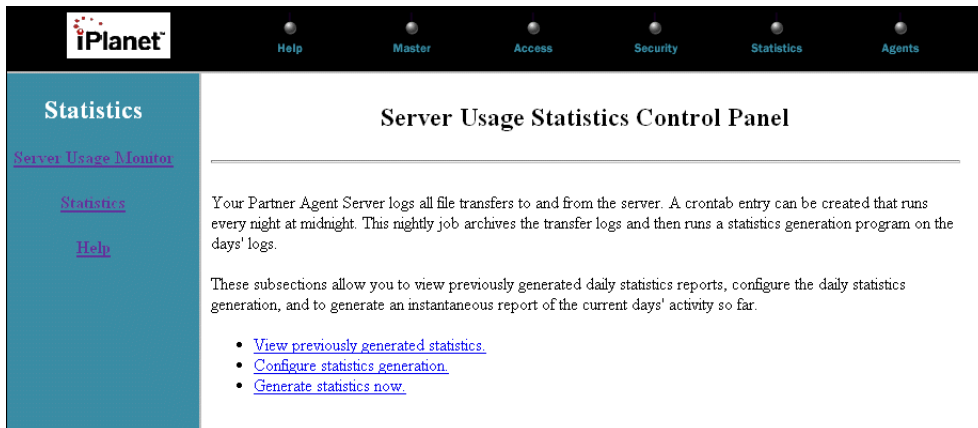
To kill a connection, click Kill next to the connection.

Server Usage Statistics Control Panel

The server automatically generates a nightly set of server activity statistics based on the daily transfer logs. These statistics are saved as a set of HTML pages. They are accessed from the Server Usage Statistics Control Panel page.

To access this page, click Statistics on the left-hand side of the screen.

Figure 7-2 Statistics pages, Server Usage Statistics Control Panel screen



Server Usage Statistics Viewer

The Server Usage Statistics Viewer page allows you to view the archive of daily statistics reports. To access this page, from the Server Usage Statistics Control Panel page, click View previously generated statistics.

Figure 7-3 Statistics pages, Server Usage Statistics Control Panel, Server Usage Statistics Viewer screen



A maximum of twenty reports display per page. If there are more than twenty reports, use the Next and Previous links to view more pages of reports.

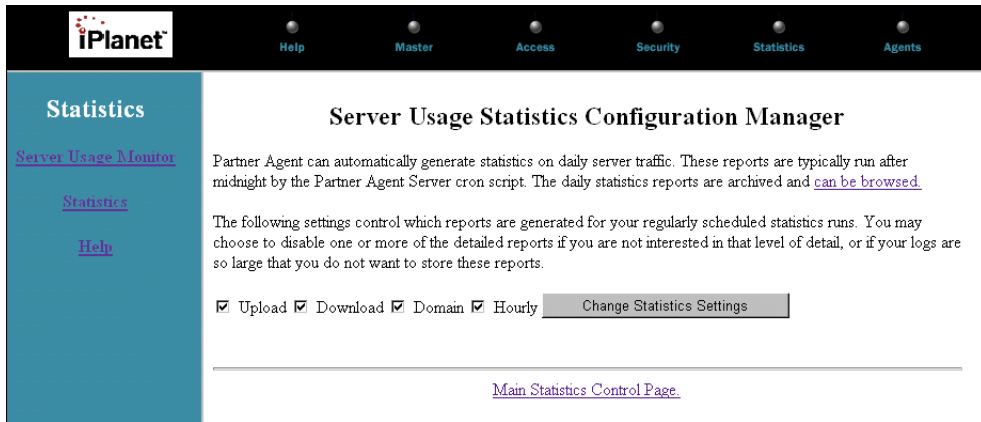
To view a report, click the appropriate link.

Server Usage Statistics Configuration Manager

The Server Usage Statistics Configuration Manager page allows you to change the settings on the statistics that are generated. Currently all statistics files are archived. You may want to disable one or more of the detailed reports if you are not interested in that level of detail, or if your logs are too large.

To access the Server Usage Statistics Configuration Manager page, from the Server Usage Statistics Control Panel page, click Configure statistics generation.

Figure 7-4 Statistics pages, Server Usage Statistics Control Panel, Server Usage Statistics Configuration Manager screen



On the Server Usage Statistics Configuration Manager page there are a list of report options that can be enabled or disabled. Each option has a checkbox. A checkmark in a item's checkbox means that item is enabled, no checkmark means it is disabled.

The following reports can be enabled or disabled:

Table 7-1 ReportDescription

Upload	Statistics about files that were uploaded to the server.
Download	Statistics about files that were downloaded from the server.
Domain	Statistics about the number of different hosts that connected to the server.
Hourly	Statistics about the hourly server traffic during a 24 hour period.

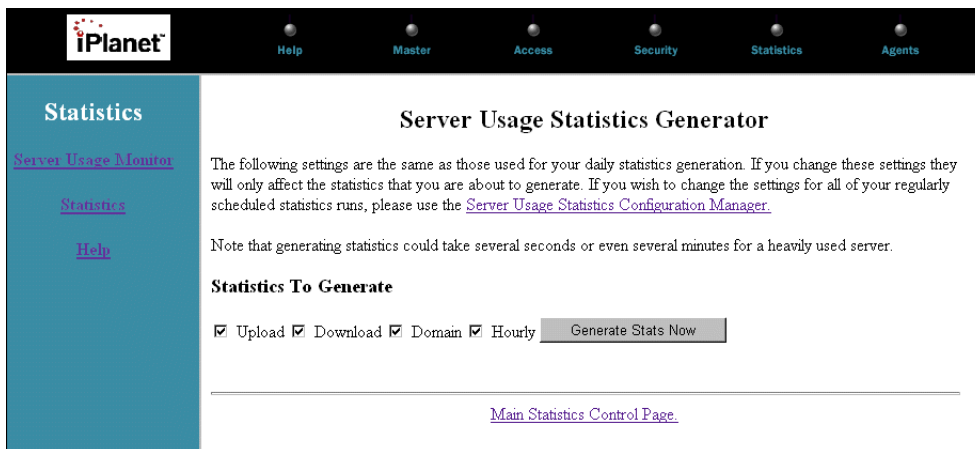
To enable or disable a report:

1. Click in the appropriate checkbox.
2. To commit your changes click Change Stats Settings.

Server Usage Statistics Generator

The Server Usage Statistics Generator page allows you to generate statistics immediately. The default setting of the server is for statistics to be run every night when the nightly Partner Agent Server cron script runs. To access the Server Usage Statistics Generator page, from the Server Usage Statistics Control Panel page, click Generate statistics now.

Figure 7-5 Statistics pages, Server Usage Statistics Control Panel, Server Usage Statistics Generator screen



The initial settings are taken from your statistics settings. You can change the settings before you run the generation process. There are a list of report options that can be enabled or disabled. Each option has a checkbox. A checkmark in a item's checkbox means that item is enabled, no checkmark means it is disabled.

NOTE Generating statistics could take several seconds or even several minutes for a heavily used server.

The following reports can be enabled or disabled:

Table 7-2 ReportDescription

Upload	Statistics about files that were uploaded to the server.
Download	Statistics about files that were downloaded from the server.
Domain	Statistics about the number of different hosts that connected to the server.
Hourly	Statistics about the hourly server traffic during a 24 hour period.

To enable or disable a report, click in the appropriate checkbox.

To generate the statistics, click [Generate Stats Now](#).

Once the statistics have been computed (this could take several minutes if you have a lot of traffic on your site), a link displays, that lets you view the statistics results.

To view the results, click [Click Here To View The Results](#).

To return to the Server Usage Statistics Control Panel page, click [Main Statistics Control Page](#).

Server Usage Statistics Control Panel

(Optional) Using the Server ActiveAgents

This chapter describes ActiveAgents, Server side programs that are triggered by user activity on the Server, and how to set them up.

The following topics are discussed in this section:

- Introducing ActiveAgents
- Agent Access
- Agent Server Port
- ActiveAgents
- ActiveAgent Descriptions

Introducing ActiveAgents

ActiveAgents are triggered when certain events occur, for example when a user logs in or out, when a file transfer is initiated or completed, or as a file filters during transfer.

The following types of agent processes are supported.

- Login agents are run when a user logs into the Partner Agent Server.
- Logout agents are run when a user disconnects from the Partner Agent Server.
- Incoming agents are run when files are being uploaded to the Partner Agent Server.
- Outgoing agents are run when files are being downloaded from the Partner Agent Server.
- Cert agents are run during the SSL negotiation if certificate verification is enabled.
- Auth agents are run when the PASS command is received from a client.
- Config agents are run when the USER command is received from a client.
- FTP/HTTP commands are run when particular FTP or HTTP commands are received from a client.
- FTP commands are run when particular FTP commands are received from a client.

Several ActiveAgents that work specifically with ECXpert are automatically installed with the Partner Agent Server (see “ECXpert ActiveAgents,” on page 24).

ActiveAgent Server

ActiveAgents are started by the ActiveAgent Server (agentd daemon) that was installed during the Partner Agent Server installation. The agentd routes packets between Partner Agent Server file transfer processes and the ActiveAgents. You can run your agentd on a different Server machine from your Partner Agent Server, thereby creating a multi-tiered architecture where agent processes are run on the remote ActiveAgents Server. This architecture has many security benefits, as well as the scalability benefit of being able to create multi-tiered file processing applications.

NOTE To run your agentd on different Server from your Partner Agent Server, you must install Partner Agent Server on both Servers, and you must configure both ActiveAgent systems identically. The ActiveAgent system relies on the following configuration files being identical on the Partner Agent ftpd and agentd Servers:

`$NSBASE/NS-apps/paserver/conf/agentd.conf`

`$NSBASE/NS-apps/paserver/conf/agentd.host`

`$NSBASE/NS-apps/paserver/conf/agentd.user`

`$NSBASE/NS-apps/paserver/conf/agents.conf`

Environment Variables

ActiveAgents can process parameters passed in as environment variables. Some types of incoming and outgoing agents act as filters on files and so must be able to either accept or generate file streams on the standard UNIX I/O streams (stdin and stdout). An ActiveAgent can be written in several languages such as C, C++ and PERL.

An ActiveAgent is passed any optional arguments that were specified at configuration time. The calling sequence for an ActiveAgent is:

`agent [optional arguments]`

The environment variables that are passed into ActiveAgents take the form:

`DXAGENT_VARNAME=value` environment variables

The environment variables that are passed into ActiveAgents are:

Environment Variable Name	Description
DXAGENT_TARGET	This variable is set to the filename matching a target wildcard in the <code>agents.conf</code> file for incoming or outgoing agents, or the user name for auth, config, login, and logout agents.
DXAGENT_TARGETDIR	This is the dirname portion of the fully qualified target path, relative to the root of the filesystem in effect for this user.
DXAGENT_TARGETPATH	This is the dirname portion of the fully qualified target path, relative to the real root of the filesystem. For real users, <code>DXAGENT_TARGETDIR</code> and <code>DXAGENT_TARGETPATH</code> are the same. <ul style="list-style-type: none"> For anonymous users, <code>DXAGENT_TARGETPATH</code> is the concatenation of the <code>DXAGENT_ROOTDIR</code> and <code>DXAGENT_TARGETDIR</code> variables. For virtual users, <code>DXAGENT_TARGETPATH</code> is the concatenation of the <code>DXAGENT_HOMEDIR</code> and <code>DXAGENT_TARGETDIR</code> variables.
DXAGENT_FULLTARGET	Complete absolute pathname of the target.
DXAGENT_CERTCOOKIE	The variable that is set by the cert agent. For more information on cookies, "Notes on Agent Supplied Cookies," on page 158.
DXAGENT_AUTHCOOKIE	The variable that is set by the auth agent. For more information on cookies, "Notes on Agent Supplied Cookies," on page 158.
DXAGENT_USERCOOKIE	The variable that is set by the user agent. For more information on cookies, "Notes on Agent Supplied Cookies," on page 158.
DXAGENT_COOKIE	A persistent cookie that can be set by the cert, auth or login agents. The last cookie that is set by one of these three agents. If no cookie is supplied the value of this variable is null. For more information on cookies, "Notes on Agent Supplied Cookies," on page 158.
DXAGENT_PWD	The current working directory in which the user is logged in.
DXAGENT_ROOTDIR	The filesystem root in effect for a user. <ul style="list-style-type: none"> For real and virtual users, this is always <code>/</code>. For anonymous users, this is the directory that anonymous logins get chrooted into.

Environment Variable Name	Description
DXAGENT_HOMEDIR	<p>The users home directory.</p> <ul style="list-style-type: none"> • For real and virtual users, this is their home directory as obtained from their passwd file entry. • In the case of virtual users, this is the directory we perform a virtual chroot into, and always appears as / to the virtual user. • For anonymous user, this is always /.
DXAGENT_REMOTEHOST	<p>The DNS name of the host the client is connecting to the Partner Agent Server from.</p> <p>Note: In a proxy environment, this can be the name of the proxy Server host.</p>
DXAGENT_REMOTEADDR	<p>The IP address of the host the client is connecting to the Partner Agent Server from.</p> <p>Note: In a proxy environment, this can be the address of the proxy Server host.</p>
DXAGENT_LOGINNAME	Login name of the user.
DXAGENT_LOGINPASS	Password of the user (email address for anonymous users).
DXAGENT_USERTYPE	The user type (real, anonymous, guest or virtual).
DXAGENT_CLIENT	The client that connected to agentd to trigger this agent. Typically this is a Partner Agent Server ftpd or httpd.
DXAGENT_TRIGGER	The agent trigger type.
DXAGENT_TYPE	The agent type.

Notes on Agent Supplied Cookies

- If an auth agent is defined, the first line of output, up to a `\n`, is treated as a cookie.
- If the first line of output of a cert, auth or login agent consists solely of the `\n` character, it is considered to be a NULL cookie.
- If there is no cert, auth or login agent defined, or if the agent supplied cookies are NULL, there is no cookie, and the `DXAGENT_COOKIE` environment variable is not set.
- If a login agent is also defined, the first line of output, up to a `\n`, is treated as a cookie and overwrites the auth agent supplied cookie. If the first line of output consists solely of the `\n` character, it is considered a NULL cookie and the auth agent supplied cookie remains in force. When a login agent is not defined, the auth agent cookie is continued to be used for the rest of the session.
- The cert cookie sets the `DXAGENT_CERTCOOKIE` environment variable.
- The auth cookie sets the `DXAGENT_AUTHCOOKIE` environment variable.
- The login cookie sets the `DXAGENT_USERCOOKIE` environment variable.
- The `DXAGENT_COOKIE` environment is set to the last cookie supplied by an agent.

Bundled ActiveAgents

Partner Agent Server comes bundled with several ActiveAgents:

- A Login and a Logout agent that demonstrate how to use the `DXAGENT_TARGET` variable in login/logout agents.
- An Incoming End agent called `notify` that sends e-mail to the user `ftp@localhost` whenever a new file is uploaded into the `/incoming/` directory.
- An Outgoing End agent called `notify` that sends e-mail to the user `ftp@localhost` whenever a file is downloaded from the `/pub/` directory.
- A cert verify agent called `verify` that demonstrates how to preform custom client certificate verification. It works in conjunction with client certificates generated by `gencerts`.

Agent Access

The Agent Server Host Access page is where you set up the rules that determine which Partner Agent Servers are allowed to connect to the agentd ActiveAgents Server. The access rules allow and deny access from programs and network IP addresses. It is important to confine access to the agentd Server to trusted hosts and to trusted applications. The preferred applications are the Partner Agent Server ftpd and httpd processes.

ActiveAgent Server Host Access rules either allow or deny access to the agentd Server by host name or host IP address. When a process tries to connect to the agentd to run an ActiveAgent, the agentd Server applies its access rules to determine if the connecting process is allowed to run ActiveAgents. Because you could have some fairly powerful ActiveAgents defined, you should maximize the security of the ActiveAgent Server Access rules to prevent unauthorized programs from attempting to run ActiveAgents.

Figure 8-1 Agents pages, Agent Server Host Access screen

The screenshot displays the iPlanet Agent Server Host Access configuration page. The top navigation bar includes links for Help, Master, Access, Security, Statistics, and Agents. The left sidebar shows the 'Agents' menu with sub-links for Agent Server Host Access, Agent Server Port, ActiveAgents, and Help. The main content area is titled 'Agent Server Host Access' and features a section for 'Add New Agent Server Host Access Entry' with a form containing a 'Rule' dropdown (set to 'Allow access from'), an 'Address' text input, a 'Server Client' dropdown (set to '*'), and an 'Add Entry' button. Below this is a section for 'Current Agent Server Host Access Entries' with a 'Rule Order' dropdown (set to 'Deny then Allow') and a 'Change Order' button. A table lists the current access rules:

Access Rule	Address	Server Client	Status	Action
deny	*	*	Enabled	Disable Edit Delete
allow	*	ftpd	Enabled	Disable Edit Delete
allow	*	httpd	Enabled	Disable Edit Delete
allow	*	creator	Enabled	Disable Edit Delete

Reordering the Rules

The order that the access rules are applied is important, and can be configured. The default setting is that deny rules are applied first, followed by the allow rules. The most typical, and default, configuration is to deny access from all Servers (deny from *), and then to allow access only from localhost.

To change the order that the access rules are applied:

1. Select the rule order, (Allow then Deny or Deny then Allow), from the drop-down list in the Rule Order section.
2. Click Change Order.

NOTE Do not set the order of the rules to be Allow then Deny and also have a rule that denies connections from *. If you do, no processes are allowed to connect to your ActiveAgent agentd Server.

Adding a New Agent Server Host Access Rule Entry

To add a new Agent Server Host Access rule:

1. Select if the rule is an allow or a deny rule from the Rule drop-down list.
2. Enter the IP address or host name of the Server that is to be allowed or denied, in the Address field. You may use UNIX-style wildcards such as *. For example, allowing connections from *.mydomain.com allows Partner Agent Servers from the mydomain.com network to connect to your ActiveAgent agentd Server.
3. Select the client process from the Server Client drop-down list.
4. Click Add Entry.

The rule is added to the list of Current Agent Server Host Access Entries, with a status of Disabled.

Enabling or Disabling an Agent Server Host Access Rule Entry

To enable or disable an agent Server host access rule, click Enable or Disable, next to the desired rule.

Editing an Agent Server Host Access Rule

To edit an agent Server host access rule from the list of Current Agent Server Host Access Entries:

1. In the Action column, next to the desired class definition, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit Agent Server Host Access Entry section above the list of Current Agent Server Host Access Entries.
3. Click Apply.

Your changes are reflected in the list of Current Agent Server Host Access Entries.

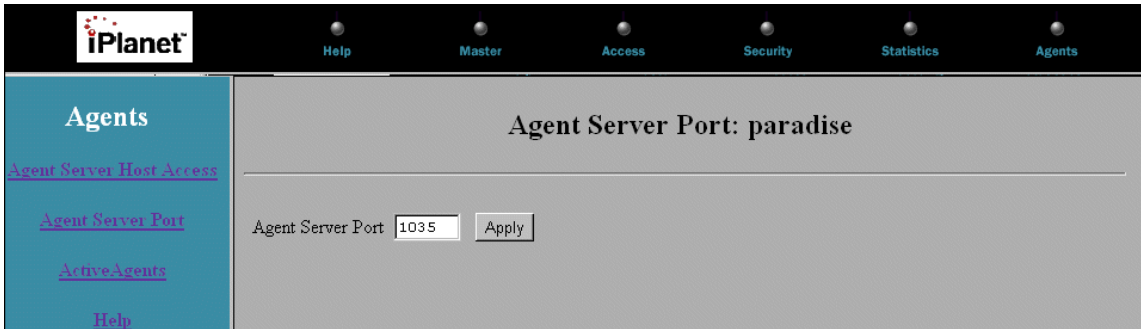
Deleting an Agent Server Host Access Rule

To delete an agent Server host access rule, in the Action column, next to the desired rule, click Delete.

Agent Server Port

The Agent Server Port page is where you configure the network port your ActiveAgents agentd Server is listening on for Partner Agent Server connections.

Figure 8-2 Agents pages, Agent Server Port screen



The default port is 4455. To change the network port:

1. Enter the port in the Agent Server Port field.
2. Click Apply.

When you change the port, the agentd Server is re-initialized with this new port. All new Partner Agent Server sessions connect to the agentd on the new port.

ActiveAgents

There are a number of events that can trigger the ActiveAgent agentd Server to run an agent. You can define a different agent for each user type, and you can specify that filenames match your predefined target filename patterns before an agent is run. This gives you the utmost flexibility in defining active Server-based processing that is integrated with your file transfers.

The ActiveAgents page displays any ActiveAgents that have been configured. You can enable, disable, or remove any ActiveAgent in the list of Current ActiveAgents Entries. You can also add new ActiveAgent entries.

The ActiveAgent programs shown in Figure 8-3 are preconfigured and preinstalled for Partner Agent Server.

Figure 8-3 Agents pages, Active Agents screen

The screenshot shows the ActiveAgents web interface. On the left is a navigation menu with links for Agent Server Host Access, Agent Server Port, ActiveAgents, and Help. The main content area is titled 'ActiveAgents' and contains a form to 'Add New ActiveAgent Entry'. The form has several fields: Agent Type (Certificate Verification), User (*), Execution (User/Group), Exec As User (-), and Exec As Group (-). Below these are fields for Target, Agent, and Arguments. At the bottom of the form are fields for Server Address, Server Port, and an Action button labeled 'Add Agent'.

Below the form is a table titled 'Current ActiveAgents Entries' with the following data:

Agent Type	User	Exec As	Target	Agent	S
Certificate Verification	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa-fd-certify	lo
Password Authentication	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa	lo
User Configuration	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa	lo
Login	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa-welcome	lo
Logout	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa-bye	lo
Incoming End	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa	lo
Outgoing End	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa	lo
Outgoing Error	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa	lo
Outgoing Start	*	actraadm/actra	*	/sunny/actraadm/ecx/smg/NS-apps/ECXpert/bin/ecxpa	lo

An ActiveAgent entry consists of the following items.

- Agent Type lists the type of the agent.
- User lists the user name, (or users via wildcards), which causes this agent to be executed (in conjunction with the target).
- Execution lists if the execution permissions of the agent are User/Group or for an FTP user.
- Exec As User lists which user ID the agent runs as.
- Exec As Group lists which group ID the agent runs as.
- Target lists the filenames that trigger the agent.

- Agent lists the ActiveAgent name.
- Server lists the IP address of the ActiveAgents agentd Server that Partner Agent Server connect to. Typically your agentd runs on the same machine as your Partner Agent Server ftpd.
- Port lists the port of the ActiveAgents agentd Server that Partner Agent Server connect to.
- Status displays whether the particular agent is enabled or disabled.

Chaining ActiveAgents

The same event and target can invoke more than one Agent. This is known as chaining agents. The Agents are invoked in the order they appear in the list of Current Active Agent Entries. To change the order of chained agents, use the arrows next to the left of the entries in the list of ActiveAgent Entries.

Adding a New ActiveAgent Entry

To add and configure a new ActiveAgent entry:

1. Select the agent type from the Agent Type drop-down list.
2. Select a user name that you want to trigger your agent, (in conjunction with the target), from the User drop-down list.
3. Select, from the Execution drop-down list, whether you want the ActiveAgent to run with specified User/Group permissions or with the permissions of the user who triggers the ActiveAgent.

NOTE If the agent is to be run with the user group and ID of the user who is logged in to Partner Agent Server, then a “—” is displayed in the next two fields.

4. Select the User who's permissions you want to run the ActiveAgent with, from the Exec as User drop-down list.
5. Select the User Group who's permissions you want to run the ActiveAgent with, from the Exec as Group drop-down list.

6. Enter a Target filename pattern that triggers the agent in the Target field. The incoming or outgoing agent only runs if the filename that is being transferred matches the target of an Incoming or Outgoing agent (depending on whether the file is being uploaded or downloaded). UNIX-style wildcards are permitted. For example, a Target of `*.exe` matches all files with a suffix of `.exe`, while a Target of `*` matches all files.

NOTE All target matching is done with an absolute path, so if you want to match a target in any directory, prepend the wildcard character `*` to the target. For example, to match the target `README` in any directory, use `*README` and not just `README`. In addition, all targets must be specified based on the file system root in use by the user. For anonymous FTP, this is the directory specified in the FTP user account. For example, if the FTP hierarchy is rooted in `/home/ftp`, and the target is `/home/ftp/incoming/foo`, you must only specify `/incoming/foo` as the target. Similarly, for virtual users, this is the virtual root directory specified in the virtual password file. For example, if the virtual root is `/home/ftp/virtual/user1` and you want to specify a target of `/home/ftp/virtual/user1/bar`, you must only specify `/bar` as the target.

7. Enter the name or pathname of the executable agent program or script in the Agent field. If you do not specify an absolute pathname, `agentd` searches in `$NSBASE/NS-apps/paserver/bin/agents/` for the agent executable.
8. Enter any command-line arguments that you want to pass to the agent in the Arguments field.
9. Enter the Host IP address of the ActiveAgent `agentd` Server in the Server Address field. This can be your loopback address (typically `127.0.0.1`) if the `agentd` and the Partner Agent Server `ftpd` are running on the same machine.
10. Specify the port on which the `agentd` is listening for connections in the Server Port field.
11. Click Add Agent.

The new agent definition is added to the list of Current ActiveAgent Entries with a status of Disabled.

Enabling or Disabling an ActiveAgent entry

To enable or disable an ActiveAgent entry, click Enable or Disable, next to the desired entry.

Editing an ActiveAgent entry

To edit an ActiveAgent entry from the list of Current ActiveAgent Entries:

1. In the Action column, next to the desired class definition, click Edit.
2. Make the desired changes in the fields and drop-down lists in the Edit ActiveAgent Entry section above the list of Current ActiveAgent Entries.
3. Click Apply.

Your changes are reflected in the list of Current ActiveAgent Entries.

Deleting an ActiveAgent entry

To delete an ActiveAgent entry, in the Action column next to the desired entry, click Delete.

ActiveAgent Descriptions

The following ActiveAgents are bundled with Partner Agent Server.

Certificate Agent (cert)

The cert agent is invoked during the SSL negotiation if certificate verification is enabled. The cert agent receives the client certificate in PEM-encoded format via standard input, and is delimited by:

```
-----BEGIN CERTIFICATE-----  
<base-64 certificate data>  
-----END CERTIFICATE-----
```

This certificate may be decoded and then validated via any mechanism desired. The agent is required to output multiple lines of information. Each line is terminated with the newline character. The lines have the following significance:

Line 1	specifies the certificate cookie which is used to identify the session. This cookie is passed to other agents to allow state maintenance across agents.
Line 2	specifies the local user name that Partner Agent Server uses to set up the permissions of this user.
Line 3	... n are sent back to the client as a Server side message. The client displays this information in the interactive FTP session, or in its logs.

The agent also returns an exit code which determines how the results are interpreted:

Exit code 0	This user is authenticated, require password authentication with user returned.
Exit code 1	This user is authenticated, do not require a password.
Any other exit code	This user is not authenticated, terminate the SSL negotiation and disconnect session.

User Configuration Agent (config)

The config agent is called immediately after receiving the USER command from a client. The config agent can provide per user information to the Partner Agent Server such as a password file entry, upload restrictions and access control.

In the following example, a password entry for the user demo is provided so that an `etc/passwd` entry on the system running Partner Agent Server is not needed. In addition, the user is tagged as virtual, effectively chrooting to the virtual user's home directory, without requiring an anonymous login. The config agent output is:

```
[passwd]
virtual demo: <password>:4000:4000:Agent Demo:/tmp/demo:/bin/csh
```

The following example demonstrates how you can provide access control on a per user basis. The default rule order for Partner Agent Server is defined as deny then allow in `paserver.host`. This can be changed to allow then deny.

The rule, shown below, only allows the user demo access to Partner Agent Server via localhost.

```
[access]
allow demo localhost
deny demo *
```

Password Authentication Agent (auth)

The auth agent is called immediately after receiving the PASS command from a client. The first line of output, up to a \n is treated as an auth cookie by the Partner Agent Server. Remaining lines are sent transparently to the user as an authentication phase message. The agent is required to output multiple lines of information. Each line is terminated with the newline character. The lines have the following significance:

Line 1	specifies the authentication cookie which can be used to identify this session. This cookie is passed to other agents to allow state maintenance across agents.
Line 2	... n are sent back to the client as a Server side message. The client displays this information in the interactive FTP session, or in its logs.

Any non-zero exit status is treated as an authentication failure by Partner Agent Server.

NOTE An auth agent is never invoked for anonymous logins.

There are two **filedrive.conf** directives: **auth_magic** and **auth_order**. The default **filedrive.conf** contains the following two lines:

```
auth-magic @
auth-order agent passwd
```

If **auth-magic** is defined, its value is used to check against the <password> field. If it matches, only the auth agent is called. If the value does not match, only standard password based authentication is used.

If auth-magic is not defined, the auth-order is checked. If the auth-order directive is passwd agent, standard password based authentication is used. If it fails, the auth agent is called as a second chance.

If the auth-order directive is agent passwd, the auth agent is called. If it fails, standard password based authentication is used as a second chance.

A non-existent auth agent is considered an authentication failure. For example, if auth-order is agent passwd, and there is no agent, the first round of authentication fails and standard password based authentication is attempted for the second round.

If auth-order is not defined, only standard password based authentication is done.

Login and Logout Agents

Login Agent

The login agent exit status is ignored and no longer has any effect on the login process. It is called in the first stages of the login after all authentication has been completed.

The first line of output, up to a `\n` is treated as a login cookie by the Partner Agent Server. All remaining lines are sent transparently to the user as a login message.

Logout Agent

The logout agent is called when the user session is terminated. Any output is sent transparently to the user as a logout message.

Incoming and Outgoing Agents

Incoming and outgoing agents are used for some of the following reasons when you are uploading and downloading files from a Server for data transmission:

- To push data back and forth.
- To allow permissions to be granted to connect to a Server.
- To deny permissions to connect to a Server.
- To notify the system administrator or other designated users when files have been uploaded to or downloaded from the Server.

Incoming Agents

Incoming agents occur whenever you perform an upload to the Server.

Incoming Start Agent

This agent is called at the beginning of an upload. Permissions can be given or denied for users to connect to the Server through the Incoming Start Agent.

Incoming End Agent

This agent is called at the end of an upload session. It primarily alerts someone that files have been uploaded to the Server.

Incoming Error Agent

This agent is called when an unexpected interruption occurs during a file upload to the Server. The most common reason for this type of error is usually due to a network problem.

Incoming Abort Agent

This agent is called when you want to perform an intentional interruption of a file transmission. This can be done through [Control-C], break, or some other kill method.

Outgoing Agents

Outgoing agents occur whenever you perform a download from the Server.

Outgoing Start Agent

This agent is called at the beginning of a download. Permissions can be given or denied for users to connect to the server through the Outgoing Start Agent.

Outgoing End Agent

This agent is called at the end of a download session. It primarily alerts someone that files have been downloaded from the Server.

Outgoing Error Agent

This agent is called when an unexpected interruption occurs during a file download from the Server. The most common reason for this type of error is usually due to a network problem.

Outgoing Abort Agent

This agent is called when you want to perform an intentional interruption of a file transmission. This can be done through [Control-C], break, or some other kill method.

FTP and HTTP Command Agents

If a command agent is defined for a particular command, Partner Agent Server does not perform any action for the command, except to invoke the agent and send a response based on the agent's exit status.

Every command that involves filesystem access has an associated agent. A non-zero exit status is treated as a command failure.

File Download	This agent generates data that is sent to the client.
File Upload	This agent handles any incoming data from the client.
Directory List	The LIST agent generates <code>ls -al</code> style listings.
Transfer Restart	The REST agent is used when restarting a previously upload or download transfer.
Modification Time	The MDTM agent displays the last modification time of a remote file.
File Size	The SIZE agent reports the size of the specified file. Only the first line of output up to a <code>\n</code> is sent to the client as the size. All other output is discarded.
MD5 Checksum	The RTCK agent is used to compute the digest of a file.
FTP Command Agent - CWD	The CWD agent is used to change the current working directory.
FTP Command Agent - DELE	The DELE agent is used to delete a file. It is subject to the Partner Agent Server delete restrictions.
FTP Command Agent - MKD	The MKD agent is used to make a new directory. It is subject to the Partner Agent Server mkdir restrictions.
FTP Command Agent - NLST	The NLST agent generates <code>ls -l</code> style listings. This is required for clients issuing the <code>mget</code> and <code>mdelete</code> commands.
FTP Command Agent - PWD	The PWD agent reports the current working directory. Only the first line of output up to a <code>\n</code> is sent to the client as the pwd. All other output is discarded.
FTP Command Agent - RMD	The RMD agent is used to remove a directory. It is subject to the Partner Agent Server rmdir restrictions.
FTP Command Agent - RNFR	The RNFR agent is used to examine the existence of the destination filename right after a rename command is issued.

FTP Command Agent - RNTO	The RNTO agent is used to rename a file to a new name.
FTP Command Agent - SITE	The SITE agent is used to send custom SITE commands to the FTP server.
FTP Command Agent - CHMOD	The CHMOD agent changes the modes and permissions of a file in place of the system chmod.
FTP Command Agent - MIRR	The MIRR agent gets a list of mirror locations for mirroring data in the form of a URL, including the pathname in the URL, hostname, and port of each mirror Server.

Appendices

Appendix A, “(Optional) Installing a Stand-alone FileDrive Server”

Appendix B, “(Optional) Using the Partner Agent Server Command Line Client”

(Optional) Installing a Stand-alone FileDrive Server

This chapter describes the stand-alone FileDrive Server, which optionally can be used to exchange files with the Partner Agent Server, and consequently with ECXpert, through a firewall.

This chapter explains how to optionally install a stand-alone FileDrive Server, how to configure FileDrive Server to transfer files to and from Partner Agent Server through a firewall, and how to uninstall FileDrive Server. It also provides answers to frequently asked questions about FileDrive Server.

The following topics are discussed in this section:

- FileDrive Server
- Hardware Requirements for a Stand-alone Instance of FileDrive Server
- Server Distribution
- Installing a Stand-alone FileDrive Server
- Uninstalling a Stand-alone Instance of FileDrive Server
- FileDrive Server FAQs

FileDrive Server

The Partner Agent Server is installed directly on the ECXpert machine, so file transfers between the two servers do not go through a firewall. If you want to be able to transfer files to ECXpert from an FTP or HTTP(S) server in a DMZ outside of your firewall, you can install a separate FileDrive Server, in addition to Partner Agent Server. You can then use the FileDrive Server to transfer files from outside the firewall to Partner Agent Server, which can then transfer the files to and from ECXpert.

Hardware Requirements for a Stand-alone Instance of FileDrive Server

- Approximately 12 MB of disk space to hold the installed FileDrive Server directory.
- Approximately 12 MB of temporary disk space to hold the FileDrive Server tar file, the extracted distribution, and the installer. These can be backed up and deleted once FileDrive Server is installed.
- 64 MB of memory and 128 MB of swap space for the operating system and Server are recommended.
- In addition, FileDrive Server produces logfiles, security audits, and configuration version histories that are stored in the FileDrive Server directory hierarchy. The size and growth rate of these files are highly dependent on server activity. Expect a lightly used Server to use up a minimum of 2 MB of additional disk space during several months of operation.

NOTE These minimums do not take into account other applications that may be running simultaneously with FileDrive Server on the same machine.

Server Distribution

The FileDrive Server is distributed with the ECXpert 3.0 Service Pack 1 for Solaris. To download and decompress the server installation script, even if you will be installing the FileDrive Server separate from ECXpert, follow these steps.

1. Log on as root to the machine on which you will install FileDrive Server.
2. Download the Service Pack 1 installation file.
 - a. Display the ProductTracker by SubscribNet web page.
The URL is `http://subscribnet.netscape.com/`.
 - b. Enter your Subscribnet user ID and password.
The main Subscribnet page is displayed.
 - c. Click the link in “Click here to access your software.”
An index of the Netscape and iPlanet software registered for your user ID is displayed.
 - d. Click the “Netscape ECXpert” link.
A page is displayed that asks you to select the version and platform.
 - e. Locate the link for the FileDrive 2.1 Server, either Domestic (for customers in the U.S. or Canada) or Export (for customers in all other countries).
 - f. Click the download link.
Download the ECXpert 3.0 Service Pack 1 installation file into the directory in which you will install FileDrive Server.

3. Unzip the downloaded file.

Use a PKZip-compatible decompression utility that supports encryption, or download the Info-ZIP WiZTM utility available free from Subscribnet.

The downloaded file will be unzipped into the following files:

```
m dist-Solaris.tar
m license110299sdk.txt
m Install
m README.Install
m README.Certificates
```

- m relnotes.html
- m Uninstall
- m WHATS-NEW-2.1

4. Install FileDrive Server using the Install script.

See “Installing a Stand-alone FileDrive Server,” on page 178.

Obtaining a License File

FileDrive Server does not work until a license is installed. During installation, you are asked for the fully qualified path to a license file, which you should have prior to running the install script. If you do not have a license, you can run the install script and then add the license later (“Installing a License File After Installation,” on page 187).

Installing a Stand-alone FileDrive Server

NOTE These instructions are only for installing FileDrive Server as a stand-alone server, independent of ECXpert.

To install *Partner Agent Server*, which interacts with ECXpert, on the ECXpert machine, follow the installation instructions in the ECXpert Service Pack 1 Release Note.

To install the FileDrive Server as a stand-alone server, perform the following steps.

1. Log in as root.

All files and directories in a stand-alone instance of FileDrive Server must be owned by root.

2. Change to the directory in which you unzipped the downloaded installation package.

3. Run the installation script.

At the prompt, enter the following command:

```
# ./Install
```

4. Review the evaluation agreement.

An evaluation agreement displays. Use the Space key to page through the agreement. At the end of the agreement, the installer prompts:

Do you agree to the above terms? [y/n]

m To continue with the installation, type Y and press Enter.

OR

m Type N and press Enter, to cancel the installation.

5. Choose the directory in which to install the FileDrive Server.

The FileDrive Server installer creates a directory hierarchy that contains all the FileDrive Server binaries, configuration files, and support files. The location of the FileDrive Server directory is referred to as *\$FILEDRIVEHOME* in this document.

To enter a location for the FileDrive Server root directory:

m To use the default location, press Enter.

OR

m Enter a complete path name.

m Press Enter.

If the directory you have chosen does not exist, the installer asks if you want it to create the directory for you.

m To create the directory, press Enter.

m If you type N, for no, the installer asks:

Do you want to continue with the installation? [y]

m To continue, press Enter.

m Press Enter to have the installer create the directory.

The installer extracts the distribution. All files are owned by the root user, and have group bin. The following message displays:

Extracting the distribution into *\$FILEDRIVEHOME*.

The installer configures the FileDrive Server installation. The configuration files are automatically edited to reflect the location that you have chosen for the root of the directory hierarchy. The Installer creates two environment files that reflect your choice of FileDrive Server root directory. You may reference these files in your `.profile` or `.cshrc` file to set a `$FILEDRIVEHOME` environment variable at login time. The following messages display:

```
Configuring FileDrive installation
```

```
Creating /etc/fd/env.sh
```

```
Creating /etc/fd/env.csh
```

In the next four steps, the installer prompts you for a series of ports on which to run the admin and HTTP and HTTPS Servers. You are prompted for secure and non-secure ports for each Server. After you enter each port, or accept the defaults, the installer configures the required UNIX system files to properly support FileDrive Server.

6. Enter a port for the secure administration Server.

The installer asks:

```
What port would you like to run the admin server run on? [444]
```

```
m Press Enter to select the default port 444.
```

OR

```
m Enter a port.
```

```
m Press Enter.
```

7. Enter a port for the non-secure administration Server.

The installer asks:

```
What port would you like to run the non-secure admin run on? [8081]
```

```
m Press Enter to accept the default value of 8081.
```

OR

```
m Enter a port.
```

```
m Press Enter
```

8. Enter a port for the HTTP Server..

NOTE The default port for HTTPS is 443. If an existing web service is using this port, select an alternate port or disable the other service that runs on this port.

The installer asks:

What port would you like to run the httpd server run on? [443]

m Press Enter to accept the default value of 443.

OR

m Enter a port.

m Press Enter.

9. Enter a port for the non-secure HTTP Server..

NOTE The default port for HTTP is 80. If an existing web service is using this port, select an alternate port or disable the other service that runs on this port.

The installer asks:

What port would you like to run the non-secure httpd server on? [80]

m Press Enter to accept the default value of 80.

OR

m Enter a port.

m Press Enter.

A startup file is created, `/etc/rc.filedrive`.

10. Set startup option.

The installer asks:

Would you like FileDrive to load at system start? [y]

m Press Enter, to select the default yes.

A script is added that starts FileDrive Server when the system boots.

OR

m Type N, for No.

m Press Enter.

The installer checks if an anonymous FTP account exists. If it does not exist, a message displays recommending that you create an anonymous FTP account.

11. Set up nightly cron job.

The installer asks:

Would you like to install nightly log rotation? [y]

m To create a crontab entry that handles the daily log rotation and generates the daily transfer statistics, press Enter.

A crontab entry that drives the nightly log rotation and automatic statistics generation program is installed.

OR

m Type N, for No.

m Press Enter.

12. Select Server mode of operation.

FileDrive Server can run in standalone mode or as an inetd entry, listening on port 21.

NOTE We recommend using stand-alone mode in general, because it is more flexible and provides significant performance improvements over inetd-based services.

To run as an inetd entry:

m At the prompt, type N.

m Press Enter.

OR

To run in standalone mode:

m Press Enter at the prompt, to select Yes.

In standalone mode, select the port. The installer asks:

What port would you like to run the ftp server on? [21]

m To run on the default port 21, press Enter.

OR

m Enter a new port.

m Then press Enter.

The installer updates the `/etc/inetd.conf` file to reflect your choices.

13. Select a port for the ActiveAgents Server. The installer asks:

What port would you like to run the ActiveAgents server on? [4455]

m Press Enter to accept the default value of 4455.

OR

m Enter a port.

m Press Enter.

In the next part of the installation, you generate three certificates for use by the three Servers; the FileDrive Server `ftpd`, the `Agentd`, and the Admin System. Each certificate has to be generated and then signed with a CA Signing Certificate.

14. If a CA Signing Certificate does not exist, you must generate one to sign the three Server certificates. A PEM pass phrase (password) is required to encrypt the CA Signing Certificate's private key. This is a password to authorize your electronic signature on the other certificates.

m At the prompt, enter a PEM pass phrase. The pass phrase must be at least four characters long.

m Enter the PEM pass phrase again to verify it.

m At the series of following prompts, enter information about yourself in order for the certificate to be created.

After you respond to the prompts, the signing certificate is generated.

When you generate the next three certificates, you have the option to store the Server's private key encrypted. If you select this option, unattended Server startup is not possible at system boot. Instead, the PEM pass phrase will need to be entered at a console each time the Servers are started.

NOTE If you are evaluating FileDrive Server, it is recommended that you do not encrypt the private key.

15. Generate a certificate for the ActiveAgents Server.

m At the following series of prompts, enter information about yourself that is incorporated into the certificate request.

m The installer asks:

Is the above information correct? [y]

m If the information is not correct, type N.

m Re-enter the correct information at the prompts.

OR

m Press Enter, for yes.

m The installer asks:

Encrypt Private Key? [n]

m Press Enter, to select No.

OR

m To encrypt the Server's private key, type Y.

m Press Enter.

The installer generates the private key.

m Enter the PEM pass phrase from your CA Signing Certificate to sign the ActiveAgents Server certificate.

The certificate is saved.

16. Generate a certificate for the FileDrive Server.

At the following series of prompts, enter information about yourself that is incorporated into the certificate request. The information you entered for the previous certificate becomes the default values for this certificate.

m At the prompts, press Enter to accept the defaults.

OR

m Enter the desired information.

- m The installer asks:
- Is the above information correct? [y]
- m If the information is not correct, type N.
- m Re-enter the correct information at the prompts.

OR

- m Press Enter, for yes.
- m The installer asks:
- Encrypt Private Key? [n]
- m Press Enter, (to select No).

OR

- m To encrypt the Server's private key, type Y.
- m Press Enter.
- The installer generates the private key.
- m Enter the PEM pass phrase from your CA Signing Certificate to sign the certificate.

The certificate is saved.

17. Generate a certificate for the FileDrive Administration Server.

At the following series of prompts, enter information about yourself that is incorporated into the certificate request. The information you entered for the previous certificate becomes the default values for this certificate.

- m At the prompts, press Enter to accept the defaults.

OR

- m Enter the desired information.
- m The installer asks:

Is the above information correct? [y]

- m If the information is not correct, type N.
- m Re-enter the correct information at the prompts.

OR

- m Press Enter, for yes.

- m The installer asks:

Encrypt Private Key? [n]

- m Press Enter, to select No.

OR

- m To encrypt the Server's private key, type Y.

- m Press Enter.

The installer generates the private key.

- m Enter the PEM pass phrase from your CA Signing Certificate to sign the FileDrive Administration Server certificate.

The certificate is saved.

18. Enter the FileDrive Server administrator password. The administrator password is required to access the administration system.

- m Enter an administrator account name at the account name prompt and press Enter.

- m Enter a password at the New password prompt and press Enter.

- m Re-enter new password and press Enter.

NOTE If you want to change or add a new admin password after the installation, run *\$FILEDRIVEHOME/bin/addpasswd*.

19. Install your FileDrive Server license.

- m To install the FileDrive Server License, at the Install Now prompt, press Enter.

- m Enter the pathname for the license text file and press Enter, at the prompt:

Where is the FileDrive license located? (enter the pathname)

The license is installed. Your system's Server starts, allowing new connections to your FileDrive Server and the administration system starts.

The following message appears:

Congratulations, you are now running FileDrive.

Installing a License File After Installation

You can install FileDrive Server without a license file, but if you try to run it without a license, you will get the error message “530 Service not available.”

To install a license after you have installed FileDrive Server:

1. Run the license installation utility.

Enter the following command:

```
$FILEDRIVEHOME/bin/install.license
```

where *\$FILEDRIVEHOME* is the directory in which FileDrive Server is installed.

2. At the prompt, enter the pathname for the license text file.

The license is added.

3. Stop the FileDrive FTP and HTTP servers.

Enter the following commands:

```
$FILEDRIVEHOME/bin/stop_ftpd
```

```
$FILEDRIVEHOME/bin/stop_httpd
```

where *\$FILEDRIVEHOME* is the directory in which FileDrive Server is installed.

The Servers shut down.

4. Restart the FileDrive FTP and HTTP servers.

Enter the following commands:

```
$FILEDRIVEHOME/bin/start_ftpd
```

```
$FILEDRIVEHOME/bin/start_httpd
```

where *\$FILEDRIVEHOME* is the directory in which FileDrive Server is installed.

The Servers restart and read the license.

Uninstalling a Stand-alone Instance of FileDrive Server

NOTE These instructions are only for uninstalling a stand-alone instance of FileDrive Server.

To uninstall a stand-alone instance of FileDrive Server, perform the following steps.

1. Back up key components of the current installation in case there is a problem with the new installation. In particular, you want to preserve the `conf` directory, as well as the contents of `bin/agents`. Also, if logging is important, back up the `var/logs` directory as well.
2. Create a separate directory to store these files.

Use the following commands:

```
# cd $FILEDRIVEHOME/  
  
# mkdir fd_sav  
  
# tar cvf ./fd_conf.tar conf bin/agents var/logs
```

where `$FILEDRIVEHOME` is the directory in which FileDrive Server is installed.

3. Remove the existing instance using the `Uninstall` script.

```
$FILEDRIVEHOME/bin/Utils/Uninstall
```

NOTE The `Uninstall` program physically removes the directory. If you are removing FileDrive Server manually and have stopped FileDrive Server, you can remove the existing installation.

Again, it is recommended that you back up key installation files listed in Step 1.

4. If you reinstall FileDrive Server, you can copy `bin/agents` back in, but you have to manually reconfigure the Server. Do not copy the `conf` directory back into the FileDrive Server directory.

FileDrive Server FAQs

This section includes some frequently asked questions about FileDrive Server and their answers.

Q: *When I connect to my FileDrive Server host, I get the message "530 Service Not Available." What does this mean?*

A: This almost always indicates an expired or corrupted FileDrive Server license file.

To see if your license has expired:

1. Go to the FileDrive Server installation directory. (By default, this is `$FILEDRIVEHOME`.)

Look in the `conf` directory for the file `filedrive.license`.

There is a token called Valid To:. If the year is 0, then this license is set to never expire. If the Valid To: date is before the current date, then your license has expired.

To replace the license contact ECXpert Technical Support.

- In the United States, call Expert Alliance at 800-560-5749.
- OR
- Outside of the United States, call Technical Support International at 650-937-6688.

When you have a new license, run the `install.license` script in the `$FILEDRIVEHOME/bin` directory.

Q: *How do I perform a chroot for FileDrive Server users?*

A: FileDrive Server automatically performs a chroot operation on Virtual and anonymous users.

There are three different types of users known to FileDrive Server; *real*, *virtual*, and *anonymous*.

- Real—Real UNIX accounts. The account need not be a functioning shell account, but it must be in the `/etc/passwd` directory.
- Virtual—This is the FileDrive Server-specific user. FileDrive Server maintains its own copy of a password file for FileDrive Server-specific authentication. Upon authentication, a chroot operation is performed on the resultant shell.
- Anonymous— A long standing FTP concept where no password is required to gain entry to the machine through an FTP shell. Again, FileDrive Server automatically performs a chroot on the resultant shell.

This means that virtual and anonymous users in FileDrive Server can only descend their part of the file system tree. They are not allowed to go above their section of the file system.

Q: *With other implementations of FTP, the chroot requires that the anonymous users have their version of system commands. Often system directories including an / etc/ and / bin are included in their part of the chroot filesystem. Why don't virtual users require this?*

A: All FTP commands trigger events. FileDrive Server supplies its own implementation of every FTP command that can be entered. The reason is so FileDrive Server can map these to events and trigger user defined ActiveAgents. Because FileDrive Server has already implemented these command internally, system commands such as cd and other Operating System commands are not used.

Q: *How are environment variables set and passed to an ActiveAgent? I'm concerned about current file transfers from different users that will trigger multiple executions of ActiveAgents. Specifically I wonder if there is a possibility of having incorrect environment variables passed to any of the ActiveAgents. Do environment variables get generated as part of the child process and therefore are not visible to other child processes?*

A: As with many interesting questions, there is a long answer and a short one.

Short Answer: Environment variables are guaranteed to be available only to the agent specifically invoked by FileDrive Server.

Long Answer: The environment variables are generated by the FileDrive Server which is handling the request for a given session. The variables are passed to the agentd which then uses them to set up the environment for the process that will execute the agent. These variables do not actually exist as environment variables until agentd executes the agent process. There is no possibility of any environment variable getting inherited or passed to any other agent processes since once an agent is done executing, its process dies and all traces of the variables go away. In addition, the environment variables for a given session are regenerated each time an agent is executed, so there is also no way for agents to share environment variables even if this is desirable. Furthermore, the FileDrive Server to agentd connection is SSL encrypted, so the possibility of obtaining the values of these variables prior to agent execution is extremely unlikely.

(Optional) Using the Partner Agent Server Command Line Client

Partner Agent Server Command Line Client optionally can be used to test that Partner Agent Server is transferring files properly to ECXpert or to another machine. Typically, Partner Agent Windows Client is used for transferring files to ECXpert or another machine.

This appendix describes how to start the Partner Agent Server Command Line Client, the options and commands available, and how to transfer files non-interactively via a shell script.

The following topics are discussed in this section:

- The Partner Agent Server Command Line Client
- Starting Partner Agent Server Command Line Client Interactively
- Transferring Files
- Command Line Options
- Interactive Commands
- Tracking File Transfers in ECXpert

The Partner Agent Server Command Line Client

The Partner Agent Server Command Line Client can securely transfer files to ECXpert or to another machine using the FTP protocol, as the Windows Client does, in addition to the HTTP, and HTTPS protocols. It can be used interactively, or it can be called as part of a program or script.

Partner Agent Server Command Line Client is installed as part of the Partner Agent Server installation process. It is located, by default, in the `SNSBASE/NS-apps/paserver/bin/` directory, where `SNSBASE/NS-apps/paserver` is the base directory that houses all of the components of Partner Agent Server.

Starting Partner Agent Server Command Line Client Interactively

To start the Command Line Client and immediately establish a connection to another machine, follow these steps:

1. Set environment variables for your certificate and private key.

The Partner Agent Servers are pre-configured to expect a certificate-based login. In order to send the correct certificate and private key to the Server, set variables in the shell environment of the `fdx` utility by entering the following commands.

For the C shell:

```
setenv SSL_PKEY_FILE <User ID>-key.pem
```

```
setenv SSL_PKEY_FILE <User ID>-cert.pem
```

where `<User ID>-key.pem` is the full pathname of the private key and `<User ID>-cert.pem` is the full pathname of the certificate.

For the Bourne and Korn shells:

```
export SSL_PKEY_FILE=<User ID>-key.pem
```

```
export SSL_X509_FILE=<User ID>-cert.pem
```

where `<User ID>-key.pem` is the full pathname of the private key and `<User ID>-cert.pem` is the full pathname of the certificate.

2. Start the command interpreter, specifying a host to connect to automatically.

Enter the following command:

```
$NSBASE/NS-apps/paserver/bin/fdx <scheme>://<hostname>:[<port>]
[-<options>]
```

where the *<scheme>* is FTP, HTTP, or HTTPS; the *<hostname>* is the name of the host; *<port>* is the port on which the Server is listening; and *<options>* are any command line options you want to specify at start-up. See “Command Line Options,” on page 210 for a list of all available options.

Command Line Client immediately attempts to establish a connection between Partner Agent Server and the remote server, and requests a secure certificate-authenticated session.

NOTE Alternately, you can start the command interpreter without immediately connecting to another machine by entering the command

```
$NSBASE/NS-apps/paserver/bin/fdx
```

Partner Agent Server enters its command interpreter and awaits instructions from the user. The prompt `fdx>` appears, at which you can enter interactive commands.

To connect to a host from the `fdx>` prompt, use the `open` command. For information on using the `open` command with FTP, see page 216; for information on using the `open` command with HTTP or HTTPS, see page 220.

3. Once you are connected to the remote host, enter the PEM pass phrase associated with the certificate and the ECXpert member password.

When Partner Agent Server makes a connection to a remote server, the certificate is transmitted to that server. After the PEM pass phrase is authenticated, the correct member name is extracted from the certificate and you will be prompted for the ECXpert member password. Once the username and password are authenticated against the ECXpert member database, you can perform any of the commands listed in “Interactive Commands,” on page 212.

Changing Transfer Protocol Schemes

Once you connect with the FTP scheme, you can switch to HTTP or HTTPS with the `open` command.

When you connect with the HTTP or HTTPS schemes, to change to FTP you must terminate the session and re-start the client.

Operating in Tunnel Mode

When transferring a file using the FTP scheme, you can operate in tunnel mode. In tunnel mode, the SSL session is established on a data connection rather than on the control connection. This is done because some firewalls terminate a connection when ciphered data is sent over the control connection. You must specify tunnel mode before a connection to the server is made.

To use tunnel mode, before a connection to the server is made:

- Specify the `-m tun` option on the command line.
- OR
- At the `fdx>` prompt, use the command `sslmode tun`.

Environment Variables

Partner Agent Server Command Line Client utilizes the following environment variables:

Table B-1 Command Line Client environment variables

COLUMNS	Correctly formats help display.
PAGER	Used for the built-in <code>more</code> command.
SHELL	Used for the default shell.
FTP_ANON_USER	The name to use when logging in anonymously.
FTP_ANON_PASS	The password to use when logging in anonymously.
FDX_PROGRESS	Turns on the progress meter.

Aborting a File Transfer

To abort a file transfer, use the terminal interrupt key (usually Ctrl-C). Transfers that are sending at that time are immediately halted. Sending an FTP protocol ABOR command to the remote server halts receiving transfers, discarding any further data received. The speed at which this occurs depends upon the remote server's support for ABORT processing. If the remote server does not support the ABOR command, the `fdx>` prompt does not appear until the remote server has completed transmitting the requested file.

The terminal interrupt key sequence is ignored when Partner Agent Server has completed any local processing and is awaiting a reply from the remote server. A long delay in this mode can result from the ABOR processing described above or from unexpected behavior by the remote server, including violations of the FTP protocol. If the delay results from unexpected remote server behavior, the local Partner Agent Server program must be killed by hand.

Transferring Files

You can transfer files non-interactively using shell scripts, from the UNIX command line, or interactively at the `fdx>` prompt.

The following sections describe how to perform common types of file transfers and activities.

Uploading or Downloading Files Using Shell Scripts

The client can be used non-interactively in shell scripts. When a file transfer is called as part of a script, use the following format:

```
$NSBASE/NS-apps/paserver/bin/fdx [<options>] [<URL>]
```

where *<options>* includes any of the options outlined in “Command Line Options,” on page 210 and *<URL>* is an HTTP, HTTPS, or FTP address, including the full upload pathname of the file to be transferred. If the port is not specified in the URL, the default port is used (21 for FTP, 80 for HTTP, and 443 for HTTPS).

Uploading Files from the Command Line

- Enter the following command from the UNIX command line:

```
$NSBASE/NS-apps/paserver/bin/fdx [<options>] -u [<local filename>] <URL>
```

where *<options>* includes any of the options outlined in “Command Line Options,” on page 210; *<local filename>* is the full pathname of the local file to be uploaded; and *<URL>* is an HTTP, HTTPS, or FTP address, including the full upload pathname of the file to be transferred. If the port is not specified in the URL, the default port is used (21 for FTP, 80 for HTTP, and 443 for HTTPS).

NOTE The URL can include your username and password, in the form *<scheme>://<user>:<pass>@<host.domain.com>/<file_path_and_name>*

Otherwise, you will be prompted for a username and password when you make the connection to the remote server.

Figure B-1 shows an example FTP session in which user *actraadm*, with password *actraadm*, uploads the file *20000208.html* to the */u/bus_docs/850/* directory on *siroe.com*'s FTP site.

Figure B-1 Example FTP upload session from the UNIX command line

```
$ fdx -u ../850/20000208.html
ftp://actraadm:actraadm@siroe.com/u/bus_docs/850/20000208.html
Trying 205.211.46.86:35 ... Connected to siroe.com.
220 Siroe Corporation FTP server (SunOS 5.6) ready.
[SSL Not Available]
331 Password required for actraadm.
230 User actraadm logged in.
200 PORT command successful.
150 Binary data connection for u/bus_docs/850/20000208.html
(207.142.43.215,64319).
226 Transfer complete.
8058 bytes sent in 0.00035 seconds (2.2e+04 Kbytes/s)
Upload OK: Local '../850/20000208.html' Remote
'u/bus_docs/850/20000208.html'
221 Goodbye.
$
```

Uploading Files Interactively

- Enter the following command from the `fdx>` prompt:

```
put <local filename> <remote filename>
```

NOTE `fdx` and other FTP command-line clients do not support ECXpert batch submission, i.e., `mput` behavior.

The Partner Agent Windows Client, however, does support `mput` behavior by decomposing batch file transfers into individual transfers, transparently to the user.

Figure B-2 shows an example FTP session in which user *actraadm* uploads the file `20000208.html` to the `/u/bus_docs/850/` directory on *siroe.com*'s FTP site.

Figure B-2 Sample FTP upload (`put`) session from the `fdx>` prompt

```
$ fdx
fdx> open siroe.com
Trying 205.211.46.86:35 ... Connected to siroe.com.
220 Siroe Corporation FTP server (SunOS 5.6) ready.
[SSL Not Available]
Name (siroe:actraadm): actraadm
331 Password required for actraadm.
Password:
230 User actraadm logged in.
fdx> put ../850/20000208.html /u/bus_docs/850/20000208.html
200 PORT command successful.
150 Binary data connection for /u/bus_docs/850/20000208.html
(207.142.43.215,64319).
226 Transfer complete.
8058 bytes sent in 0.01 seconds (7.8e+02 Kbytes/s)
fdx>
```

Uploading Files to ECXpert from the Command Line

- Enter the following command from the UNIX command line:

```
$NSBASE/NS-apps/paserver/bin/fdx [<options>] -u [<local filename>]  
<URL>@<unique ID>@<sender>@<sender password>@<receiver>@<document  
type>@
```

where *<options>* includes any of the options outlined in “Command Line Options,” on page 210; *<local filename>* is the full pathname of the local file to be uploaded; *<URL>* is an HTTP, HTTPS, or FTP address, including the full upload pathname of the file to be transferred; *<unique ID>* is any unique alphanumeric identifier, used to prevent existing files from being overwritten and stripped out by ECXpert; *<sender>* is the ECXpert Member ID of the sender; *<sender password>* is the ECXpert Member password of the sender; *<receiver>* is the ECXpert Member ID of the receiver; and *<document type>* is the document type specified in the trading partnership.

If the port is not specified in the URL, the default port is used (21 for FTP, 80 for HTTP, and 443 for HTTPS).

NOTE The URL can include your username and password, in the form
<scheme>://*<user>*:*<pass>*@*<host.domain.com>*/*<file_path_and_name*
>

Otherwise, you will be prompted for a username and password when you make the connection to the remote server.

Figure B-3 shows an example FTP session in which ECXpert member *john* uploads a file, *ecx.ini*, to ECXpert member *jane*, using the document type of *pas_test* and the outbound protocol *poll* specified in the trading partnership. The ECXpert submission parameters supplied to send the file include *<sender>*, *<sender password>*, *<receiver>*, and *<document type>*. Note that the ECXpert tracking ID is displayed to the client in both human-readable and tag-based (programmatically-readable) forms.

Figure B-3 Sample FTP upload to ECXpert from the UNIX command line

```
$ pwd /actraadm/NS-apps/ECXpert/config
$ export SSL_PKEY_FILE=/actraadm/NS-apps/ECXpert/config/john-key.pem
$ export SSL_X509_FILE=/actraadm/NS-apps/ECXpert/config/john-crt.pem
$ fdx -u ecx.ini
ftp://actraadm:actraadm@siroe.com/CompanyA/1@john@john@jane@pas_test
Trying 208.12.34.124:1027 ... Connected to remoteserver.
220 remoteserver FTP server (Partner Agent 1.0) ready.
Enter PEM pass phrase:
[SSLv3 Cipher DES-CBC3-SHA]
331 Password required for john.
230-User john authenticated by ECXpert.
230-Welcome to ECXpert
230 Virtual user john logged in.
200 PORT command successful.
150 Opening BINARY mode SSL data connection for 1@john@john@jane@pas_test@.
226 Transfer Complete: Submitted to ECXpert successfully with tracking ID
5.<SR><TI>5</TI><RC>0</RC><EM>Submitted to ECXpert successfully with tracking
ID 5</EM></SR>
69099 bytes sent in 0.16 seconds (4.2e+02 Kbytes/s)
fdx> quit
221-Logged out from ECXpert
221-
221 Goodbye.
$
```

Uploading Files to ECXpert Interactively

- Enter the following command from the `fdx>` prompt if you are already connected to the ECXpert server:

```
put <local filename> <remote filename>@<unique ID>@<sender>@<sender password>@
<receiver>@<document type>@
```

NOTE fdx and other FTP command-line clients do not support ECXpert batch submission, i.e., `mput` behavior.

The Partner Agent Windows Client, however, does support `mput` behavior by decomposing batch file transfers into individual transfers, transparently to the user.

Figure B-4 shows an example FTP session in which ECXpert member *john* uploads (using `put`) a file, `ecx.ini`, to ECXpert member *jane*, using the document type of `pas_test` and the outbound protocol `poll` specified in the trading partnership. The ECXpert submission parameters supplied to send the file include `<sender>`, `<sender password>`, `<receiver>`, and `<document type>`. Note that the ECXpert tracking ID is displayed to the client in both human-readable and tag-based (programmatically-readable) forms.

Figure B-4 Sample FTP upload (`put`) to ECXpert from the `fdx>` prompt

```
$ pwd /actraadm/NS-apps/ECXpert/config
$ export SSL_PKEY_FILE=/actraadm/NS-apps/ECXpert/config/john-key.pem
$ export SSL_X509_FILE=/actraadm/NS-apps/ECXpert/config/john-crt.pem
$ /actraadm/NS-apps/paserver/bin/fdx ftp://remoteserver:1027
Trying 208.12.34.124:1027 ... Connected to remoteserver.
220 remoteserver FTP server (Partner Agent 1.0) ready.
Enter PEM pass phrase:
[SSLv3 Cipher DES-CBC3-SHA]
331 Password required for john.
Password:
230-User john authenticated by ECXpert.
230-Welcome to ECXpert
230-
230 Virtual user john logged in.
fdx> put ecx.ini l@john@john@jane@pas_test@
200 PORT command successful.
150 Opening BINARY mode SSL data connection for l@john@john@jane@pas_test@.
226 Transfer Complete: Submitted to ECXpert successfully with tracking ID
6.<SR><TI>6</TI><RC>0</RC><EM>Submitted to ECXpert successfully with tracking
ID 6</EM></SR>
69099 bytes sent in 0.16 seconds (4.2e+02 Kbytes/s)
fdx> quit
221-Logged out from ECXpert
221-
221 Goodbye.
$
```


Downloading Files from the Command Line

- Enter the following command from the UNIX command line:

```
SNSBASE/NS-apps/paserver/bin/fdx [<options>] -d <URL> [<local filename>]
```

where *<options>* includes any of the options outlined in “Command Line Options,” on page 210; *<URL>* is an HTTP, HTTPS, or FTP address, including the full upload pathname of the file to be transferred; and *<local filename>* is the full download path of the file to be transferred. If the port is not specified in the URL, the default port is used (21 for FTP, 80 for HTTP, and 443 for HTTPS).

For example:

```
fdx -d ftp://user:pass@host.domain.com/<remote filename> [<local filename>]
```

NOTE The URL can include your username and password, in the form *<scheme>://<user>:<pass>@<host.domain.com>/<file_path_and_name>*

Otherwise, you will be prompted for a username and password when you make the connection to the remote server.

Figure B-5 shows an example FTP session in which user *actraadm*, with password *actraadm*, downloads the file *20000208.html* from the */u/bus_docs/850/* directory on *siroe.com*'s FTP site and places it in the *../850/* local directory.

Figure B-5 Sample FTP upload from the UNIX command line prompt

```
$ fdx -d
ftp://actraadm:actraadm@siroe.com/u/bus_docs/850/20000208.html
../850/20000208.html
Trying 205.211.46.86:35 ... Connected to siroe.com.
220 Siroe Corporation FTP server (SunOS 5.6) ready.
[SSL Not Available]
331 Password required for actraadm.
230 User actraadm logged in.
200 PORT command successful.
150 Binary data connection for u/bus_docs/850/20000208.html
(207.142.43.215,64319).
226 Transfer complete.
8058 bytes sent in 0.00035 seconds (2.2e+04 Kbytes/s)
```

Figure B-5 Sample FTP upload from the UNIX command line prompt (*Continued*)

```
Upload OK: Local './850/20000208.html' Remote
'u/bus_docs/850/20000208.html'
221 Goodbye.
$
```

Downloading Files Interactively

- Enter the following command from the `fdx>` prompt:

```
get <remote filename> <local filename>
```

NOTE `fdx` and other FTP command-line clients do not support ECXpert batch retrieval, i.e., `mget` behavior.

The Partner Agent Windows Client, however, does support `mget` behavior by decomposing batch file transfers into individual transfers, transparently to the user.

Figure B-6 shows an example FTP session in which user *actraadm* downloads the file `20000208.html` from the `/u/bus_docs/850/` directory on *siroe.com*'s FTP site and places it in the `../850/` local directory.

Figure B-6 Sample FTP upload (`get`) from the `fdx>` prompt

```
$ fdx
fdx> open siroe.com
Trying 205.211.46.86:35 ... Connected to siroe.com.
220 Siroe Corporation FTP server (SunOS 5.6) ready.
[SSL Not Available]
Name (siroe:actraadm): actraadm
331 Password required for actraadm.
Password:
230 User actraadm logged in.
fdx> get /u/bus_docs/850/20000208.html ../850/20000208.html
200 PORT command successful.
150 Binary data connection for /u/bus_docs/850/20000208.html
(207.142.43.215,64319).
226 Transfer complete.
8058 bytes sent in 0.01 seconds (7.8e+02 Kbytes/s)
fdx>
```

Downloading Files to ECXpert from the Command Line

- Enter the following command from the UNIX command line:

```
SNSBASE/NS-apps/paserver/bin/fdx [<options>] -d <URL>@<unique ID>@<receiver>@<sender>@<document type>@ [<local filename>]
```

where *<options>* includes any of the options outlined in “Command Line Options,” on page 210; *<URL>* is an HTTP, HTTPS, or FTP address, including the full upload pathname of the file to be transferred; *<unique ID>* is any unique alphanumeric identifier, used to prevent existing files from being overwritten and stripped out by ECXpert; *<receiver>* is the ECXpert Member ID of the receiver, *<sender>* is the ECXpert Member ID of the sender, *<document type>* is the document type specified in the trading partnership; *<local filename>* is the full pathname of the local file to be uploaded.

If the port is not specified in the URL, the default port is used (21 for FTP, 80 for HTTP, and 443 for HTTPS)..

NOTE The URL can include your username and password, in the form *<scheme>://<user>:<pass>@<host.domain.com>/<file_path_and_name>*

Otherwise, you will be prompted for a username and password when you make the connection to the remote server.

Figure B-7 shows an example FTP session in which ECXpert member *john* polls files from ECXpert sent by another member, *jane*. The ECXpert submission parameters supplied to retrieve the file include *<receiver>*, *<sender>*, and *<document type>*. Note that the ECXpert tracking ID is displayed to the client in both human-readable and tag-based (programmatically-readable) forms.

Figure B-7 Sample FTP session download from ECXpert from the UNIX command line

```

$ pwd /actraadm/NS-apps/ECXpert/config
$ export SSL_PKEY_FILE=/actraadm/NS-apps/ECXpert/config/john-key.pem
$ export SSL_X509_FILE=/actraadm/NS-apps/ECXpert/config/john-crt.pem
$ fdx -d ftp://actraadm:actraadm@siroe.com/CompanyA/1@john@jane@pas_test
ecx.ini
Trying 208.12.34.124:1027 ... Connected to remoteserver.
220 remoteserver FTP server (Partner Agent 1.0) ready.
Enter PEM pass phrase:
[SSLv3 Cipher DES-CBC3-SHA]
331 Password required for john.
230-User john authenticated by ECXpert.
230-Welcome to ECXpert
230 Virtual user john logged in.
200 PORT command successful.
150 Opening BINARY mode SSL data connection for 1@john@jane@pas_test@. (69099
bytes)
226 Transfer Complete: Retrieved data from ECXpert successfully with tracking
ID 7.<SR><TI>7</TI><RC>0</RC><EM>Retrieved data from ECXpert successfully with
tracking ID 7</EM></SR>
69099 bytes sent in 1.5 seconds (44 Kbytes/s)
fdx> quit
221-Logged out from ECXpert
221-
221 Goodbye.
$

```

Downloading Files to ECXpert Interactively

- Enter the following command from the `fdx>` prompt if you are already connected to the ECXpert server:

```
get <remote filename>@<unique ID>@<receiver>@<sender>@<document type>@ [ <local filename> ]
```

NOTE `fdx` and other FTP command-line clients do not support ECXpert batch retrieval, i.e., `mget` behavior.

The Partner Agent Windows Client, however, does support `mget` behavior by decomposing batch file transfers into individual transfers, transparently to the user.

Figure B-8 shows an example FTP session in which ECXpert member *john* polls (using `get`) files from ECXpert sent by another member, *jane*. The ECXpert submission parameters supplied to retrieve the file include *<receiver>*, *<sender>*, and *<document type>*. Note that the ECXpert tracking ID is displayed to the client in both human-readable and tag-based (programmatically-readable) forms.

Figure B-8 Sample FTP session download (get) from ECXpert from the fdx> prompt

```
$ pwd /actraadm/NS-apps/ECXpert/config
$ export SSL_PKEY_FILE=/actraadm/NS-apps/ECXpert/config/john-key.pem
$ export SSL_X509_FILE=/actraadm/NS-apps/ECXpert/config/john-crt.pem
$ /actraadm/NS-apps/paserver/bin/fdx ftp://remoteserver:1027
Trying 208.12.34.124:1027 ... Connected to remoteserver.
220 remoteserver FTP server (Partner Agent 1.0) ready.
Enter PEM pass phrase:
[SSLv3 Cipher DES-CBC3-SHA]
331 Password required for john.
Password:
230-User john authenticated by ECXpert.
230-Welcome to ECXpert
230-
230 Virtual user john logged in.
fdx> get l@john@jane@pas_test@
200 PORT command successful.
150 Opening BINARY mode SSL data connection for l@john@jane@pas_test@. (69099
bytes)
226 Transfer Complete: Retrieved data from ECXpert successfully with tracking
ID 8.<SR><TI>8</TI><RC>0</RC><EM>Retrieved data from ECXpert successfully with
tracking ID 8</EM></SR>
69099 bytes sent in 1.5 seconds (44 Kbytes/s)
fdx> quit
221-Logged out from ECXpert
221-
221 Goodbye.
$
```

Command Line Options

The command line options that are available depend on the transfer scheme (FTP, HTTP, or HTTPS) in which you are operating.

FTP Command Line Options

The following command line options are available with the FTP scheme:

Table B-2 FTP command line options

Option	Description
-h	Show help.
-d	Download the specified file.
-u	Upload the specified file.
-e	Delete the specified file.
-l	List the contents of the specified directory.
-i	Turns off interactive prompting during multiple file transfers.
-q	Does not print messages to the server during non-interactive mode. Reports only exit status. Primarily a quiet mode.
-p	Enables passive mode for use behind connection filtering firewalls.
-a	Log in anonymously.
-n	Turn off auto-restart.
-r	Restart a command line transfer.
-f	Retry if connection fails, (default is on).
-w <i>N</i>	Wait <i>N</i> seconds between connect attempts, (default is 30).
-g <i>N</i>	Give up after <i>N</i> connect attempts, (default is 3).
-b <i>N</i>	Set bandwidth throttle to <i>N</i> Kb/s.
-x <i>host</i>	Send user name as <i>user@host</i> for use in a proxy environment.
-M a	Set the transfer mode to ascii.
-M b	Set the transfer mode to EBCDIC.
-M i	Set the transfer mode to binary.

Table B-2 FTP command line options *(Continued)*

Option	Description
-s req	Only connect to SSL enabled servers.
-s off	Turn off SSL.
-s opt	SSL is optional (default option).
-m std	Use AUTH SSL negotiation on control channel, (default mode).
-m spe	Use AUTH SPE (SSL payload encryption) on control channel.
-m tun	Negotiate SSL via an sslftp tunnel (SSLv3 only).
-v 2 3	Support only SSL v2 or v3 (default is v23).
-F off	Disable Partner Agent server probe: server is not Partner Agent Server.
-P	Turn on a progress meter for transfers.

HTTP(S) Command Line Options

The command line options available with the HTTP(S) scheme are a subset of those available for FTP. Following are the HTTP(S) options:

Table B-3 HTTP(S) command line options

Option	Description
-q	Does not print messages to the server during non-interactive mode. Reports only exit status. Primarily a quiet mode.
-d	Download the specified file.
-u	Upload the specified file.
-e	Delete the specified file.
-l	List the contents of the specified directory.
-h	Show help.
-i	Turns off interactive prompting during multiple file transfers.
-a	Log in anonymously.
-n	Turn off auto-restart.
-r	Restart a command line transfer.

Table B-3 HTTP(S) command line options *(Continued)*

Option	Description
-f	Retry if connection fails, (default is on).
-w <i>N</i>	Wait <i>N</i> seconds between connect attempts, (default is 30).
-g <i>N</i>	Give up after <i>N</i> connect attempts, (default is 3).
-b <i>N</i>	Set bandwidth throttle to <i>N</i> Kb/s.
-x <i>host</i>	Send user name as user@host for use in a proxy environment.
-v 2 3	Support only SSL v2 or v3, (default is v23).
-F off	Disable Partner Agent server probe: server is not Partner Agent Server.
-P	Turn on a progress meter for transfers.

Interactive Commands

The commands that are available depend on the scheme (FTP, HTTP, or HTTPS) in which you are operating.

File Naming Conventions

Files specified as arguments to Partner Agent Server commands are processed according to the following rules:

- If the file name “-” is specified, the stdin (for reading) or stdout (for writing) is used. If the first character of the file name is “|,” the remainder of the argument is interpreted as a shell command. Partner Agent Server then forks a shell, using `popen(3)` with the argument supplied, and reads (writes) from the stdout (stdin). If the shell command includes spaces, the argument must be quoted, for example:

```
get README "|wc -l"
```

OR

```
put "|ls -al" listing
```

- Failing the above checks, local file names are expanded according to the rules used by `csh(1)`. If the command expects a single local file (e.g. `put`), only the first filename generated by the “globbing” operation is used.

- For `mget` and `get` commands with unspecified local file names, the local filename is the remote file name.
- For `mput` and `put` commands with unspecified remote file names, the remote file name is the local file name.

NOTE `fdx` and other FTP command-line clients do not support ECXpert batch submission and retrieval, i.e., `mput` and `mget` behavior.

The Partner Agent Windows Client, however, does support `mput` and `mget` behavior by decomposing batch file transfers into individual transfers, transparently to the user.

File Transfer Parameters

The FTP specification defines many parameters that can affect an FTP file transfer. These parameters are *type*, *mode form*, and *struct*. Partner Agent Server supports only the default values for these, except for *type*. Type is either:

- `ascii`
- OR
- `image` (binary).

FTP Interactive Commands

The following commands are recognized by Partner Agent Server Command Line Client in the FTP scheme.

NOTE Commands marked with an * are available only when the Client is connected to a Partner Agent Server.

Table B-4 FTP interactive commands

Command	Description
<code>!</code> <i>[command [args]]</i>	Invoke an interactive shell on the local machine. If there are arguments, the first is taken to be a command to execute directly, with the rest of the arguments as the command's arguments.
<code>account</code> <i>[passwd]</i>	Supply a supplemental password required by a remote system for access to resources once a login has been successfully completed. If no argument is included, the user is prompted for an account password in a non-echoing input mode. Note: This command is not supported by Partner Agent Server.
<code>alias</code>	Get server alias list.
<code>anonymous</code>	Toggle anonymous logins.
<code>append</code> <i>local-file</i> <i>[remote-file]</i>	Append a local file to a file on the remote machine. If <i>remote-file</i> is left unspecified, the local file name is used in naming the remote file. File transfer uses the current settings for type, format, mode, and structure. Note: This command is not supported by Partner Agent Server.
<code>ascii</code>	Set the file transfer type to network ASCII. This is the default type.
<code>*autoreset</code>	Toggle automatic restart of partial transfers.
<code>bandwidth</code> <i>[N]</i>	Set throttle bandwidth in KB/s.
<code>binary</code>	Set the file transfer type to support binary image transfer.
<code>bye</code>	Terminate the FTP session with the remote server and exit FTP. An end of file, (Ctrl-D), also terminates the session and exits.
<code>cd</code> <i>[remote-directory]</i>	Change the working directory on the remote machine to remote directory.
<code>cat</code> <i>[file-name]</i>	View contents of remote file.
<code>cdpath</code>	Get server cdpath list.
<code>cdup</code>	Change the remote machine working directory to the parent of the current remote machine working directory.
<code>*checksum</code>	Toggle MD5 checksums on <i>get/put</i> .
<code>chmod</code> <i>mode</i> <i>file-name</i>	Change the permission modes of the file <i>file-name</i> on the remote system to <i>mode</i> .
<code>close</code>	Terminate the FTP session with the remote server, and return to the command interpreter.
<code>commands</code>	Show FTP commands sent to server.

Table B-4 FTP interactive commands (*Continued*)

Command	Description
<code>delete remote-file</code>	Delete the file <code>remote-file</code> on the remote machine.
<code>dir</code> <code>[remote-directory]</code>	Print a list of the contents of a directory on the remote machine. The listing includes any system-dependent information that the server chooses to include. If <code>remote-directory</code> is left unspecified, the current working directory is used. If you <code>dir</code> a file-name, information about the file is printed.
<code>exit</code>	Terminate the FTP session with the remote server and exit. An end of file also terminates the session and exits.
<code>form format</code>	Set the file transfer form to <code>format</code> . The default format is “non-print.” Partner Agent Server only supports the default mode.
<code>get remote-file</code> <code>[local-file]</code>	Retrieve the <code>remote-file</code> and store it on the local machine. If the local file name is not specified, it is given the same name it has on the remote machine. The current settings for type, form, mode, and structure are used while transferring the file.
<code>help [command]</code>	Print an informative message about the meaning of <code>command</code> . If no argument is given, Partner Agent Server prints a list of the known commands.
<code>idle [seconds]</code>	Set the inactivity timer on the remote server to <code>seconds</code> . If <code>seconds</code> is omitted, the current inactivity timer is printed.
<code>image</code>	Set the file transfer type to support binary image transfer.
<code>lcd [directory]</code>	Change the working directory on the local machine. If no directory is specified, the user’s home directory is used.
<code>lcdup</code>	Change the local working directory to parent.
<code>*lmd5 [local-file]</code>	Compute MD5 checksum of local file.
<code>lpwd</code>	Get local working directory.
<code>ls</code> <code>[remote-directory]</code>	Print a list of the contents of a directory on the remote machine. The listing includes any system-dependent information that the server chooses to include; for example, most UNIX systems produce output from the command <code>ls-l</code> . (See also <code>nlist</code>). If <code>remote-directory</code> is left unspecified, the current working directory is used. If you <code>ls</code> a file-name, information about the file is printed.
<code>lsd [directory name]</code>	Page contents of remote directory.
<code>md directory-name</code>	Make a directory on the remote machine.
<code>*md5 remote-file</code>	Compute MD5 checksum of remote file.
<code>mdelete</code> <code>[remote-files]</code>	Delete the remote-files on the remote machine.

Table B-4 FTP interactive commands (*Continued*)

Command	Description
<code>mget remote-files</code>	Expand the remote-files on the remote machine and do a <code>get</code> for each file name that is produced. Files are transferred into the local working directory, which can be changed with the <code>lcd directory</code> command. New local directories can be created with <code>!</code> .
<code>mkdir</code>	Make a directory on the remote machine.
<code>mode [mode-name]</code>	Set the file transfer mode to mode-name. The default mode is “stream” mode. Partner Agent Server only supports the default mode.
<code>modtime file-name</code>	Show the last modification time of the file on the remote machine.
<code>more file-name</code>	Page contents of remote file.
<code>mput local-files</code>	Expand wild cards in the list of local files given as arguments and do a <code>put</code> for each file in the resulting list.
<code>newer file-name</code>	Get the file only if the modification time of the remote file is more recent than the file on the current system. If the file does not exist on the current system, the remote file is considered newer. Otherwise, this command is identical to <code>get</code> .
<code>nlist [remote-directory]</code>	Print a list of the files in a directory on the remote machine. If remote directory is left unspecified, the current working directory is used.
<code>open host [port]</code>	Establish a connection to the specified host server. An optional port number can be supplied, in which case, Partner Agent Server attempts to contact a server at that port.
<code>passive</code>	Enable passive mode operation for use behind connection filtering firewalls.
<code>progress</code>	Toggle the progress meter for file transfers. The default is for the progress meter to be off.
<code>prompt</code>	Toggle interactive prompting. Interactive prompting occurs during multiple file transfers to allow the user to selectively retrieve or store files. If prompting is turned off (default is on), any <code>mget</code> or <code>mput</code> transfers all files, and any <code>mdelete</code> deletes all files.
<code>put local-file [remote-file]</code>	Store a local file on the remote machine. If remote-file is left unspecified, the local file name is used. File transfer uses the current settings for type, format, mode, and structure.
<code>pwd</code>	Print the name of the current working directory on the remote machine.
<code>quit</code>	Terminate the FTP session with the remote server and exit FTP. An end of file also terminates the session and exits.
<code>quote arg 1 arg 2 . . .</code>	The arguments specified are sent, verbatim, to the remote FTP server.
<code>rd directory-name</code>	Delete a directory on the remote machine.

Table B-4 FTP interactive commands (*Continued*)

Command	Description
<code>reget remote-file [local-file]</code>	Reget acts like get, except that if local-file exists and is smaller than remote-file, local-file is presumed to be a partially transferred copy of remote-file and the transfer is continued from the apparent point of failure. This command is useful when transferring very large files over networks that are prone to dropping connections. An md5 checksum is taken on the partial transmitted file and compared to the original to insure the data integrity of the transfer. If it is different you are asked if you wish to continue the transfer, abort or start over.
<code>restart</code>	A manual way of invoking the restart function if the connection to the server is interrupted.
<code>rename [from] [to]</code>	Rename a remote file.
<code>reput local-file [remote-file]</code>	Reput acts like put, except that if remote-file exists and is smaller than local-file, remote-file is presumed to be a partially transferred copy of remote-file and the transfer is continued from the apparent point of failure. This command is useful when transferring very large files over networks that are prone to dropping connections. An MD5 checksum is taken on the partial transmitted file and compared to the original to insure the data integrity of the transfer. If it is different you are asked if you want to continue the transfer, abort or start over.
<code>retry</code>	Toggle connection retry.
<code>rhel [command-name]</code>	Request help from the remote FTP server. If a command-name is specified, it is supplied to the server as well.
<code>rmdir directory-name</code>	Delete a directory on the remote machine.
<code>rstatus [file-name]</code>	With no arguments, show status of remote machine. If file-name is specified, show status of file-name on remote machine.
<code>sendport</code>	Toggle the use of PORT commands. By default, Partner Agent Server attempts to use a PORT command when establishing a connection for each data transfer. The use of PORT commands can prevent delays when performing multiple file transfers. If the PORT command fails, Partner Agent Server uses the default data port. When the use of PORT commands is disabled, no attempts are made to use PORT commands for each data transfer. This is useful for certain FTP implementations that do ignore PORT commands but, incorrectly, indicate they have been accepted.
<code>site arg 1 arg 2 . . .</code>	The arguments specified are sent, verbatim, to the remote FTP server as a SITE command.
<code>size file-name</code>	Return size of the file-name on the remote machine.

Table B-4 FTP interactive commands (*Continued*)

Command	Description
<code>ssl option</code>	Set SSL options to <code>req</code> , <code>opt</code> , or <code>off</code> .
<code>sslmode mode</code>	Set SSL mode to <code>std</code> , <code>spe</code> , or <code>tun</code> .
<code>sslver version number</code>	Set SSL version to <code>v2</code> , <code>v3</code> , or <code>v23</code> .
<code>status</code>	Show the current status of Partner Agent Server.
<code>struct [struct-name]</code>	Set the file transfer type to <code>struct-name</code> . By default “file” structure is used. Partner Agent Server only supports the default.
<code>system</code>	Show the type of operating system running on the remote machine.
<code>throttle</code>	Toggle bandwidth throttling.
<code>type [type-name]</code>	Set the file transfer type to <code>type-name</code> . If no type is specified, the current type is printed. The default type is network ASCII.
<code>umask [newmask]</code>	Set the default umask on the remote server to <code>newmask</code> . If <code>newmask</code> is omitted, the current umask is printed.
<code>*update file-name</code>	Get if remote file is different from local copy.
<code>user user-name [password] [account]</code>	Identify yourself to the remote FTP server. If the password is not specified and the server requires it, Partner Agent Server prompts you for it (after disabling the local echo). If an account is not specified, and the FTP server requires it, you are prompted for it. If an account is specified, an account command is relayed to the remote server after the login sequence is completed if the remote server did not require it for logging in. Unless Partner Agent Server is invoked with “auto-login” disabled, this process is done automatically on initial connection to the FTP server.
<code>verbose [level]</code>	If no level is specified, toggle verbose mode, or set verbose mode to the specified level. In verbose mode, all responses from the FTP server are displayed to you. In addition, if verbose mode is on, when a file transfer completes, statistics regarding the efficiency of the transfer are reported. By default, verbose is on. Enter a number for the level of verbosity.
<code>? [command]</code>	Print an informative message about the meaning of command. If no argument is given, Partner Agent Server prints a list of the known commands. Command arguments that have embedded spaces can be quoted with quotation marks.

HTTP or HTTPS Interactive Commands

The following commands are recognized by Partner Agent Server Command Line Client in the HTTP or HTTPS schemes:

NOTE Commands marked with an * are available only when the Client is connected to a Partner Agent Server.

Table B-5 HTTP(S) interactive commands

Command	Description
! <i>[command [args]]</i>	Invoke an interactive shell on the local machine. If there are arguments, the first is taken to be a command to execute directly, with the rest of the arguments as its arguments.
anonymous	Toggle anonymous logins.
*autorestart	Toggle automatic restart of partial transfers.
bandwidth <i>[N]</i>	Set throttle bandwidth in KB/s.
bye	Terminate the HTTP session with the remote server and exit Partner Agent Server. An end of file also terminates the session and exits.
cd <i>[remote-directory]</i>	Change the working directory on the remote machine to remote directory.
cat <i>[file-name]</i>	View contents of remote file.
cdup	Change the remote machine working directory to the parent of the current remote machine working directory.
*checksum	Toggle MD5 checksums on get/put.
close	Terminate the session with the remote server, and return to the command interpreter.
commands	Show commands sent to server.
delete <i>remote-file</i>	Delete the file <i>remote-file</i> on the remote machine.
dir <i>[remote-directory]</i>	Print a list of the contents of a directory on the remote machine. The listing includes any system-dependent information that the server chooses to include. If <i>remote-directory</i> is left unspecified, the current working directory is used. If you specify a file name instead of a directory name, Partner Agent Server will get the file.

Table B-5 HTTP(S) interactive commands (*Continued*)

Command	Description
<code>exit</code>	Terminate the session with the remote server and exit Partner Agent Server. An end of file also terminates the session and exits.
<code>get remote-file</code> <code>[local-file]</code>	Retrieve the remote-file and store it on the local machine. If the local file name is not specified, it is given the same name it has on the remote machine.
<code>help [command]</code>	Print an informative message about the meaning of command. If no argument is given, Partner Agent Server prints a list of the known commands.
<code>lcd [directory]</code>	Change the working directory on the local machine. If no directory is specified, the user's home directory is used.
<code>lcdup</code>	Change the local working directory to parent.
<code>*lmd5 [local-file]</code>	Compute MD5 checksum of local file.
<code>lpwd</code>	Get local working directory.
<code>ls</code> <code>[remote-directory]</code>	Print a list of the contents of a directory on the remote machine. The listing includes any system-dependent information that the server chooses to include; for example, most UNIX systems produce output from the command <code>ls-l</code> . If <code>remote-directory</code> is left unspecified, the current working directory is used. If you specify a file name instead of a directory name, Partner Agent Server will <code>get</code> the file.
<code>lsd [directory</code> <code>name]</code>	Page contents of remote directory.
<code>*md5 remote-file</code>	Compute MD5 checksum of remote file.
<code>modtime file-name</code>	Show the last modification time of the file on the remote machine.
<code>more file-name</code>	Page contents of remote file.
<code>newer file-name</code>	Get the file only if the modification time of the remote file is more recent than the file on the current system. If the file does not exist on the current system, the remote file is considered newer. Otherwise, this command is identical to <code>get</code> .
<code>open host [port]</code>	Establish a connection to the specified host HTTP server. An optional port number can be supplied, in which case, Partner Agent Server attempts to contact the HTTP server at that port.
<code>progress</code>	Toggle the progress meter for file transfers. The default is for the progress meter to be off.
<code>prompt</code>	Toggle interactive prompting. Interactive prompting occurs during multiple file transfers to allow the user to selectively retrieve or store files. If prompting is turned off (default is on), any <code>mget</code> or <code>mput</code> transfers all files, and any <code>mdelete</code> deletes all files.

Table B-5 HTTP(S) interactive commands (*Continued*)

Command	Description
<code>put local-file [remote-file]</code>	Store a local file on the remote machine. If remote-file is left unspecified, the local file name is used.
<code>pwd</code>	Print the name of the current working directory on the remote machine.
<code>quit</code>	Terminate the session with the remote server and exit Partner Agent Server.
<code>reget remote-file [local-file]</code>	A manual way of invoking the restart function if the connection to the server is interrupted. An MD5 checksum is taken on the partial transmitted file and compared to the original to insure the data integrity of the transfer. If it is different you are asked if you wish to continue the transfer, abort or start over.
<code>reput local-file [remote-file]</code>	Reput acts like put, except that if remote-file exists and is smaller than local-file, remote-file is presumed to be a partially transferred copy of remote-file and the transfer is continued from the apparent point of failure. This command is useful when transferring very large files over networks that are prone to dropping connections. An MD5 checksum is taken on the partial transmitted file and compared to the original to insure the data integrity of the transfer. If it is different you are asked if you want to continue the transfer, abort or start over.
<code>restart</code>	A manual way of invoking the restart function if the connection to the server is interrupted.
<code>retry</code>	Toggle connection retry.
<code>size file-name</code>	Return size of the file-name on the remote machine.
<code>status</code>	Show the current status of Partner Agent Server.
<code>throttle</code>	Toggle bandwidth throttling.
<code>*update file-name</code>	Get if remote file is different from local copy.
<code>user user-name [password]</code>	Identify yourself to the remote server. If the password is not specified and the server requires it, Partner Agent Server prompts you for it (after disabling the local echo).
<code>verbose [level]</code>	If no level is specified, toggle verbose mode, or set verbose mode to the specified level. In verbose mode, all responses from the server are displayed to you. In addition, if verbose mode is on, when a file transfer completes, statistics regarding the efficiency of the transfer are reported. By default, verbose mode is on. Enter a number for the level of verbosity.
<code>? [command]</code>	Print an informative message about the meaning of command. If no argument is given, Partner Agent Server prints a list of the known commands. Command arguments that have embedded spaces can be quoted with quotation marks.

Tracking File Transfers in ECXpert

When you transfer files to or from ECXpert using the Command Line Client, ECXpert tracking information is displayed in the Client window in both human-readable form and in and tag-based—i.e., programmatically-readable—form (see Figure B-9).

Figure B-9 Sample ECXpert tracking information displayed by Command Line Client

```
226 Transfer Complete: Retrieved data from ECXpert successfully with tracking
ID 6.<SR><TI>6</TI><RC>0</RC><EM>Retrieved data from ECXpert successfully with
tracking ID 6</EM></SR>
```

The tag-based information is used by the Partner Agent Windows Client parser to display ECXpert tracking information to the Windows Client user. The following are the tags displayed by the Command Line Client after a file is transferred. Each tag-value pair is closed by the corresponding `</ X>`, where *X* is a tag.

Table B-6 ECXpert tracking tags displayed by Command Line Client

Tag	Definition
<SR>	Start message
<TI>	ECXpert tracking ID (set to 0 on error)
<RC>	Return code (set to zero on success)
	Error message (could be set to nothing)

To track a file transfer from the ECXpert product administrative interface,

1. Log into the ECXpert Product Administrative Interface.
2. Click the Tracking button.

The Enter Search Constraints tab is displayed.

3. Click any of the other tabs.
4. Enter the Tracking ID for the file transfer and click Search.

For more information on using the ECXpert Tracking feature, see the *ECXpert Site Administrator's Handbook*.

NUMERICS

- 530 Service Not Available error 192
- 530 Service not available error 191

A

- Aborting file transfer 199
- About this book 15
- Access
 - ActiveAgents 163, 164, 165
 - ActiveAgents rules 163
 - allowing
 - to groups 117
 - to users 115
 - anonymous logins 117
 - enabling or disabling 118
 - passwords 119
 - denying 114
 - to groups 116, 117
 - to users 115
 - download restrictions 125
 - adding entry 125
 - deleting entry 126
 - editing entry 126
 - enabling or disabling entry 126
 - filesystem restrictions 119
 - adding entry 121
 - deleting entry 121
 - editing entry 121
 - enabling or disabling entry 121
 - limiting number of users 111, 112, 113
 - upload restrictions 122
 - adding entry 123
 - deleting entry 124
 - editing entry 124
 - enabling or disabling entry 124
- Access control pages 93
- Access rules
 - administration system
 - adding entry 95
 - deleting entry 96
 - enabling or disabling entry 95
 - example entry 96
 - reordering 95
 - server
 - adding entry 98
 - deleting entry 99
 - editing entry 99
 - enabling or disabling entry 98
 - example entry 99
 - reordering 98
- ActiveAgent entry 167
- ActiveAgent server 159
- ActiveAgents 158, 166, 170
 - access 163
 - access rules 163
 - deleting entry 165

- editing entry 165
- enabling or disabling entry 165
- reordering 164
- adding entry 168
- agentd server 166
- auth 172
- bundled 162
- cert 170
- chaining 168
- config 171
- deleting entry 170
- descriptions 170
- editing entry 170
- enabling or disabling entry 170
- environment variables 159
- FTP Command 175
- HTTP Command 175
- incoming 174
- incoming abort 174
- incoming end 174
- incoming error 174
- incoming start 174
- login 173
- logout 173
- outgoing abort 174
- outgoing end 174
- outgoing error 174
- outgoing start 174
- ActiveAgents server 43
- adding limit entry 112
- addpasswd utility 48
- Admin server 42
- admin server 43
- Administration system 21, 54
 - access controls 93
 - access rules
 - adding entry 95
 - deleting entry 96
 - enabling or disabling entry 95
 - example entry 96
 - reordering 95
 - accessing 55
 - host access 94
 - navigating 55
 - starting 55
- Administrator email address 86

- Administrator password
 - adding 48
 - changing default 48
- Agent server port 166
- Agent supplied cookies 162
- Agentd server 42, 166
- agentd server 43
- Agents
 - auth 158
 - cert 158
 - config 158
 - FTP commands 158
 - incoming 158
 - login 158
 - logout 158
 - outgoing 158
- Anonymous logins 117
 - enabling or disabling 118
 - passwords 119
- Anonymous users 68
- Archive 152
- Audience and roles 19
- Auth agents 158
- Authentication 132
 - failure 133
 - magic cookie 133
 - non-existent agent 133
 - order 133
 - setting options 133
- Authentication issues 133
- Auto refresh 150

B

- Base port and range for passive mode 82
- Baseline
 - creating 90
- Before you begin 16
- Bounce options 64
 - setting 64
- Bouncing FTP server manually 65
- Bundled ActiveAgents 162

C

CA signing certificate 54

Cert agents 158

Certificate

client 130

enabling or disabling verification 130

issuer 54

Certificate (cert) agent 170

Certificates

importing user certificates 49

Chaining ActiveAgents 168

Changing system configurations 57

Class definition

adding 70

deleting 71

disabling 71

editing 71

enabling 71

Classes 68

Client certificates 130

enabling or disabling verification 130

Command Line Client

aborting file transfer 199

arguments 213

environment variables 198

file naming conventions 213

FTP command line options 211

FTP interactive commands 214, 215

? 219

alias 215

anonymous login 215

append file 215

arguments 217

ascii file transfer 215

bandwidth 215

binary file transfer 215

binary image transfer 216

bye 215

cat 215

cd 215

cdpath 215

cdup 215

change directory 215

checksum 215

chmod 215

delete 216

delete directory 217, 218

delete remote file 216

dir 216

establish connection 217

exit 216

form 216

get 216

help 216, 218

idle 216

image 216

lcd 216

lcdup 216

list 216

list directory 217

ls 216

lsd 216

make directory 216, 217

md 216

md5 216

mdelete 216

mget 217

mkdir 217

mode 217

modification 217

modtime 217

more 217

mput 217

newer 217

nlist 217

open 217

operating system 219

passive mode 217

password 215

permission mode 215

PORT commands 218

print directory name 217

progress 217

prompt 217

put 217

pwd 217

quit 217

quote 217

rd 217

reget 218

rename 218

reput 218

- restart 215, 218
- retry 218
- rhel 218
- rmdir 218
- rstatus 218
- sendport 218
- shell 215
- show commands 215
- site 218
- size 218
- SSL 219
- sslmode 219
- sslv 219
- status 219
- struct 219
- system 219
- terminate 215, 216, 217
- throttle 219
- throttle bandwidth set 215
- type 219
- umask 219
- update 219
- user 219
- verbose 219
- working directory 216
- FTP options 211
- FTP parameters 214
- HTTP and HTTPS interactive commands 220
 - ! 220
 - ? 222
 - anonymous login 220
 - autorestart 220
 - bandwidth 220
 - bandwidth throttling 222
 - bye 220
 - cat 220
 - cd 220
 - cdup 220
 - change directory 220
 - checksum 220
 - close 220
 - commands 220
 - connection retry 222
 - delete 220
 - dir 220
 - exit 221
 - get 221
 - help 221
 - lcd 221
 - lcdup 221
 - lmd5 221
 - lpwd 221
 - ls 221
 - lsd 221
 - md5 221
 - modification time 221
 - modtime 221
 - more 221
 - newer 221
 - open 221
 - prompt 221
 - put 222
 - pwd 222
 - quit 222
 - reget 222
 - reput 222
 - restart 222
 - retry 222
 - shell 220
 - size 222
 - status 222
 - terminate 220, 222
 - throttle 222
 - verbose 222
- HTTP options 212
- HTTP(S) command line options 212
- options 211
- protocol schemes 198
- schemes 198
 - FTP 196, 197, 198
 - HTTP 196, 197
 - HTTPS 196, 197
- SSL 198
- starting 196
- tracking ECXpert transfers 223
- transfer protocol schemes 198
- transferring files 199
 - downloading from ECXpert from the command line 207
 - downloading from ECXpert interactively 209
 - downloading from non-ECXpert machines from the command line 205
 - downloading from non-ECXpert machines interactively 206

- uploading to ECXpert from the command line 202
- uploading to ECXpert interactively 203
- uploading to non-ECXpert machines from the command line 200
- uploading to non-ECXpert machines interactively 201
- using shell scripts 199
- tunnel mode 198
- Command line FTP Client 49
- Command line options 211
 - FTP 211
 - anonymous login 211
 - ascii transfer mode 211
 - auto-restart 211
 - bandwidth throttle 211
 - binary transfer mode 211
 - control channel 212
 - EBCDIC transfer mode 211
 - firewalls 211
 - interactive prompting 211
 - quiet mode 211
 - restart transfer 211
 - retry 211
 - SSL 212
 - tunnel 212
 - user name 211
 - HTTP 212
 - anonymous login 212
 - auto-restart 212
 - bandwidth throttle 213
 - help 212
 - quiet mode 212
 - restart 212
 - retry 213
 - SSL 213
- Command logging 77
 - adding entry 78
 - deleting entry 79
 - disabling or enabling entry 79
 - editing entry 79
- Config agents 158
- Conventions used in this book 21
 - generic names 21
 - typographic 21
- Cookie

- magic 133
- Cookies 76
 - agent supplied 162
- Crontab 149

D

- Default administrator password
 - changing 48
- Default settings 36
 - ActiveAgents 36
 - administrator username and password 36
 - security settings 37
 - signing certificate password 36
- Default user classes 69
- deleting limit entry 113
- deleting rule entry 165
- Distribution 28
- Documentation
 - downloading 16
- Documentation set 17
- Download restrictions 125
 - adding entry 125
 - deleting entry 126
 - editing entry 126
 - enabling or disabling entry 126
- Downloading updated documentation 16

E

- ecx.ini file 31
- ecxpa 28
- ecxpa-bye 28
- ecxpa-cleanup 29
- ecxpa-config 29
- ecxpa-fd-certify 28
- ecxpa-login 29
- ecxpa-m-server 28
- ecxpa-retrieve 29
- 31

- expa-submit 29
- expa-welcome 28
- ECXpert
 - tracking files transfers 223
- ECXpert database
 - MSGFORMATS 35
- ECXpert documentation set 17
- ECXpert ecx.ini file 31
- ECXpert member directories 35
- Edit file 102
- Edit perms 102, 105
- editing limit entry 113
- editing rule entry 165
- enabling or disabling limit entry 113
- enabling or disabling rule entry 165
- Encryption
 - deleting entry 131
 - editing entry 131
 - enabling or disabling entry 131
- EnGuard 137
- Entrust configuration 137
- Environment variables 159, 198

F

- Failed logins 134
 - changing threshold 134
- fdx utility 49
- features 27
- Filesystem restrictions 119
 - adding entry 121
 - deleting entry 121
 - editing entry 121
 - enabling or disabling entry 121
- FTP 196, 197, 198
 - SSL 198
- FTP command agents 175
- FTP command line options 211
 - anonymous login 211
 - ascii transfer mode 211
 - auto-restart 211
 - bandwidth throttle 211
 - binary transfer mode 211
 - control channel 212
 - EBCDIC transfer mode 211
 - firewalls 211
 - interactive prompting 211
 - quiet mode 211
 - restart transfer 211
 - retry 211
 - SSL 212
 - tunnel 212
 - user name 211
- FTP command options
 - setting 136
- FTP commands 135, 158
 - deleting entry 136
 - editing entry 136
- FTP interactive commands 214, 215
 - ? 219
 - alias 215
 - anonymous login 215
 - append file 215
 - arguments 217
 - ascii file transfer 215
 - bandwidth 215
 - binary file transfer 215
 - binary image transfer 216
 - bye 215
 - cat 215
 - cd 215
 - cdpath 215
 - cdup 215
 - change directory 215
 - checksum 215
 - chmod 215
 - delete 216
 - delete directory 217, 218
 - delete remote file 216
 - dir 216
 - erminate 215
 - establish connection 217
 - exit 216
 - form 216
 - get 216
 - help 216, 218
 - idle 216
 - image 216
 - lcd 216

- lcdup 216
- list 216
- list directory 217
- ls 216
- lsd 216
- make directory 216, 217
- md 216
- md5 216
- mdelete 216
- mget 217
- mkdir 217
- mode 217
- modification 217
- modtime 217
- more 217
- mput 217
- newer 217
- nlist 217
- open 217
- operating system 219
- passive mode 217
- password 215
- permission mode 215
- PORT commands 218
- print directory name 217
- progress 217
- prompt 217
- put 217
- pwd 217
- quit 217
- quote 217
- rd 217
- reget 218
- rename 218
- reput 218
- restart 215, 218
- retry 218
- rhel 218
- rmdir 218
- rstatus 218
- sendport 218
- shell 215
- show commands 215
- site 218
- size 218
- SSL 219
- sslmode 219

- sslver 219
- status 219
- struct 219
- system 219
- terminate 215, 216, 217
- throttle 219
- throttle bandwidth set 215
- type 219
- umask 219
- update 219
- user 219
- verbose 219
- working directory 216

FTP server

- bounce options 64
 - setting 64
- bouncing manually 65
- changing mode 65
- inetd mode 65
- port 65
- standalone mode 65

FTP server modes of operation 65

Ftpd server 42

ftpd server 43

G

gencerts utility 46

Generate statistics now 155

generating self-issued certificates 46

Groups

- allow 117
- allowing access 117
- denying access 116, 117
- virtual 110

H

host access

- administration system 94
- server 97

HTTP 196, 197
 HTTP and HTTPS interactive commands 220
 ! 220
 ? 222
 anonymous login 220
 autorestart 220
 bandwidth 220
 bandwidth throttling 222
 bye 220
 cat 220
 cd 220
 cdup 220
 change directory 220
 checksum 220
 close 220
 commands 220
 connection retry 222
 delete 220
 dir 220
 exit 221
 get 221
 help 221
 lcd 221
 lcdup 221
 lmd5 221
 lpwd 221
 ls 221
 lsd 221
 md5 221
 modification time 221
 modtime 221
 more 221
 newer 221
 open 221
 prompt 221
 put 222
 pwd 222
 quit 222
 reget 222
 reput 222
 restart 222
 retry 222
 shell 220
 size 222
 status 222
 terminate 220, 222
 throttle 222
 verbose 222
 HTTP command agents 175
 HTTP command line options 212
 anonymous login 212
 auto-restart 212
 bandwidth throttle 213
 help 212
 quiet mode 212
 restart 212
 retry 213
 SSL 213
 HTTP server 66
 port 66
 HTTP(S) command line options 212
 Httpd server 42
 httpd server 43
 HTTPS 196, 197
 HTTPS server
 port 66

I
 importcert utility 49
 Incoming abort agent 174
 Incoming agents 158, 174
 Incoming end agent 174
 Incoming error agent 174
 Incoming start agent 174
 Incremental version display 90
 Inetd mode 65
 Issuer certificate 54

L
 libexpacleanup10.so 30
 libexpaconfig10.so 30
 libexpalogin10.so 30
 libexpaplugin10.so 30
 libexparetrieve10.so 30
 libexpaserver10.so 30

- libexpasubmit10.so 30
- libexpautil10.so 30
- Libraries 30
- License 66
- Login agent 173
- Login agents 158
- Login failures 134
 - changing threshold 134
- Logins
 - anonymous 117
 - enabling or disabling 118
 - passwords 119
- Logout agent 173
- Logout agents 158

M

- Magic cookie 133
- Magic cookies 76
- Master server control pages 59
- Master virtual user 109
- member directories 35
- Messages 73
 - README 75
 - run-time 75
 - startup 75
- Mirror
 - deleting entry 85
 - example entry 85
- Mirror server
 - adding entry 84
 - editing entry 84
 - enabling or disabling entry 84
- Mirror servers 83
- Miscellaneous options 85
 - administrator email address 86
 - reverse DNS lookups 87
 - session timeout 88
 - usage monitor options 87
 - valid user shell check 88
- mkpasswd utility 48
- Mode of operation 65

- mode of operation
 - changing 65
- MSGFORMATS messages 35
- Multi-tiered architecture 159

N

- Non-secure port 66

O

- Options
 - command line 211
 - FTP 211
 - HTTP 212
- Organization of this book 19
- Outgoing abort agent 174
- Outgoing agents 158
- Outgoing end agent 174
- Outgoing error agent 174
- Outgoing start agent 174

P

- Partner Agent Client 27
- Partner Agent Client/Server System 26
- Partner Agent Server 26
 - distribution 28
 - features 27
 - programs and scripts 28
 - ECXpert wrapper 28
 - starting 39
 - stopping 43
- Passive mode 81
 - specifying base port and range 82
- Password authentication (auth) agent 172
- Password files 100
 - adding entry 101, 104

- deleting entry 102, 104
- editing 103
- editing entry 102, 104
- enabling or disabling entry 102, 104
- virtual user 100
- virtual users
 - adding permission entry 106
 - changing conflict policy 107
 - deleting permission entry 107
 - editing permission entry 107
 - editing permissions 105
 - enabling or disabling permission entry 107
 - example permission entry 108
 - master 109
 - moving permission entry 107
 - permission rules 106
 - rule order and conflict policy 106
 - virtual shared directories 106

Password policy 119

Passwords

- anonymous 119

Port

- agent server 166
- FTP server 65
- HTTP server 66
- HTTPS server 66

Pre-configured settings 36

- ActiveAgents 36
- administrator username and password 36
- security settings 37
- signing certificate password 36

Previous version 91

Programs and scripts 28

- ECXpert ActiveAgents
 - ecxpa 28
 - ecxpa-bye 28
 - ecxpa-cleanup 29
 - ecxpa-config 29
 - ecxpa-fd-certify 28
 - ecxpa-login 29
 - ecxpa-retrieve 29
 - ecxpa-submit 29
 - ecxpa-welcome 28

- ECXpert Wrapper 28

- ECXpert wrapper
 - ecxpa-m-server 28

Protocol schemes 198

R

Range and base port for passive mode 82

README messages 75

Real users 68

reordering rules 164

Restrictions

- download 125

- adding entry 125

- deleting entry 126

- editing entry 126

- enabling or disabling entry 126

- filesystem 119

- adding entry 121

- deleting entry 121

- editing entry 121

- enabling or disabling entry 121

- upload 122

- adding entry 123

- deleting entry 124

- editing entry 124

- enabling or disabling entry 124

Reverse DNS lookups

- enabling or disabling 87

Rules

- access to administration system

- adding entry 95

- deleting entry 96

- enabling or disabling entry 95

- example entry 96

- reordering 95

- access to server

- adding entry 98

- deleting entry 99

- editing entry 99

- enabling or disabling entry 98

- example entry 99

- reordering 98

- ActiveAgent host access 163

- limit 111

Run-time messages 75

- adding 76

- deleting 77
- editing 77
- enabling or disabling 77

S

Scheduling a shutdown 62

Schemes 198

- FTP 196, 197, 198

- SSL 198

- HTTP 196, 197

- HTTPS 196, 197

Secure port 66

Secure Sockets Layer 128

- See also SSL

Security audit 137

- control panel 138

- features 137

- performing 147

- reports

- archival and distribution options 141

- browsing 139

- configuring archival and distribution 140

- customizing 142

- enabling or disabling report settings 144

- enabling or disabling security checks 143

- report errors 144

- report progress 144

- report violations 144

- report warnings 144

- running as a cron job 138

- See also security audit

- settings 138

Security checks

- configuring anonymous FTP check 145

- excluding directory 146

- excluding file 147

- removing directory from excluded list 147

- removing file from excluded list 147

Security control pages 127

self-issued certificates 46

Server

- access rules

- adding entry 98

- deleting entry 99

- editing entry 99

- enabling or disabling entry 98

- example entry 99

- reordering 98

- host access 97

- starting 60

Server control 63

Server license 66

Server messages 73

Server shutdown

- immediate 61

- message 62

- scheduling 62

- stopping a standalone server 63

Server shutdown options 61

Server startup messages 75

Server Status 60

Server usage

- by connection 151

- by user class 151

- statistics configuration manager 152

- statistics control panel 151

- statistics generator 154

- statistics viewer 152

Server usage monitor 150

Session timeout 88

Setting bounce options 64

Shared directories 106

Shutdown 43

Shutting down the server 61

Snapshot

- current version 90

- deleting baseline 90

- server usage by connection 151

- server usage by user class 151

Software version 60

SSL 128

- client certificates 130

- enabling or disabling verification 130

- enabling or disabling 130

- encryption

- deleting entry 131

- editing entry 131

- enabling or disabling entry 131

- users encryption
 - adding entry 131
- Stand-alone FileDrive server
 - ActiveAgent port 187
 - ActiveAgents port 187
 - administrator password 190
 - CA signing certificate 187
 - certificates 187
 - chroot 193
 - distribution 181
 - environment variables 194
 - hardware requirements 180
 - installing 182
 - license 182
 - expired 193
 - license file
 - installing 191
 - PEM pass phrase 187
 - server port 187
 - server's private key 187
 - uninstalling 191
 - users 193
- Standalone mode 65
- Starting 39
- Startup messages 75
- Statistics
 - archive 152
 - configuration manager 152
 - control panel 151
 - generate now 155
 - generator 154
 - server usage 151
 - viewer 152
- Statistics control pages 149
- Stopping 43
- Stopping a standalone server 63
- System configuration
 - changing 57

T

- Timeout 88
- Tracking file transfers in ECXpert 223

- Transfer logging 79
 - adding entry 80
 - deleting entry 81
 - editing entry 81
 - enabling or disabling entry 81
- Transfer protocol schemes 198
- Transferring Files
 - with Command Line Client 199
 - downloading from ECXpert from the command line 207
 - downloading from ECXpert interactively 209
 - downloading from non-ECXpert machines from the command line 205
 - downloading from non-ECXpert machines interactively 206
 - tracking ECXpert transfers 223
 - uploading to ECXpert from the command line 202
 - uploading to ECXpert interactively 203
 - uploading to non-ECXpert machines from the command line 200
 - uploading to non-ECXpert machines interactively 201
 - using shell scripts 199
- Tunnel mode 198

U

- Upload restrictions 122
 - adding entry 123
 - deleting entry 124
 - editing entry 124
 - enabling or disabling entry 124
- Usage monitor 150
- Usage monitor options 87
- User authentication 132
 - setting options 133
- User certificates
 - importing 49
- User Class
 - server usage 151
- User classes 68
 - default 69
 - examples 72

User configuration (config) agent 171

User limits 111

adding entry 112

deleting entry 113

editing entry 113

enabling or disabling entry 113

User types 68

anonymous 68

real 68

virtual 69

Users

allowing access 115

denying access 114, 115

limiting access 111, 112, 113

virtual 100

Users encryption

adding entry 131

Utilities

addpasswd 48

fdx 49

gencerts 46

importcert 49

mkpassword 48

V

Valid user shell check

enabling or disabling 88

Version

deleting 90

incremental version display 90

taking snapshot 90

Version control 88

creating baseline 90

deleting baseline 90

deleting entry 91

enabling or disabling 89

recommended usage 91

reverting to previous Version 91

View traffic 150

Virtual group

deleting entry 110

enabling or disabling entry 110

Virtual groups 110

adding entry 110

Virtual permissions

adding entry 106

changing conflict policy 107

deleting entry 107

editing entry 107

enabling or disabling entry 107

example entry 108

master user 109

moving entry 107

rule order and conflict policy 106

rules 106

shared directories 106

Virtual user password file 100

Virtual users 69

master 109

permission rules 106

permissions 105

adding entry 106

changing conflict policy 107

deleting entry 107

editing entry 107

enabling or disabling entry 107

example entry 108

moving entry 107

rule order and conflict policy 106

shared directories 106

