

Tekelec EAGLE[®] 5 SAS FTP-Based Table Retrieve Application (FTRA) User Guide

Table of Chapters

Table of Contents
List of Figures
List of Tables
List of Acronyms
User Guide Conventions
Overview
FTRA Initialization
Exit the FTRA
STP Connection Configuration Menu
Adding an STP Configuration Record
Displaying an Existing STP Configuration Record
Testing an STP Configuration Record
Modifying an Existing STP Configuration Record
Deleting an STP Configuration Record
Selecting the Current STP
Secure EAGLE 5 SAS Host Key Provisioning
FTP Server Configuration
Retrieve Database Tables from an STP
Command Line Interface
Updating Database Tables in the Selected STP
Update Tables Log Window
The System Log
About FTRA Window
SSH/SFTP Error Codes
Index

Tekelec EAGLE[®] 5
Signaling Application System

FTP-Based Table Retrieve Application (FTRA)
User Guide

910-0197-001 Revision B

December 2005



TEKELEC

Copyright© 2005 Tekelec.
All Rights Reserved
Printed in U.S.A.

Notice

Information in this documentation is subject to change without notice. Unauthorized use or copying of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

Trademarks

The Tekelec logo, EAGLE, G-Flex, G-Port, IP⁷, IP⁷Edge, IP⁷ Secure Gateway, and TALI are registered trademarks of Tekelec, Inc. TekServer is a trademark of Tekelec, Inc. All other trademarks are the property of their respective owners.

Patents

This product is covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:

5,008,929, 5,953,404, 6,167,129, 6,324,183, 6,327,350, 6,606,379, 6,639,981, 6,647,113, 6,662,017, 6,735,441, 6,745,041, 6,765,990, 6,795,546, 6,819,932, 6,836,477, 6,839,423, 6,885,872, 6,901,262, 6,914,973, 6,940,866, 6,944,184, 6,954,526, 6,954,794, 6,959,076, 6,965,592, 6,967,956, 6,968,048, 6,970,542

Ordering Information

Additional copies of this document can be ordered from:

Tekelec Network Signaling Group
Attention: Central Logistics
5200 Paramount Parkway
Morrisville, North Carolina, 27560

Or e-mail your request to CentralLogistics@tekelec.com.

Table of Contents

User Guide Conventions	1
Overview	1
Hardware and Software Requirements	2
Using the FTRA Application	4
Software Installation	4
FTRA Initialization	13
Exit the FTRA	14
STP Connection Configuration Menu	16
Adding an STP Configuration Record	20
Displaying an Existing STP Configuration Record	25
Testing an STP Configuration Record	33
Connectivity Test Log File Menu	34
Clearing the Connectivity Test Log Display	35
Printing the Connectivity Test Log	36
Saving the Connectivity Test Log to a File	37
Closing the Connectivity Test Log Window	38
Modifying an Existing STP Configuration Record	38
Deleting an STP Configuration Record	41
Selecting the Current STP	42
Secure EAGLE 5 SAS Host Key Provisioning	45
FTP Server Configuration	51
Retrieve Database Tables from an STP	56
Retrieve Tables Window	56
Retrieve Tables Log	69
Retrieve Tables Log File Menu	70
Clearing the Retrieve Tables Log Display	71
Printing the Retrieve Tables Log	72
Saving the Retrieve Tables Log to a File	73
Closing the Retrieve Tables Log Window	74

Command Line Interface	75
Updating Database Tables in the Selected STP	79
Validating a Command File	80
Update Validation Complete Window	85
Sending a Command File to the Selected STP	86
Stop Without Sending or Editing a Command File	87
Editing a Command File	87
Update Tables Log Window	90
File Menu in the Update Tables Log Window	94
Clearing the Update Tables Log Display	95
Printing the Update Tables Log	96
Saving the Update Tables Log to a File	97
Closing the Update Tables Log Window	98
The System Log	99
File Menu in the System Log Window	99
Clearing the System Log Display	100
Printing the System Log	101
Saving the System Log to a File	102
Closing the System Log Window	103
About FTRA Window	104
SSH/SFTP Error Codes	105
Troubleshooting Procedures	122
FTP Server Verification	122
SFTP /SSHD Server Verification	122
Connectivity Test – I	122
Connectivity Test - II	123
Network Outage Trouble Shooting	124
SSH/SFTP/SFTPD/SSHD Protocol Troubleshooting	125
Index	

List of Figures

Figure 1. FTP-Based Table Retrieve Application Window	13
Figure 2. File Menu in the FTP-Based Table Retrieve Application Window	14
Figure 3. Exit Confirmation Window	14
Figure 4. Exit Window	15
Figure 5. Edit Menu	16
Figure 6. STP Connection Configuration Menu Window (FTRA 1.0)	16
Figure 7. STP Connection Configuration Menu Window (FTRA 2.0 or greater)	17
Figure 8. Invalid STP Name Error Message	20
Figure 9. Adding an STP Configuration Record (FTRA 1.0)	21
Figure 10. Adding an STP Configuration Record (FTRA 2.0 or greater)	21
Figure 11. Invalid IP Address Error Message	22
Figure 12. Invalid STP User Name Error Message	22
Figure 13. Invalid STP Password Error Message	23
Figure 14. Invalid FTP User Name Error Message	23
Figure 15. Invalid FTP Password Error Message	24
Figure 16. STP Added Window	24
Figure 17. Selecting an STP Name from the STP Name Drop Down List (FTRA 1.0)	25
Figure 18. Selecting an STP Name from the STP Name Drop Down List (FTRA 2.0 or greater)	26
Figure 19. STP Name Selected from the STP Name Drop Down List (FTRA 1.0)	27
Figure 20. STP Name Selected from the STP Name Drop Down List (FTRA 2.0 or greater)	28
Figure 21. Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 1.0)	29
Figure 22. Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 2.0 or greater)	30
Figure 23. STP Configuration Record (FTRA 1.0)	31
Figure 24. STP Configuration Record (FTRA 2.0 or greater)	32

Figure 25. STP Name Does Not Exist Error Message	32
Figure 26. Connectivity Test Log Window with No Errors	33
Figure 27. Connectivity Test Log Window with Errors	34
Figure 28. Command Complete Connectivity Test Window	34
Figure 29. File Menu in the Connectivity Test Log Window	35
Figure 30. Print Window	36
Figure 31. Save Window	37
Figure 32. Saved File Confirmation Window	37
Figure 33. Modifying STP Configuration Record Parameters (FTRA 1.0)	39
Figure 34. Modifying STP Configuration Record Parameters (FTRA 2.0 or greater)	40
Figure 35. STP Data Modified Window	41
Figure 36. Modify Warning Window	41
Figure 37. Delete STP Window	42
Figure 38. STP Selection Change Window	43
Figure 39. Current STP Selected (FTRA 1.0)	43
Figure 40. Current STP Selected (FTRA 2.0 or greater)	44
Figure 41. IP Address Warning Message	45
Figure 42. FTP Server Configuration Menu in the FTP-Based Table Retrieve Application Window	51
Figure 43. FTP Server Configuration Menu Window	52
Figure 44. Invalid IP Address Error Message	53
Figure 45. Select Starting Directory Window	53
Figure 46. Invalid Subpath Window	54
Figure 47. FTP Server Configuration Example	55
Figure 48. FTP Server Data Set Window	55
Figure 49. GTT Warning Window	56
Figure 50. Retrieve Tables Window	57
Figure 51. Retrieve Table Log - Release Not Compatible Error	59
Figure 52. Commands Menu in the FTP-Based Table Retrieve Application Window	60
Figure 53. Selecting a Command	60
Figure 54. Selecting a Range of Commands	61
Figure 55. Selecting Multiple Commands	62
Figure 56. Adding a Command to the Selected Commands Box	62

List of Figures

Figure 57. Adding a Range of Commands to the Selected Commands Box	63
Figure 58. Adding Multiple Commands to Selected Commands Box	63
Figure 59. Command Selected to be Removed in the Selected Commands Box	64
Figure 60. Command Removed from the Selected Commands Box	65
Figure 61. Command Data Stored Window	65
Figure 62. Retrieving Database Tables from the Local Database	66
Figure 63. Retrieve Tables Log Window - Processing Retrieve Request	67
Figure 64. Command Complete Window Without Errors	68
Figure 65. Command Complete Window With Errors	68
Figure 66. Retrieve Tables Log Window without Errors	69
Figure 67. Retrieve Table Log with Errors	70
Figure 68. File Menu in the Retrieve Tables Log Window	71
Figure 69. View Menu	72
Figure 70. Print Window	72
Figure 71. Save Window	73
Figure 72. Saved File Confirmation Window	74
Figure 73. FTRA Windows Command Line Interface	76
Figure 74. FTRA UNIX Command Line Interface	76
Figure 75. FTRA Windows Task Scheduler	77
Figure 76. UNIX cron Job Scheduled using crontab	78
Figure 77. CRON FTRA Wrapper Script	78
Figure 78. Update Tables Window	79
Figure 79. Edit Menu	80
Figure 80. Update Tables with a Command File Selected	81
Figure 81. Select Window	82
Figure 82. Update Tables Window with a Command File Selected and Stop on Error Box Checked	83
Figure 83. Update Tables Log Window - Processing Retrieve Request	84
Figure 84. Must Enter Command Script File Name Message	84
Figure 85. Update Validation Complete Window without Errors	85

Figure 86. Update Validation Complete Window with Errors	86
Figure 87. Command Complete Window	86
Figure 88. Command File Editor Window	87
Figure 89. Command In progress, Cannot Close Window	88
Figure 90. Command File Editor with Invalid Command	88
Figure 91. File Menu in the Command File Editor Window	89
Figure 92. Command Complete Window	89
Figure 93. Update Tables Log Window after the Commit Command Completed	90
Figure 94. Update Tables Log	91
Figure 95. Update Tables Log with Stop on Error Box Checked in the Update Tables Window	92
Figure 96. Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window	93
Figure 97. File Menu in the Update Tables Log Window	95
Figure 98. View Menu	95
Figure 99. Print Window	96
Figure 100. Save Window	97
Figure 101. Saved Confirmation Window	98
Figure 102. System Log Window	99
Figure 103. File Menu in the System Log Window	100
Figure 104. View Menu	100
Figure 105. Print Window	101
Figure 106. Save Window	102
Figure 107. Saved Confirmation Window	103
Figure 108. Help Menu	104
Figure 109. Typical About FTRA Window	104

List of Tables

Table 1. FTP-Based Table Retrieve Application Menu Description	13
Table 2. STP Connection Configuration Menu Description	17
Table 3. FTP Server Configuration Menu Window Descriptions	52
Table 4. Select Starting Directory Window Descriptions	54
Table 5. Retrieve Tables Window Description	58
Table 6. Update Tables Window Description	80
Table 7. Select Window Descriptions	82
Table 8. Update Validation Complete Window Description	85
Table 9. FTP/SFTP/SSH Error Codes	105
Table 10. Generic Network Error Codes	119
Table 11. TCP Fault Tolerance Table for FTP/SFTP	125

List of Acronyms

CD.....	Compact Disc
CSV.....	Comma Separated Value
DOS.....	Disk Operating System
FTP.....	File Transfer Protocol
FTRA.....	FTP-Based Table Retrieve Application
GPSM.....	General Purpose Service Module
IP.....	Internet Protocol
IPSM.....	IP Services Module
JRE.....	Java™ 2 Runtime Environment
LAN.....	Local Area Network
MB.....	Megabyte
PC.....	Personal Computer
RAM.....	Random Access Memory
ROM.....	Read-only Memory
STP.....	Signal Transfer Point
TDM.....	Terminal Disk Module
UIM.....	Unsolicited Information Message

User Guide Conventions

In order to clearly differentiate between references to objects, actions, literal entries, and user-supplied information, the following conventions are used in this user guide:

- Menu selections and buttons are shown in bold, and the steps in a menu path are represented with ">". For example:

Select **Edit > STP Connection Configuration** from the menu.

The **Add** button is not enabled when the **STP Connection Configuration** menu opens.

- Commands and entries that must be entered exactly as shown in this document are shown in the 10 point Courier bold font. For example:

Using a text editor (such as Notepad) add the following lines to the AUTOEXEC.BAT file:

```
SET FTRA_HOME="C:\<download_directory>"  
SET JRE_HOME="C:\Program Files\Java\j2re1.4.0_01"
```

- User-specific information is shown in italics and enclosed in "<>". For example, the name of the folder you wish to use as the download directory in the previous example is shown as *<download_directory>*.

Overview

The FTP-Based Table Retrieve Application (FTRA) is designed in conjunction with the FTP Retrieve and Replace feature to transfer EAGLE 5 SAS database tables using an FTP session to a remote server for offline processing. The FTRA is a stand-alone application that interfaces with one or more STP's. Database tables can be retrieved from the EAGLE 5 SAS, using the EAGLE 5 SAS's retrieve commands. The output of these retrieve commands is converted to CSV (comma separated value) files. EAGLE 5 SAS commands in the form of a command file can be read into the FTRA where they are validated and sent to the selected STP. Logs are provided for event tracking and error message display.

The FTRA provides the following features through the use of a graphical user interface:

- STP Connection Configuration.
- STP Connectivity Test.
- FTP Server Configuration.
- Retrieving the EAGLE 5 SAS database tables with the results converted to CSV files.
- Automated or manual retrieval of database tables from multiple STPs with the command line interface. The results are converted to CSV files.

- Validation of the command files before being sent to the STP.
- Command file editing
- Viewing the log files for event tracking and error message display.

Hardware and Software Requirements

To run the offline application, a workstation on a Windows or Unix platform is required.

The Windows workstation requires that the following hardware and software are installed:

- Operating system – Windows[®] 98 or later
- Processor speed – Pentium III, 750 MHz or faster
- RAM – Minimum 128 MB
- Disk space – Minimum 500 MB plus 500 MB for each configured STP
- A CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java[™] 2 Runtime Environment (JRE) 1.4.0 or later.

The Unix workstation requires that the following hardware and software are installed:

- Operating system – Solaris 7 or later
- Processor speed – 500 MHz or faster
- RAM – Minimum 512 MB
- Disk space – Minimum 500 MB plus 500 MB for each configured STP
- CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java[™] 2 Runtime Environment (JRE) 1.4.0 or later

To configure the EAGLE 5 SAS for the FTP Retrieve and Replace feature, these requirements must be met:

- The IP User Interface feature is enabled and activated. The status of the IP User interface feature is shown in the EAGLE 5 SAS `rtrv-ctrl-feat` command output. If the IP User Interface feature is not enabled and activated, perform the “Activating Controlled Features” procedure in the *Database Administration Manual - System Management* and enable and activate the IP User Interface.
- Up to three IPSMs are installed and configured in the database. The IPSMs are shown with the entry IPSM in the `TYPE` column of the EAGLE 5 SAS `rtrv-card` output. If IPSMs are not shown in the `rtrv-card` output, perform the “Adding an IPSM” procedure in the *Database Administration Manual - System Management* and add the IPSMs.
- If the EAGLE 5 SAS is running release 30.2 or greater, and you wish to use a secure connection for the FTRA to EAGLE 5 SAS communication, make sure the Eagle OA&M IP Security Enhancements feature is enabled and activated. This can be verified by entering the `rtrv-ctrl-feat` command at the EAGLE 5 SAS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the “Activating the Eagle OA&M IP Security Enhancements Controlled Feature” procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature.
- GPSM-II cards must be installed in card locations 1113 and 1115. The GPSM-II cards in card locations 1113 and 1115 are shown with the entry GPSM in the `TYPE` column of the EAGLE 5 SAS `rtrv-card` output.
- TDMs, P/N 870-0774-10 or later, installed in card locations 1114 and 1116. Visually verify that these TDMs are installed in the EAGLE 5 SAS.



CAUTION: Never install or initialize MCAP cards in card locations 1113 and 1115 after GPSM-II cards have been installed and features that require GPSM-II cards have been provisioned. Attempting to initialize MCAP cards with features requiring GPSM-II cards will cause a system outage. Before replacing existing GPSM-II or MCAP cards (if the EAGLE 5 SAS currently has MCAP cards installed) in card locations 1113 or 1115, or replacing TDMs in card locations 1114 and 1116, contact the Customer Care Center at one of the following locations:

- Tekelec, UK

Phone: +44 1784 467 804

Fax: +44 1784 477 120

Email: ecsc@tekelec.com

- Tekelec, USA
Phone (within the continental US) 888-367-8552 (888-FOR-TKLC)
(outside the continental US) +1 919-460-2150.
Email: support@tekelec.com.

Using the FTRA Application

The following is an overview of the steps required to use the FTRA application.

1. Install the FTRA software on the PC (personal computer) – refer to the “Software Installation” section.
2. Start the FTRA application – refer to the “FTRA Initialization” section on page 13.
3. Select the current STP that the database tables will be retrieved from, or that the command files will be sent to – refer to the “Selecting the Current STP” procedure on page 42.

If you wish to use another STP, and that STP is not shown in the STP Name field of the **STP Connection Configuration** window, refer to the “Adding an STP Configuration Record” procedure on page 20 and add the new STP.

4. Before database tables can be retrieved from the EAGLE 5 SAS, or command files can be sent to the EAGLE 5 SAS, the FTP server configuration information for that EAGLE 5 SAS must be configured – refer to the “FTP Server Configuration” section on page 51.
5. To retrieve database tables from the selected STP, select the commands for the database tables you wish to retrieve in the Retrieve Tables Window – refer to the “Retrieve Database Tables from an STP” section on page 56.
6. To send commands to the selected STP, go to the Update Tables Window and select the command file to be sent, or create a command file – refer to the “Updating Database Tables in the Selected STP” section on page 79.
7. Exit the FTRA application – refer to the “Exit the FTRA” section on page 14.

Software Installation

The FTRA software can be installed locally or remotely through a LAN. The software installation can be accomplished in 5 to 10 minutes if the Java™ 2 Runtime Environment has been previously installed.

If the Java™ 2 Runtime Environment software has not been installed, you can install the Java™ 2 Runtime Environment software from the FTRA CD or download the Java™ 2 Runtime Environment software from Sun Microsystems' web site (for installation on the Unix platform). Should you decide to download the Java™ 2 Runtime Environment software from Sun Microsystems' web site, the software installation can take from 30 to 90 minutes, depending on the download speed of your internet connection. The FTRA is not providing service during this time. If the FTRA is being upgraded, it will not be necessary to recreate directories or environment variables that already exist.

If problems are encountered while installing the FTRA software, contact the Customer Care Center. Refer to page 3 for the contact information.

If the FTRA software is being installed for the first time, perform one of these procedures:

- "FTRA Software Installation on Windows"
- "FTRA Software Installation on Unix" on page 9

If the FTRA software is being upgraded from FTRA 1.0 to FTRA 2.x or greater, perform one of these procedures:

- "Upgrade to FTRA 2.x or Greater on Windows" on page 11
- "Upgrade to FTRA 2.x or Greater on Unix" on page 12

Procedure – FTRA Software Installation on Windows

1. Place the FTRA CD in the CD-ROM drive.

2. Install the Java™ 2 Runtime Environment SE V1.4.0 from the CD. Right-click on the **My Computer** icon on the desktop and select **Explore**. Select the CD-ROM drive. From Windows Explorer, double-click on the **j2re-1_4_0_01_windows-i586-1** icon and follow the InstallShield Wizard instructions.

3. Create a folder that the FTRA software will be installed into (the *<base_directory>*). The folder `C:\ftra` is recommended and used in the examples for this procedure, but you may place it wherever you would prefer.

NOTE: The path to this directory and the name of the directory cannot contain any blank spaces.

To create the *<base_directory>*, select the location of the *<base_directory>* from Windows Explorer. Select **File > New > Folder** and rename the new folder with the desired folder name.

For example, if the *<base_directory>* is to be `C:\ftra`, in Windows Explorer, select **C: Drive**. Select **File > New > Folder** and rename it `ftra`.

-
4. Extract the FTRA program files from the FTRA CD.

If you are installing FTRA 1.0, in the *<base_directory>*, create a folder named `bin`. From Windows Explorer, select the new *<base_directory>* (for example, `C:\ftra`). Select **File>New>Folder** and rename it to `bin`. Copy the file `ftra_install.exe` from the FTRA CD to the new `\bin` folder (for example, `C:\ftra\bin`). From Windows Explorer, double-click on the `ftra_install.exe` file. This will extract the program files into the new `\bin` folder created in this step.

For FTRA 2.x or greater, copy the `ftra_install.exe` file from the FTRA CD to the *<base_directory>*. The FTRA files can be extracted from the new directory (for example, `C:\ftra`). This can be done in one of two ways.

NOTE: Extract the FTRA file from the *<base_directory>* using only the command prompt. Do not use a Windows Explorer window for the extraction.

- a. From the Windows command line, the **MS-DOS** prompt, enter the command `ftra_install -d`.
- b. From the **Start** menu, select **Start > Run** and enter the path to the *<base_directory>* and the `ftra_install -d` command. For example, enter `C:\ftra\ftra_install -d`.

The `ftra_install -d` command creates all the required directories and extracts the program files.

5. Set the required system/user environment variables.

FTRA_HOME = C:\<base_directory> (typically, C:\ftra)

JRE_HOME = C:\Program Files\Java\j2re1.4.0_01
(typically, the folder where Java is installed)

NOTE: If the directory name has spaces, or is over eight characters in length, the DOS short name may be required to define the environment variable. For example, using the JRE_HOME environment variable above, the variable would be defined as "C:\Progra~1\Java\j2re1.4.0_01" (without the quotes) with the maximum eight characters for the directory name.

The method for defining environment variables differs between Windows systems.

- a. **Windows 2000 operating system** – Right-click the **My Computer** icon on the desktop and select **Properties**. In the **Advanced** tab, click **Environment Variables...**
Click **New...** under User variables, and enter the variable name and value.
- b. **Windows NT[®] operating system** – Right-click the **My Computer** icon on the desktop and select **Properties**. In the **Environment** tab, select any user environment variable, enter the new variable name and value, and click **Set**.
- c. **Windows 98 operating system** – Using a text editor (such as Notepad) append the following lines to the AUTOEXEC.BAT file:
SET FTRA_HOME="C:\<base_directory>"
SET JRE_HOME="C:\Program Files\Java\j2re1.4.0_01"

-
6. Create a shortcut from the C:\<base_directory>\bin\ftra.bat file to the desktop by right clicking on the **ftra.bat** icon and dragging it to the desktop.

NOTE: On multi-user systems, the shortcut should be placed in the **Default User** or **All Users** desktop folder in order to make it available to all users.

Procedure – Java™ 2 Runtime Environment Installation from the FTRA CD

1. Place the FTRA CD in the CD-ROM drive.

2. Install the Java™ 2 Runtime Environment, SE V1.4.0 software from the FTRA CD.

To install the Java™ 2 Runtime Environment, SE V1.4.0 software from the FTRA CD, open **FileManager** and go to the CDROM drive. From **FileManager**, double-click on the `j2re-1_4_1_01-solaris-sparc.sh` file.

3. Log in to the Unix workstation with root access priviledges.
-

4. Go to the `/usr` directory by entering this command.

```
cd /usr
```

5. Verify that you are in the `/usr` directory by entering this command.

```
pwd
```

6. Copy the Java installation file from the FTRA CD to the `/usr` directory by entering this command.

```
cp <path to the FTRA CD>/j2re1_4_0_01-solsparc.sh
```

NOTE: You should be in the `/usr` directory, and there should be a directory named `jr2re-1_4_1_01-solaris-sparc.sh` (use the `pwd` and `ls` commands to verify that the `jr2re-1_4_1_01-solaris-sparc.sh` directory is in the `/usr` directory).

7. Create a symbolic link to Java by entering this command.

```
ln -s j2re1_4_0_01 java
```

NOTE: If a Java link already exists in the directory (use the `ls -l` command to verify that the link exists), remove the existing link first by entering this command, `rm java`.

8. Verify that the symbolic link was created by entering this command.

```
ls -l /usr/java
```

After you have completed this procedure, perform the “FTRA Software Installation on Unix” procedure on page 9.

Procedure – Java™ 2 Runtime Environment Installation from Sun Microsystem's Website

To install the Java™ 2 Runtime Environment (JRE) 1.4.0 from Sun Microsystem's web site, enter the following address into your web browser and follow the product installation instructions.

```
http://java.sun.com/j2se/1.4/jre/install-solaris.html
```

Procedure FTRA Software Installation on Unix

NOTE: Before performing this procedure, make sure the Java™ 2 Runtime Environment software has been installed by performing either the "Java™ 2 Runtime Environment Installation from the FTRA CD" procedure on page 8 or the "Java™ 2 Runtime Environment Installation from Sun Microsystem's Website" procedure on page 9.

1. Log into the workstation as **root**.
2. Set the required environment variables by adding the following lines to the user's **.cshrc** file:

```
setenv FTRA_HOME '/FTRA'  
setenv JRE_HOME '/usr/j2re1.4.0_01'
```

3. Create an FTRA directory in by entering this command.

```
mkdir /FTRA
```

4. Go into this newly created directory and verify that this directory is empty by entering these commands.

```
cd /FTRA  
ls -l
```

5. Copy the FTRA file (**ftra_install.tar**) from the CD to this directory by entering this command.

```
cp <path to the ftra_install.tar file on the FTRA CD> /FTRA
```

6. The FTRA file (**ftra_install.tar**) is zipped on the FTRA CD and will need to be expanded after the FTRA file is copied to the FTRA directory. Enter this command to expand the file.

```
tar -xvf ftra_install.tar
```

7. View the directory and verify that all the files were expanded into the FTRA directory by entering this command.

```
ls -l
```

8. Create a global user account for FTRA by entering these commands.

```
useradd -d /export/home/<username>/-s/sbin/csh <username>
passwd <username>
```

9. Create a home directory for the user created in step 8 by entering this command.

```
mkdir /export/home/<user>
```

10. Change the ownership of the directory created in step 9 to the username added in step 8 by performing this command.

```
chown <username added in step 8>
```

11. Exit the workstation as **root** by entering this command.

```
su -newusr; cd
```

12. Go to the directory created in step 9 by entering this command.

```
cd /<directory name created in step 9>
```

13. Verify the correct user by entering the following command in Shell.

```
echo $USER
```

14. Verify that the Shell is CSH by entering this command.

```
echo $SHELL
```

If you are not in Shell, enter the command **csh**.

15. Create a **.cshrc** file by entering this command.

```
cat .cshrc
setenv FTRA_HOME '/FTRA'
setenv JRE_HOME '/usr/j2rel.4.0_01'
```

16. Go to the home directory and list the `.cshrc` file by entering these commands.

```
cd
ls -al .cshrc
```

17. Make sure you are in the home directory of the current user by entering this command.

```
pwd
```

18. Source the runtime environment variables by entering these commands.

```
cd
source .cshrc
```

19. Verify that the environment variable locations match what was specified in step 15, without the trailing slash, by entering these commands.

```
echo $FTRA_HOME; echo $JRE_HOME
```

Example output: `FTRA_HOME= /FTRA`

`JRE_HOME=/usr/j2rel.4.0_01`

20. To launch the FTRA from the command line, enter this command.

```
$FTRA_HOME/bin/ftra
```

Procedure – Upgrade to FTRA 2.x or Greater on Windows

1. Place the FTRA CD in the CD-ROM drive.
 2. From Windows Explorer, copy the `ftra_install.exe` file from the FTRA CD to the existing folder containing the FTRA software. For details on the folder containing the FTRA software, see step 3 on page 6.
-

3. Extract the FTRA program files from the FTRA CD using only the command prompt. Do not use a Windows Explorer window for the extraction. From the Windows command line, the **MS-DOS** prompt, enter the command **ftra_install -d**. The **ftra_install -d** command creates all the required directories and extracts the program files. During the execution of the **ftra_install -d** command, you will be asked if you wish to overwrite an existing file. Answer **yes** for the upgrade to continue. When the **ftra_install -d** command has finished executing, the FTRA software has been installed.
-
4. Start the FTRA software. See the “FTRA Initialization” section on page 13 for more information on starting the FTRA software. The existing STP Connection Configuration data will automatically be converted during the FTRA system initialization.
-

Procedure – Upgrade to FTRA 2.x or Greater on Unix

1. Place the FTRA CD in the CD-ROM drive.
-
2. From **FileManager**, copy the **ftra_install.tar** file from the FTRA CD to the existing directory containing the FTRA software by entering this command.

```
cp <path to the ftra_install.tar file on the FTRA CD> /FTRA
```
-
3. From **FileManager**, right-click on the **ftra_install.tar** file that was copied from the FTRA CD, not the **ftra_install.tar** file on the FTRA CD, and select **Archive Unpack**. This will create the sub-directories and extract the program files into the existing directory containing the FTRA software.
NOTE: The Archive Unpack function is only available when using the CDE (Common Desktop Environment) X-window File Manager. If the CDE is not being used, the Unix tar command should be used to extract the program files. Please refer to the man pages for the tar command for more information about using the tar command.
When the extraction of the FTRA program files has completed, the FTRA software has been installed.
-
4. Start the FTRA software. See the “FTRA Initialization” section on page 13 for more information on starting the FTRA software. The existing STP Connection Configuration data will automatically be converted during the FTRA system initialization.
-

FTRA Initialization

To start the FTRA, double-click the FTRA icon on the desktop. When the application starts, the **FTP-Based Table Retrieve Application** window is displayed. See Figure 1. The **Initializing** window opens and displays the message “Initializing, please wait.....” until the initialization process has been completed.

Figure 1. FTP-Based Table Retrieve Application Window



Table 1 shows the description of the menus in the **FTP-Based Table Retrieve Application** window.

Table 1. FTP-Based Table Retrieve Application Menu Description

Item	Description
File	Selects the Exit menu.
Edit	Selects the STP Connection Configuration menu, the FTP Server Configuration menu, or the Commands menu
View	Selects these logs: <ul style="list-style-type: none"> • The Retrieve Tables Log • The Update Tables Log • The System Log.
Help	Selects the About FTRA window.

Exit the FTRA

To close the **FTP-Based Table Retrieve Application** window and exit the FTRA, either select **File > Exit** from the **File** menu, see Figure 2, or click the close window button in the upper right hand corner of the window.

Figure 2. File Menu in the FTP-Based Table Retrieve Application Window

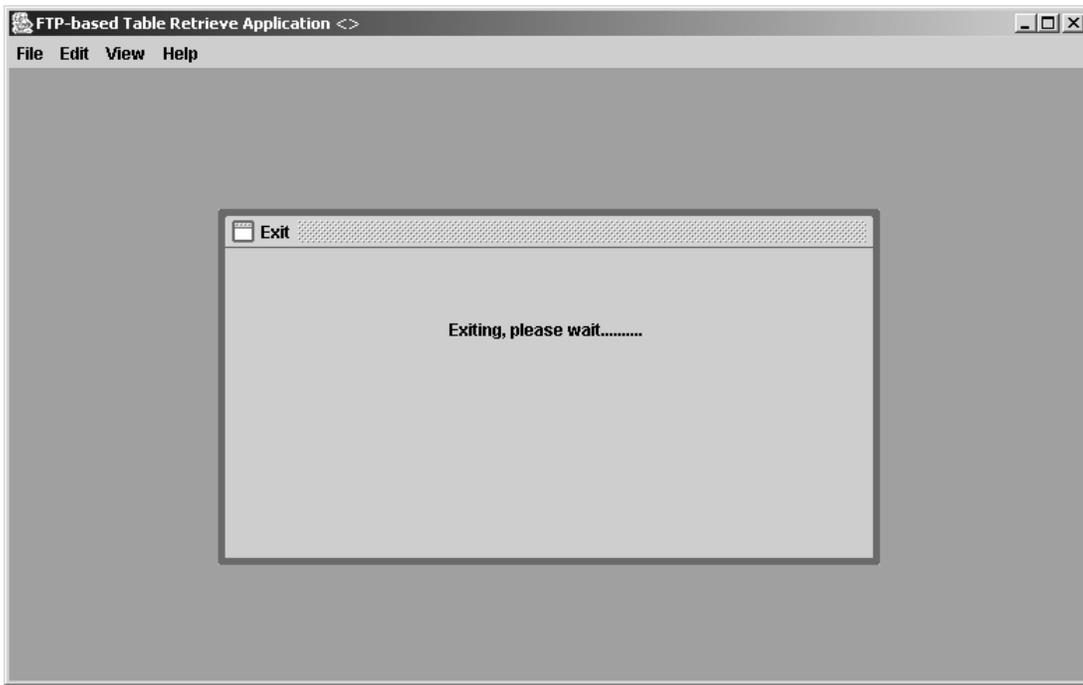


The **Exit?** confirmation window (see Figure 3) opens with “You are about to exit. Continue?” Click **OK** to exit and close the application. The **Exit** window (see Figure 4 on page 15) is displayed until the Exit process is completed. To cancel the exit and resume using the application, click **Cancel**.

Figure 3. Exit Confirmation Window



Figure 4. Exit Window



STP Connection Configuration Menu

Before database tables can be retrieved from an STP, or command files can be sent to an STP, the STP must be defined as an STP configuration record in the STP Connection Configuration database. The STP configuration record is configured and selected using the **STP Connection Configuration Menu** window.

The **STP Connection Configuration Menu** window is displayed by selecting **Edit > STP Connection Configuration**. See Figure 5.

Figure 5. Edit Menu



The **STP Connection Configuration Menu** window, see Figure 6 (FTRA 1.0) or Figure 7 on page 17 (FTRA 2.0 or greater), can be used also to delete and modify an STP configuration record.

Figure 6. STP Connection Configuration Menu Window (FTRA 1.0)

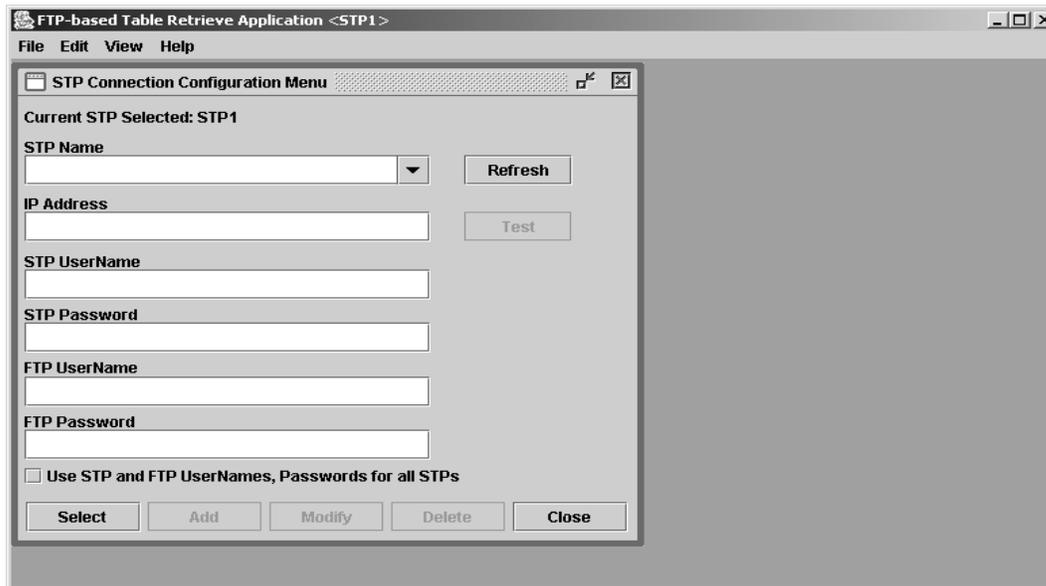


Figure 7. STP Connection Configuration Menu Window (FTRA 2.0 or greater)

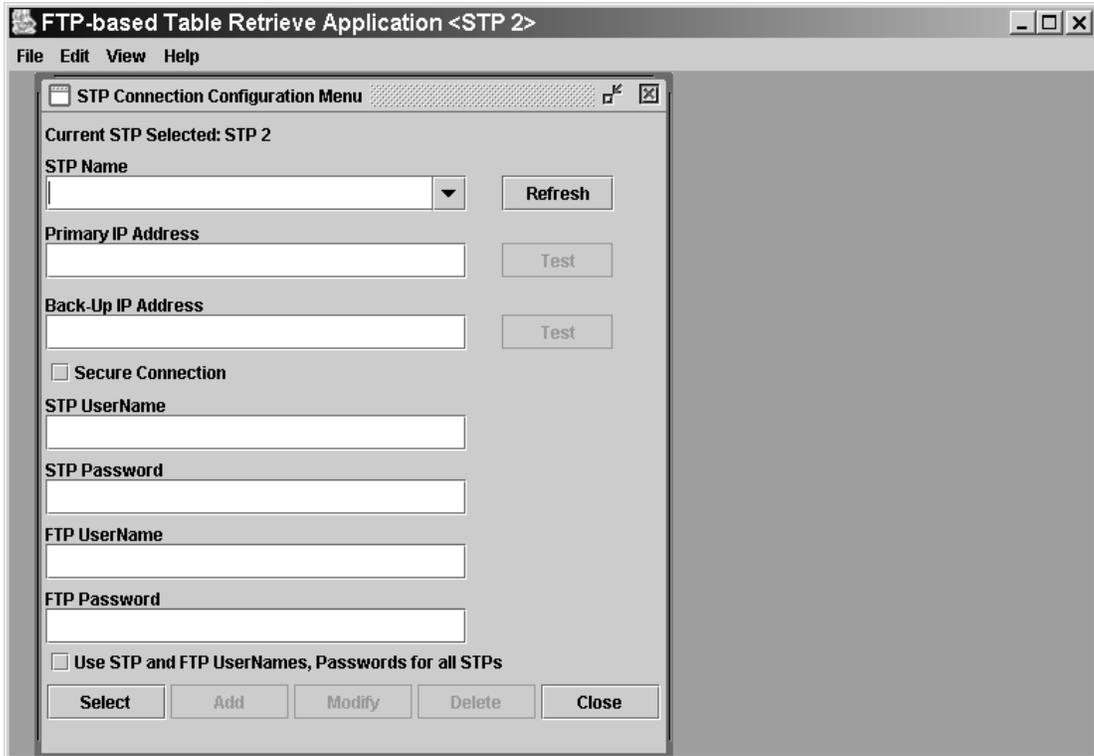


Table 2 shows the description of the fields, buttons, and boxes in the **STP Connection Configuration Menu** window.

Table 2. STP Connection Configuration Menu Description

Item	Description
Fields	
STP Name	Contains the STP Names. The STP name must contain at least one alphanumeric character and a maximum of 64 upper-case alphanumeric characters. The STP Name will always be entered in uppercase regardless of the Caps Lock key setting on your keyboard. This field also provides a drop down list for selecting stored STP configuration records.
IP Address (FTRA 1.0 only)	The IP address of the associated STP (used for telnet sessions). The IP address is the IP address of an IPSM in the associated EAGLE 5 SAS.
Primary IP Address (FTRA 2.0 or greater)	The primary IP address of the associated STP (used for telnet sessions). The FTRA uses this IP address first when connecting to the STP. The primary IP address is the IP address of an IPSM in the associated EAGLE 5 SAS.

Table 2. STP Connection Configuration Menu Description

Item	Description
Backup IP Address (FTRA 2.0 or greater)	The backup IP address of the associated STP (used for telnet sessions). The FTRA uses this IP address when the connection using the primary IP address fails. The backup IP address should be the IP address of another IPSM in the same EAGLE 5 SAS.
STP UserName	The user name assigned to the user by the STP system administrator (used for telnet sessions).
STP Password	The password assigned to the user by the STP system administrator (used for telnet sessions).
FTP UserName	The FTP user name assigned to the user by the administrator (used for FTP). Any FTP user name with symbols must be enclosed within double quotation marks (for example, to specify the FTP user name <code>mylogin#1</code> , you would enter <code>"mylogin#1"</code>).
FTP Password	The FTP password assigned to the user by the administrator (used for FTP).
Buttons	
Refresh	Displays the data of the STP configuration record typed in the STP Name field. If an STP name is selected from the STP Name drop down list, the data fields are automatically displayed.
Test	Verifies that the FTRA can successfully connect and login to the EAGLE 5 SAS through an available telnet terminal at the specified IP address. For FTRA 1.0, the STP Connection Configuration Menu window has only one Test button. For FTRA 2.0 or greater, the STP Connection Configuration Menu window has two Test buttons, one for the Primary IP address, and one for the Backup IP address.
Select	Selects the displayed STP name to be connected to the FTRA. The STP Selection Change window opens to verify if you want to proceed.
Add	Adds a newly entered STP configuration record and associated data to the STP Connection Configuration database.
Modify	Modifies the fields of the displayed STP configuration record.
Delete	Deletes the displayed STP configuration record and associated data from the STP Connection Configuration database.
Close	Closes the STP Connection Configuration Menu window.

Table 2. STP Connection Configuration Menu Description

Item	Description
Boxes	
Secure Connection (FTRA 2.0 or greater)	<p>Enables the FTRA to use a secure IP connection to the STP.</p> <p>To use a secure connection for the FTRA to EAGLE 5 SAS communication, make sure the EAGLE 5 SAS is running release 30.2 or greater and that the Eagle OA&M IP Security Enhancements feature is enabled and activated. This can be verified by entering the <code>rtrv-ctrl-feat</code> command at the EAGLE 5 SAS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the "Activating the Eagle OA&M IP Security Enhancements Controlled Feature" procedure in the <i>Database Administration Manual - System Management</i> and enable and activate the Eagle OA&M IP Security Enhancements feature.</p> <p>NOTE: This box should be unchecked if the Eagle OA&M IP Security Enhancements feature is not enabled or activated, and will not be enabled or activated.</p> <p>If this box is checked, the public key fingerprint for the EAGLE 5 SAS specified in this window must be installed onto the FTRA for the FTRA and the specified EAGLE 5 SAS to use a secure connection. After this STP is added to the STP Connection Configuration database, add the public key fingerprint to the FTRA by performing the "Secure EAGLE 5 SAS Host Key Provisioning" procedure on page 45.</p>
Use STP and FTP UserNames, Passwords for all STPs Box	<p>All the STP and FTP user names and passwords of all the provisioned STPs are changed to the user name and password of the displayed STP name. This change occurs only when the Add or Modify buttons are used.</p>

Adding an STP Configuration Record

Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 5 on page 16. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 16. The **Add** button is not enabled when the **STP Connection Configuration Menu** window opens.
2. Enter the STP name in the **STP Name** field of the **STP Connection Configuration Menu** window. The STP name must contain at least one alphanumeric character, with a maximum of 64 upper-case characters (alphanumeric, letters and numbers, and spaces). See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater). The STP Name will always be entered in uppercase regardless of the Caps Lock key setting on your keyboard.

If characters other than alphanumeric characters or spaces are included in the STP name, the **Invalid STP Name** warning window is displayed. See Figure 8. If the **Invalid STP Name** window appears, click **OK**, and reenter the STP name in the **STP Name** field with the correct characters.

NOTE: When the new STP name is entered into the **STP Name** field, the **Add** button is enabled. If the STP name matches an existing STP name in the **STP Connection Configuration** database, the **Add** button is disabled. If you wish to display the existing STP names, go to the “**Displaying an Existing STP Configuration Record**” procedure on page 25.

NOTE: If the “**Use STP and FTP UserNames and Passwords for all STPs**” box is checked when the **Add** button is clicked, all the user names and passwords for all provisioned STP Names are changed to those of the added STP name.

NOTE: Existing STP configuration records can be changed. Go to the “**Modifying an Existing STP Configuration Record**” procedure on page 38 to change an existing STP configuration record.

Figure 8. Invalid STP Name Error Message

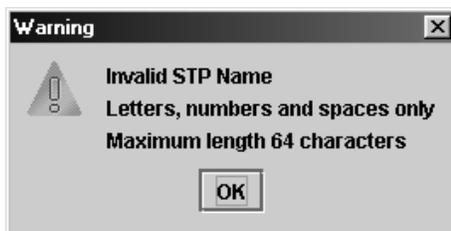


Figure 9. Adding an STP Configuration Record (FTRA 1.0)

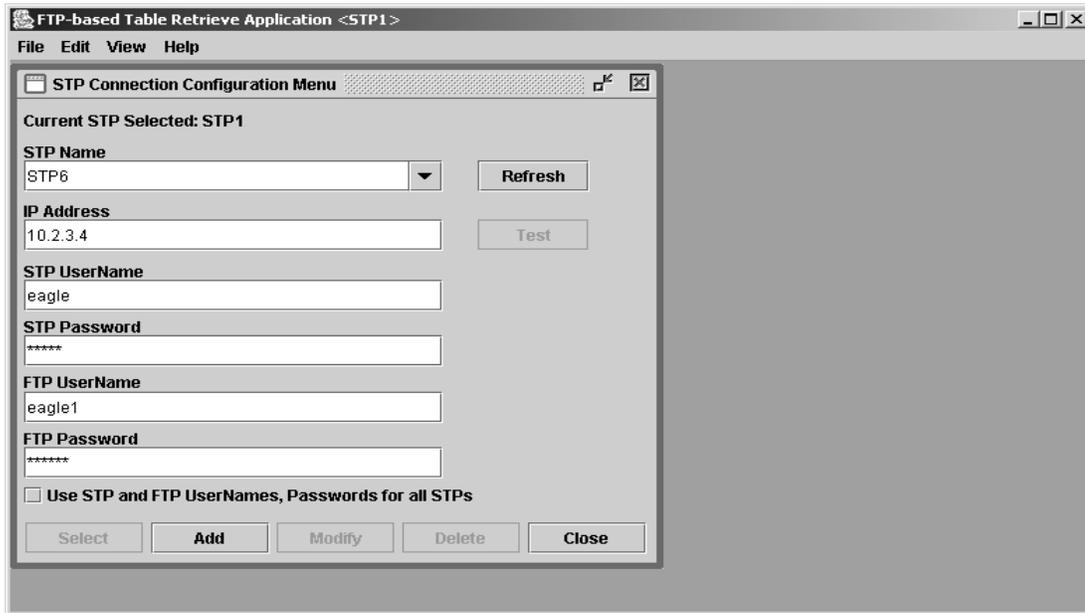
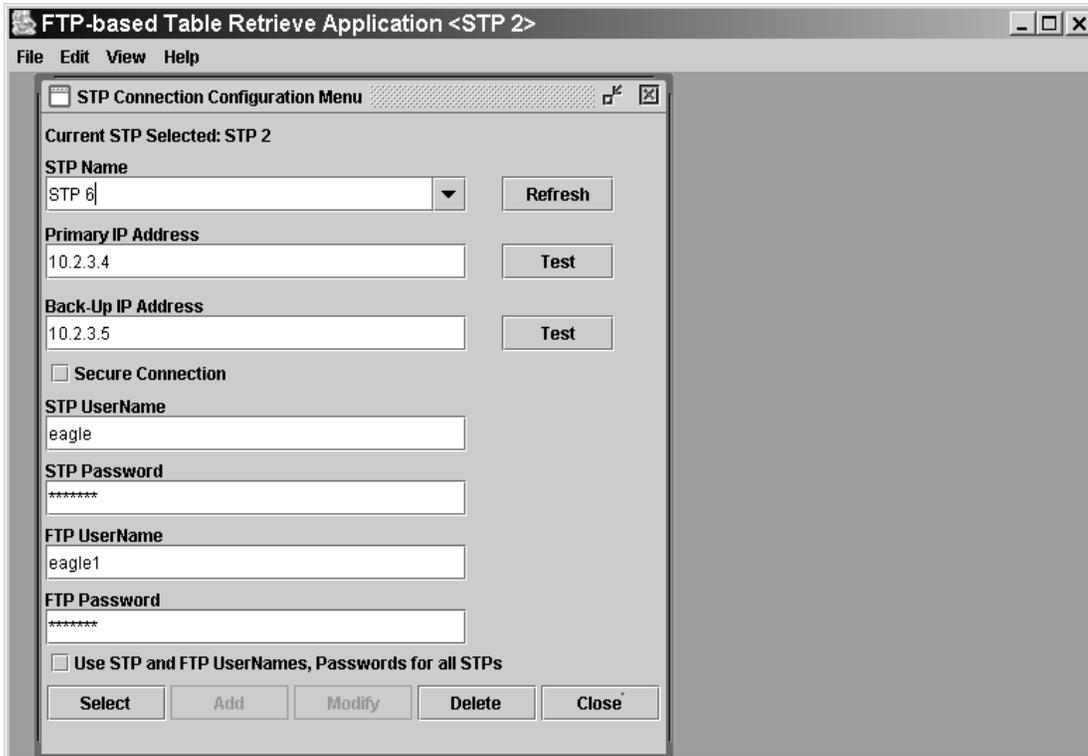


Figure 10. Adding an STP Configuration Record (FTRA 2.0 or greater)



3. Enter the IP address of the STP in the **IP Address** field (FTRA 1.0). If the FTRA is running version 2.0 or greater, enter the IP address you wish to use to connect to the STP in the **Primary IP Address** field, and a backup IP address in the **Backup IP Address** field. See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater).



CAUTION: If the backup IP address is not entered for FTRAs running 2.0 or greater, the FTRA will not be able to connect to the STP when the connection to the STP using the primary IP address fails. It is recommended that you specify a backup IP address for the STP.

If the format of the IP address (FTRA 1.0), or the primary and backup IP addresses (FTRA 2.0 or greater) is not entered correctly, the **Invalid IP Address** warning window is displayed. See Figure 11. If the **Invalid IP Address** window appears, click **OK**, and reenter the IP address in the **IP Address** field (FTRA 1.0) or the primary or backup IP addresses (FTRA 2.0 or greater) in the **Primary IP Address** or **Backup IP Address** fields in the correct format.

Figure 11. Invalid IP Address Error Message



4. Enter the STP user name for this STP in the **STP UserName** field. The user name is assigned to the user by the STP system administrator for telnet sessions. See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater). If the format of the STP user name is not correct, the **Invalid STP User Name** warning window is displayed. See Figure 12. If the **Invalid STP User Name** window appears, click **OK**, and re-enter the STP user name in the **STP UserName** field.

Figure 12. Invalid STP User Name Error Message



5. Enter the STP password for this STP in the **STP Password** field. The password is assigned to the user by the EAGLE 5 SAS system administrator for telnet sessions. See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater). If the format of the STP password is not correct, the **Invalid STP Password** warning window is displayed. See Figure 13. If the **Invalid STP Password** window appears, click **OK**, and re-enter the STP password in the **STP Password** field.

NOTE: The **STP Password** field does not check for invalid EAGLE 5 SAS passwords. The passwords are validated by the EAGLE 5 SAS when the FTRA attempts a connection to the EAGLE 5 SAS. The requirements for the format of EAGLE 5 SAS passwords is shown in the output of the EAGLE 5 SAS's `rtrv-secu-dflt` command.

Figure 13. Invalid STP Password Error Message



-
6. Enter the FTP user name assigned by the FTP server administrator in the **FTP UserName** field. See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater). Any FTP user name with symbols must be enclosed within double quotation marks (for example, to specify the FTP user name `mylogin#1`, you would enter `"mylogin#1"`). If the format of the FTP user name is not correct, the **Invalid FTP User Name** warning window is displayed. See Figure 14. If the **Invalid FTP User Name** window appears, click **OK**, and re-enter the FTP user name in the **FTP UserName** field.

NOTE: Any firewall between the FTRA and the FTP server configured in the **FTP Server Configuration Menu** window (Figure 43 on page 52), must allow FTPs to the IP address specified in the **FTP Server Configuration Menu** window.

Figure 14. Invalid FTP User Name Error Message



7. Enter the FTP password assigned by the FTP server administrator in the **FTP Password** field. See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater). If the format of the STP user name is not correct, the **Invalid FTP Password** warning window is displayed. See Figure 15. If the **Invalid FTP Password** window appears, click **OK**, and re-enter the FTP password in the **FTP Password** field.

Figure 15. Invalid FTP Password Error Message



NOTE: If you are running FTRA 1.0, or running FTRA 2.0 or greater and not enabling a secure connection to the STP, skip this step and go to step 9.

8. To enable a secure connection between the FTRA and the STP being added in this procedure, click in the **Secure Connection** box.

Make sure the EAGLE 5 SAS is running release 30.2 or greater and that the Eagle OA&M IP Security Enhancements feature is enabled and activated. This can be verified by entering the `rtrv-ctrl-feat` command at the EAGLE 5 SAS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the "Activating the Eagle OA&M IP Security Enhancements Controlled Feature" procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature.

9. Click the **Add** button. See Figure 9 on page 21 (FTRA 1.0) or Figure 10 on page 21 (FTRA 2.0 or greater). The newly entered STP Name and associated data is added to the STP Connection Configuration database, and the **STP Added** window (Figure 16) is displayed. Click **OK** to continue.

Figure 16. STP Added Window



10. Verify the addition of the new STP name. See the "Displaying an Existing STP Configuration Record" procedure on page 25.
-

Displaying an Existing STP Configuration Record

An existing STP configuration record can be displayed by either selecting the STP Name from the STP Name drop down list, or by re-entering the STP name in the **STP Name** field in the **STP Connection Configuration Menu** window and clicking the **Refresh** button.

To Use the STP Name Drop Down List

Procedure

1. In the **STP Connection Configuration Menu** window, click on the **STP Name** drop down list. The **STP Name** drop down list opens. Move the cursor to the STP name to be selected. Click on the desired STP name in the drop down list. See Figure 17 (FTRA 1.0) or Figure 18 on page 26 (FTRA 2.0 or greater).

Figure 17. Selecting an STP Name from the STP Name Drop Down List (FTRA 1.0)

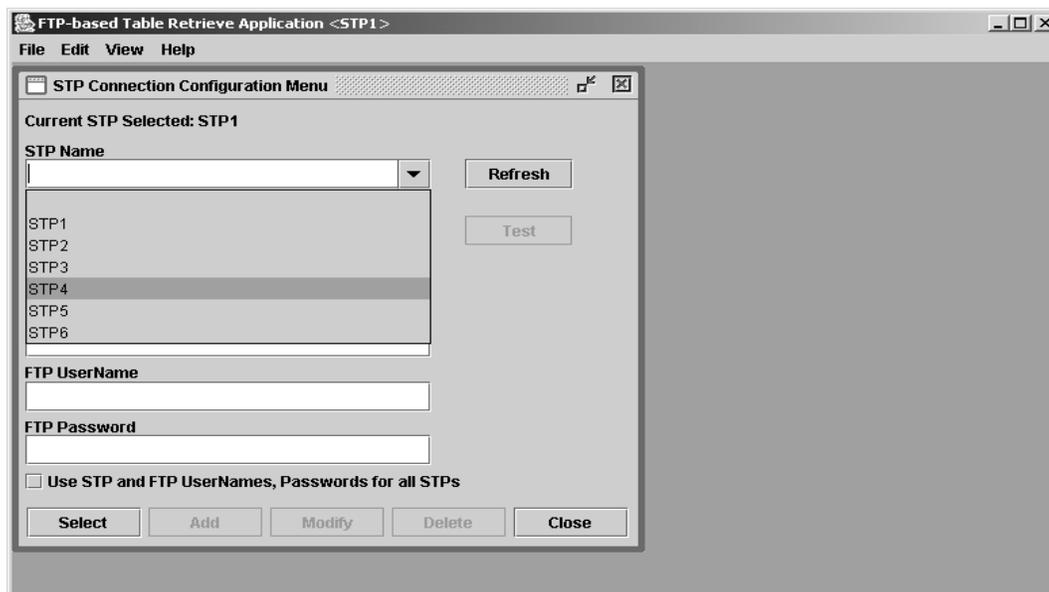
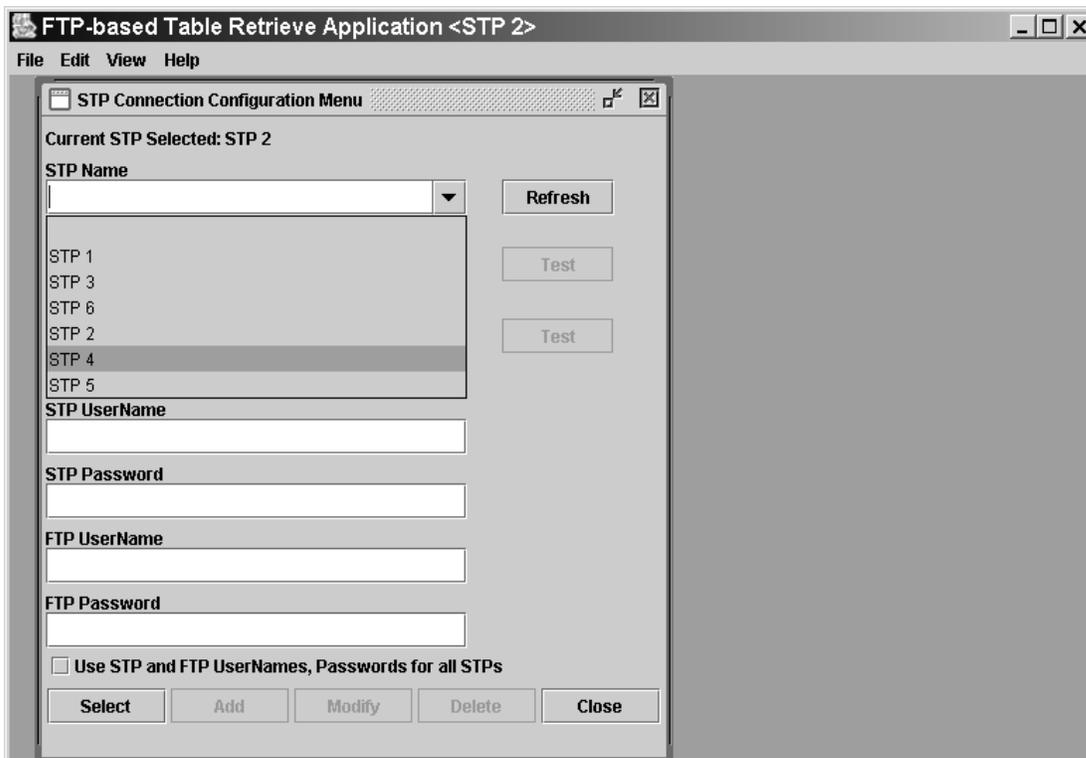


Figure 18. Selecting an STP Name from the STP Name Drop Down List (FTRA 2.0 or greater)



2. When the STP name is selected in step 1, the STP configuration record for the specified STP is displayed. See Figure 19 (FTRA 1.0) or Figure 20 on page 28 (FTRA 2.0 or greater). The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

Figure 19. STP Name Selected from the STP Name Drop Down List (FTRA 1.0)

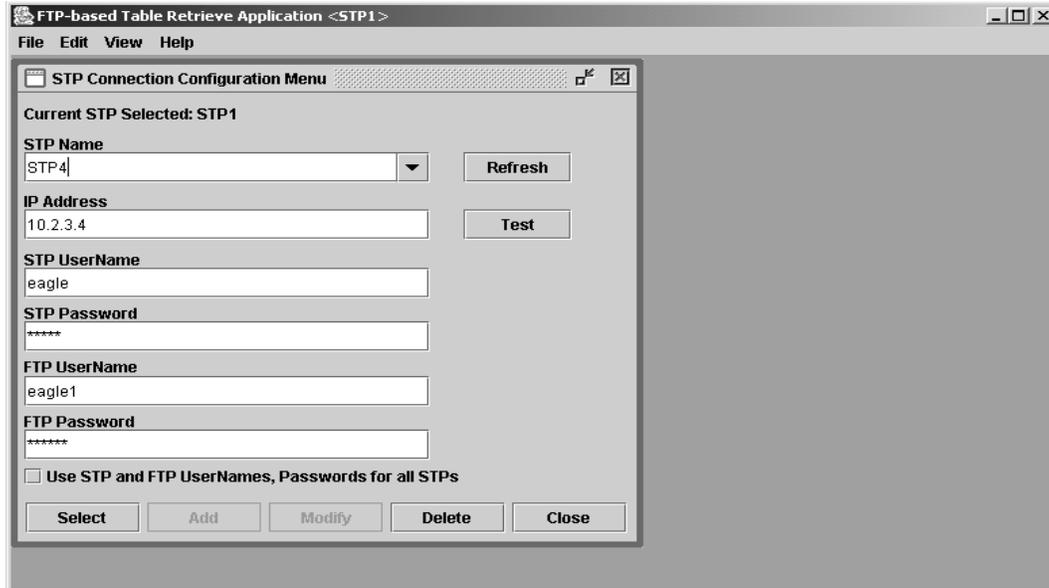
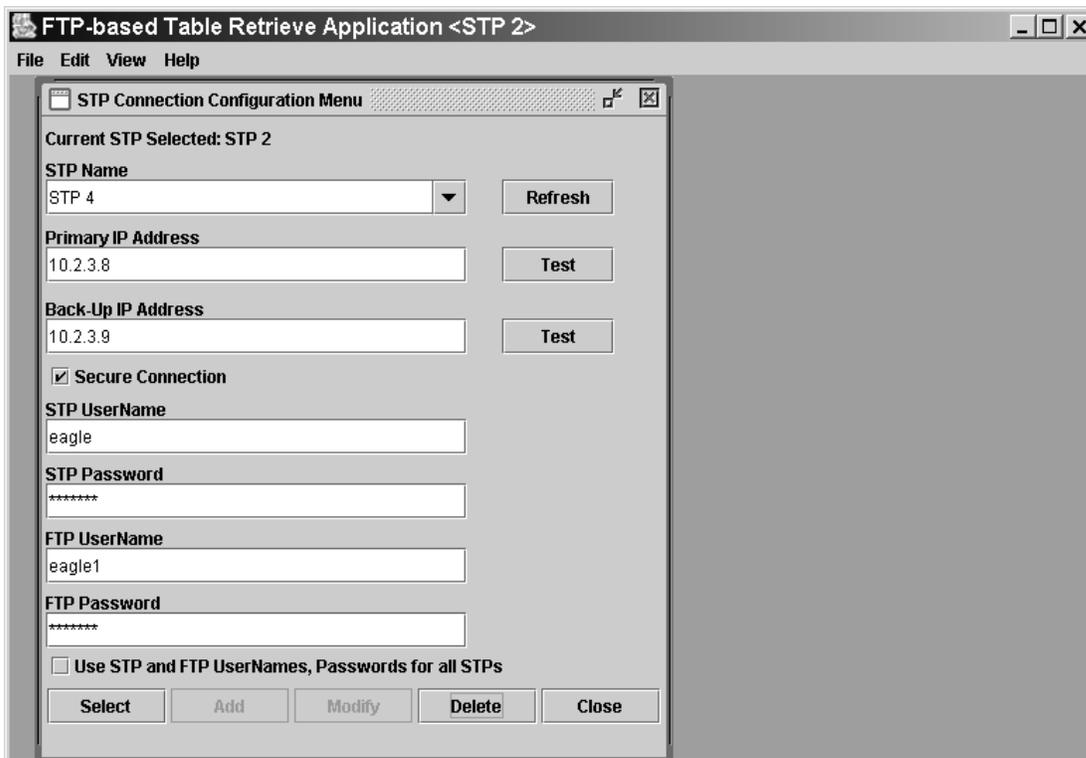


Figure 20. STP Name Selected from the STP Name Drop Down List (FTRA 2.0 or greater)



To Enter the STP Name

Procedure

1. Type the STP name in the **STP Name** field in the **STP Connection Configuration Menu** window. See Figure 21 (FTRA 1.0) or Figure 22 on page 30 (FTRA 2.0 or greater). The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

Figure 21. Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 1.0)

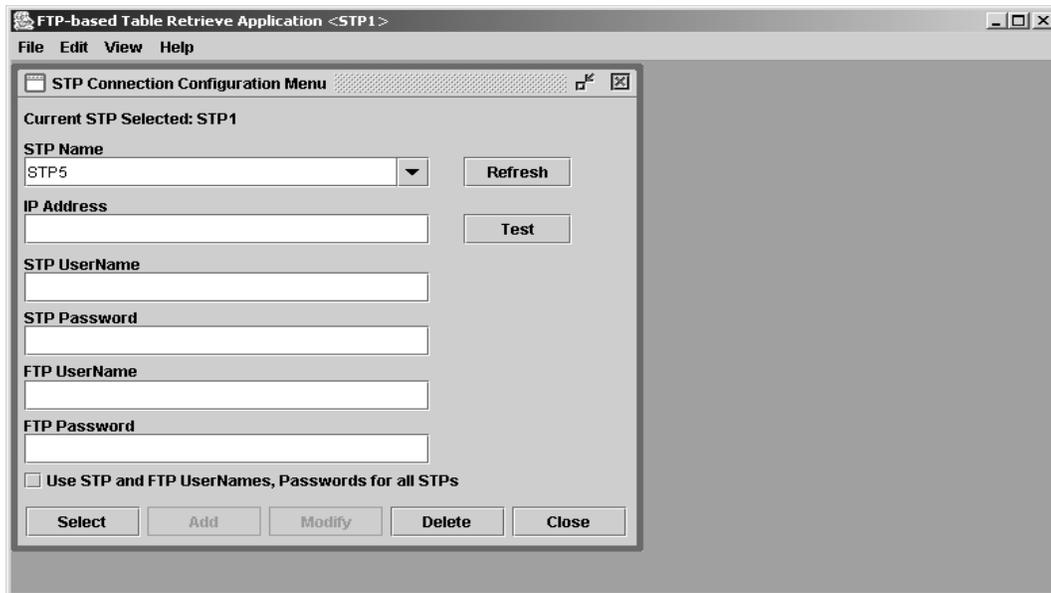
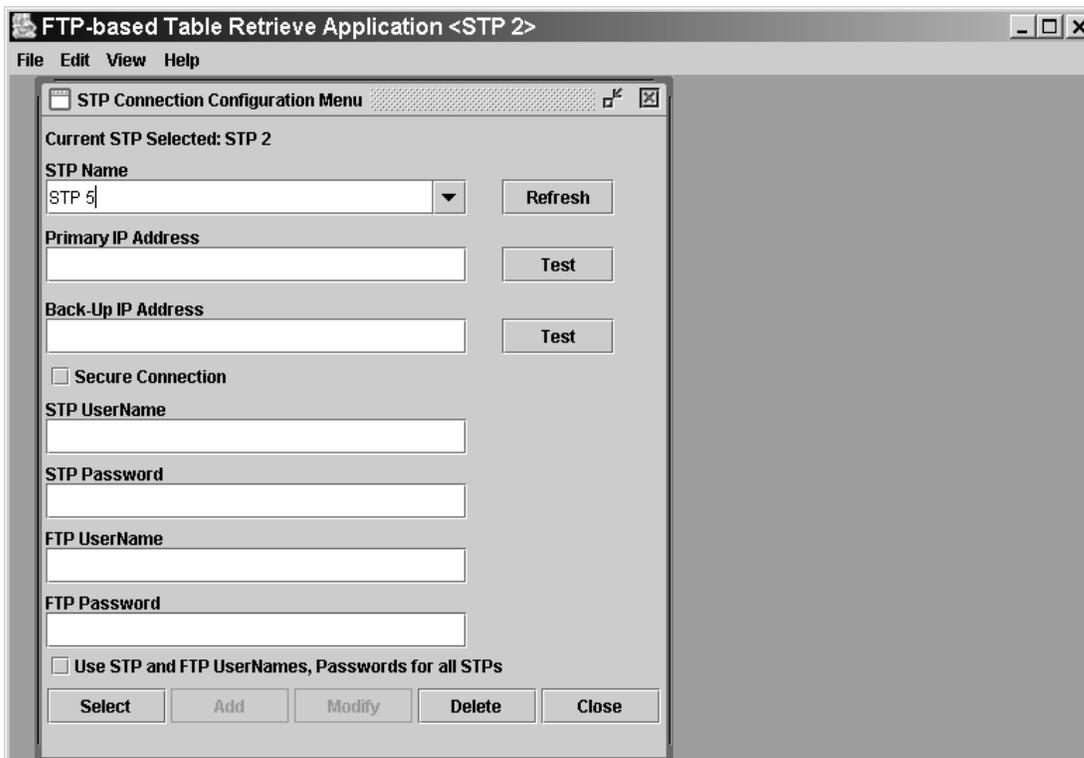


Figure 22. Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 2.0 or greater)



2. Click the **Refresh** button. The STP configuration record for the specified STP is displayed. See Figure 23 (FTRA 1.0) or Figure 24 on page 32 (FTRA 2.0 or greater).

Figure 23. STP Configuration Record (FTRA 1.0)

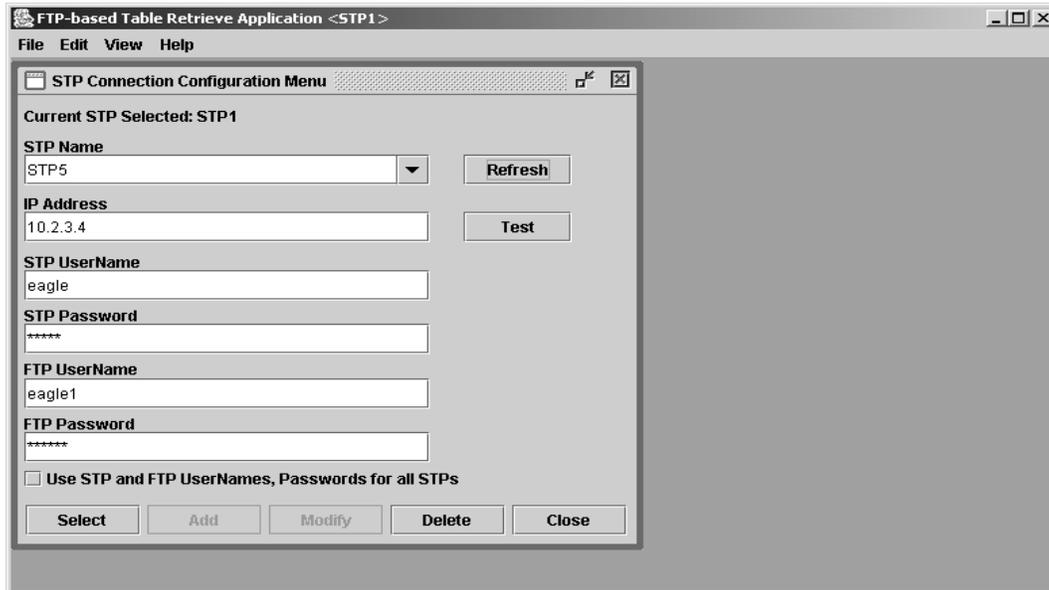
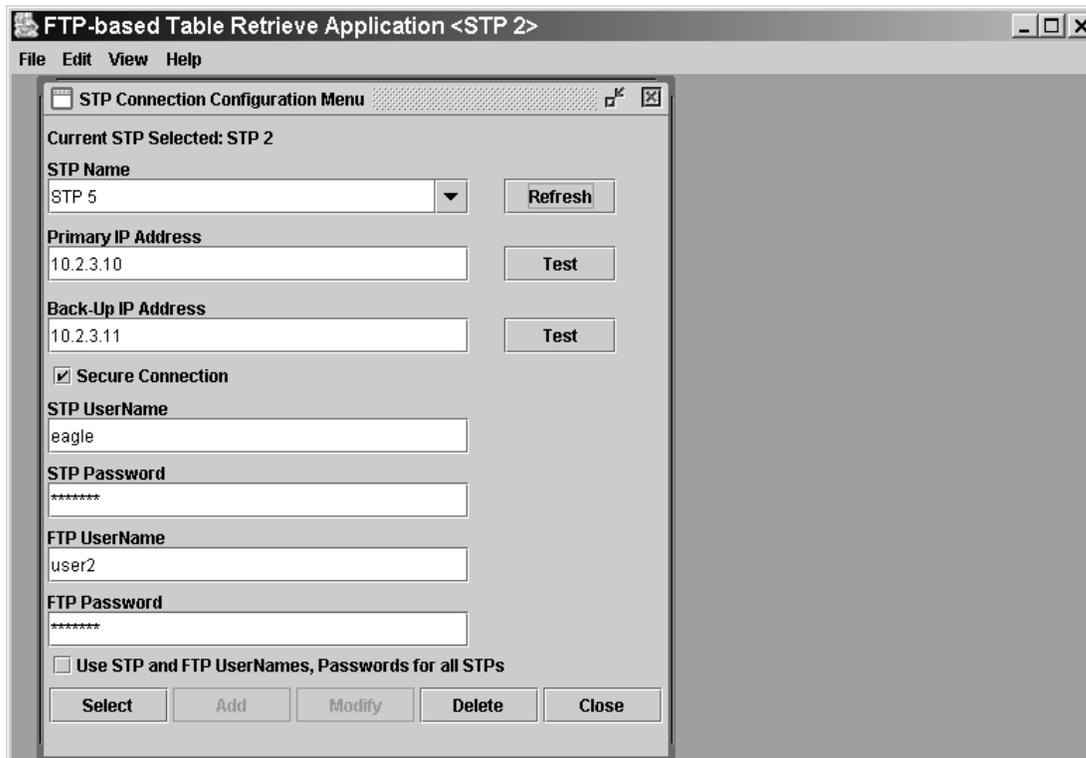


Figure 24. STP Configuration Record (FTRA 2.0 or greater)



3. If the STP name was entered incorrectly, or is not in the STP configuration record database, the "STP Name does not exist" error message is displayed. See Figure 25.

Figure 25. STP Name Does Not Exist Error Message



Testing an STP Configuration Record

Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 5 on page 16. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 16.

2. Display the STP configuration record being modified. Go to the “Displaying an Existing STP Configuration Record” procedure on page 25.

3. Click the **Test** button. The **Connectivity Test Log** window opens. See Figure 26 and Figure 27 on page 34. The Connectivity Test Log contains the events of the Test process and any error messages that may have occurred. The **Connectivity Test Log** window opens at the start of the Test process and is automatically cleared whenever a subsequent Test process is initiated.

Figure 26. Connectivity Test Log Window with No Errors

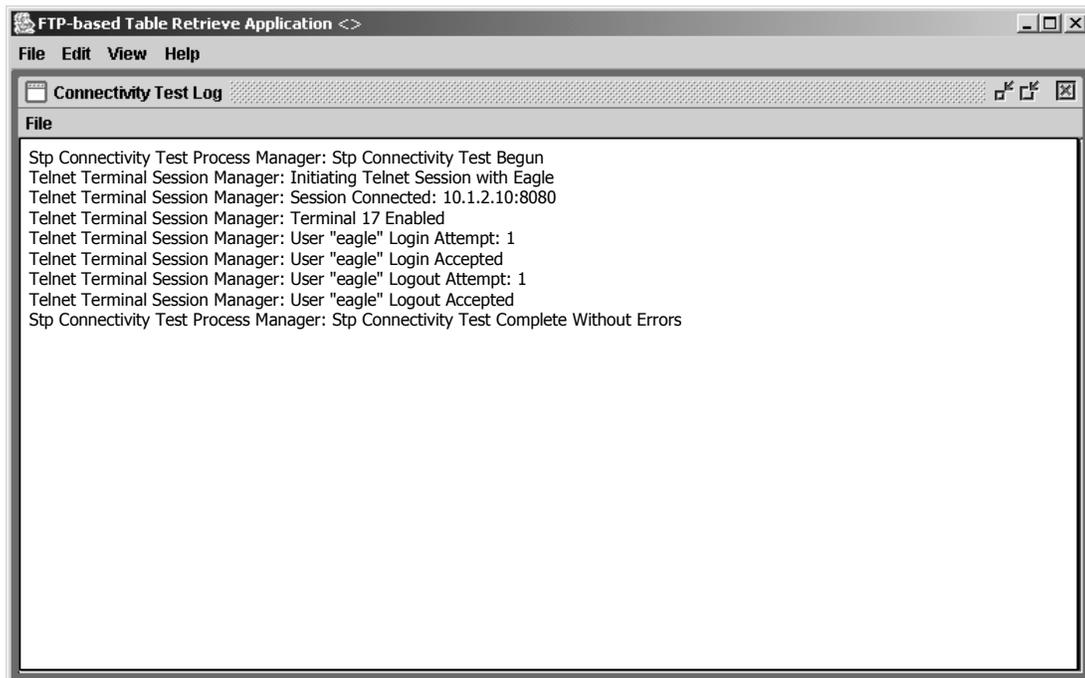
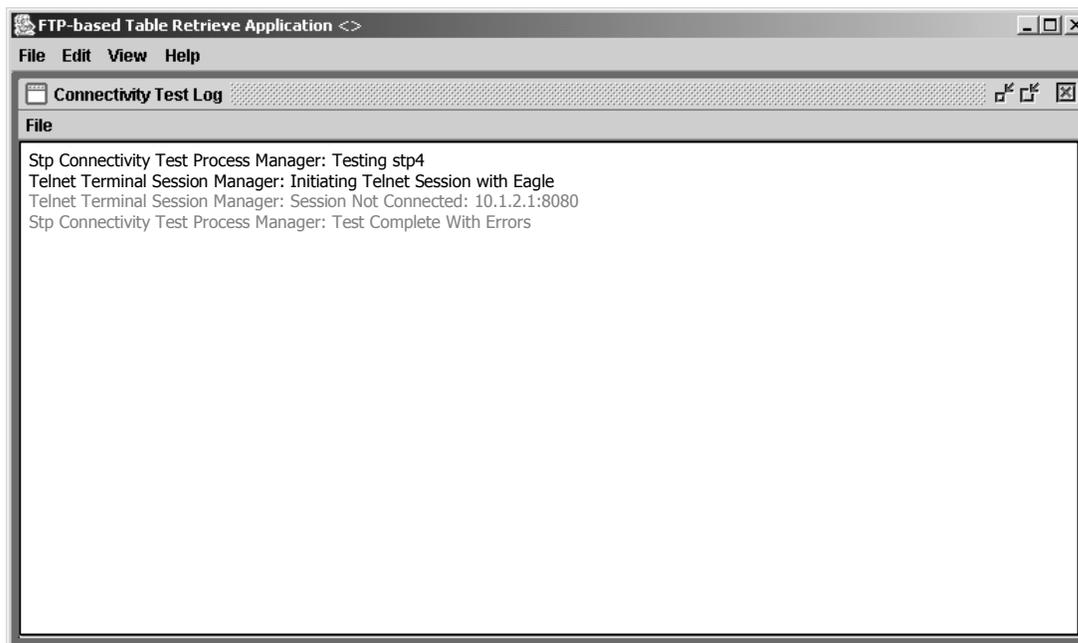
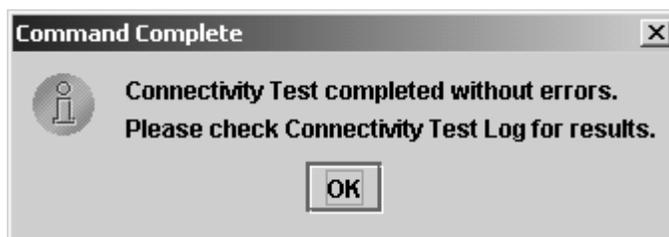


Figure 27. Connectivity Test Log Window with Errors



-
4. When the test is complete, the **Command Complete** window opens. See Figure 28. Click **OK** to continue.

Figure 28. Command Complete Connectivity Test Window

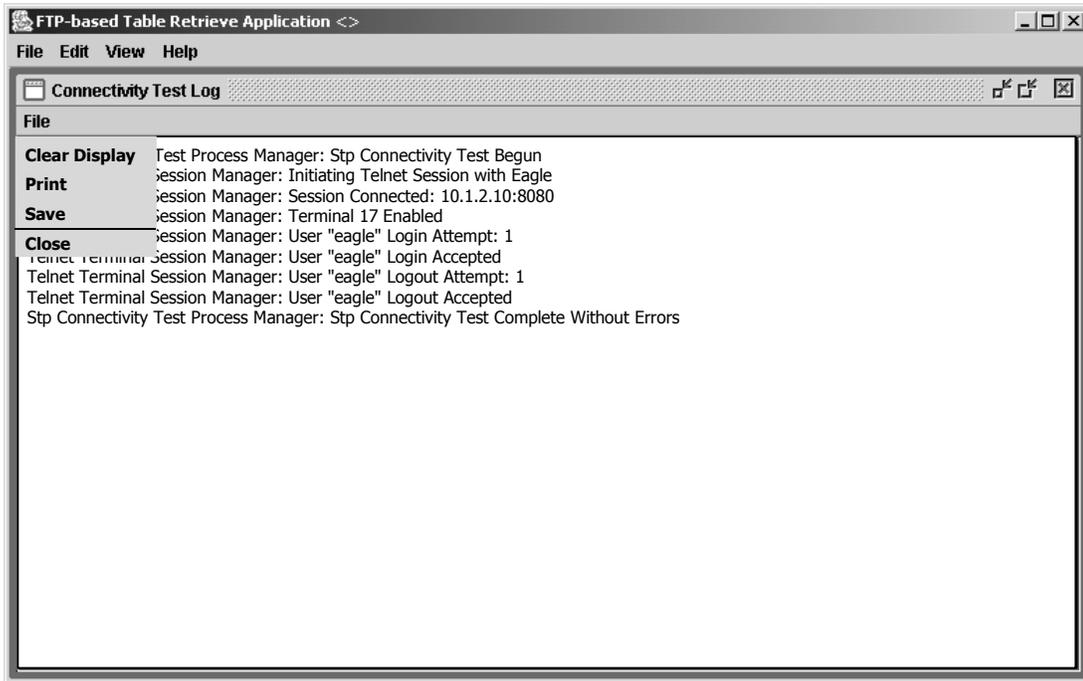


Connectivity Test Log File Menu

The **File** menu in the **Connectivity Test Log** window, shown in Figure 29 on page 35, provides these selections:

- Clearing the Connectivity Test Log display
- Printing the Connectivity Test Log
- Saving the Connectivity Test Log to a file
- Closing the **Connectivity Test Log** window.

Figure 29. File Menu in the Connectivity Test Log Window



Clearing the Connectivity Test Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is save to a file or printed before the display is cleared.

Procedure

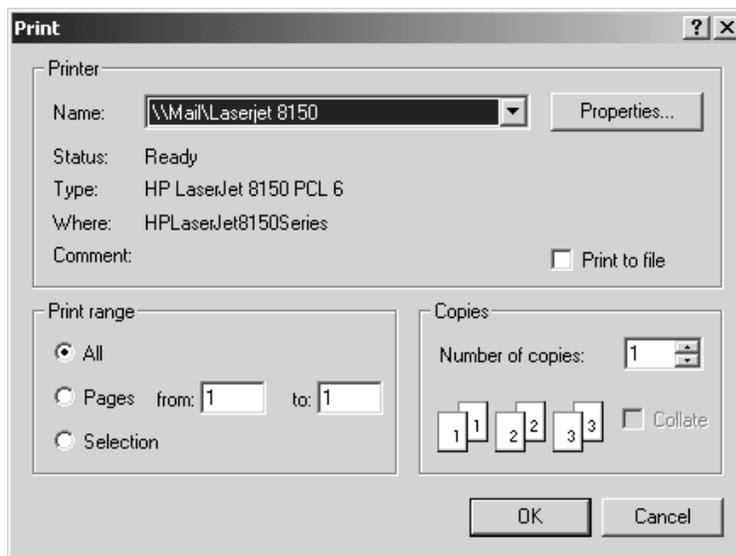
1. Select **File > Clear Display** in the **Connectivity Test Log** window. See Figure 29. The Connectivity Test Log display clears.
-

Printing the Connectivity Test Log

Procedure

1. Select **File > Print** in the **Connectivity Test Log** window. See Figure 29 on page 35. The **Print** window opens. See Figure 30.

Figure 30. Print Window



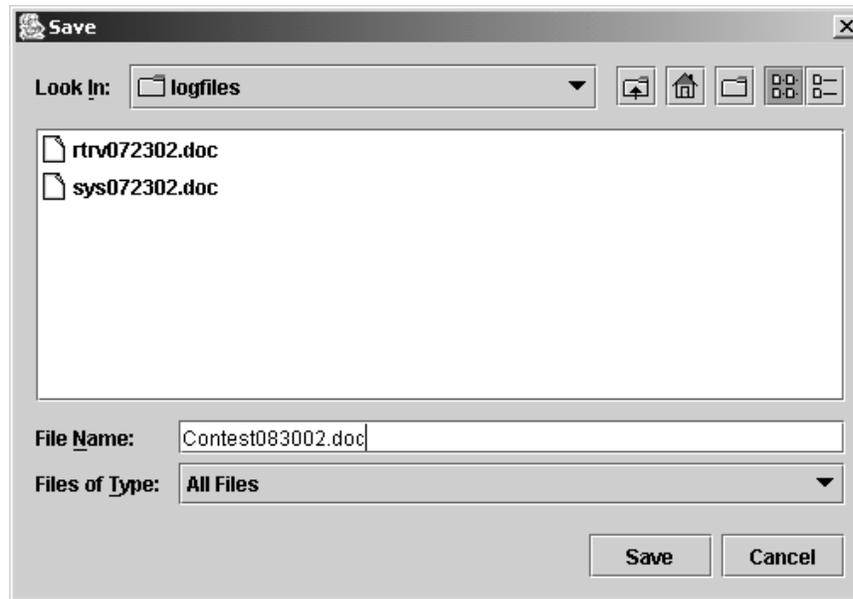
2. Configure the printer settings.
-
3. To print the Connectivity Test Log, click the **OK** button in the **Print** window. The current contents of the Connectivity Test Log are printed.
-
4. If you decide not to print the Connectivity Test Log, click the **Cancel** button in the **Print** window.
-

Saving the Connectivity Test Log to a File

Procedure

1. Select **File > Save** in the **Connectivity Test Log** window. See Figure 29 on page 35. The **Save** window opens. See Figure 31.

Figure 31. Save Window



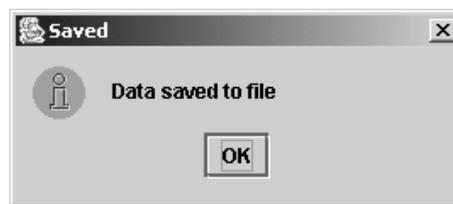
2. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.

NOTE: If you decide not to save the file, do not perform steps 3 and 4, but click **Cancel** in the **Save** window.

3. Click the **Save** button. A **Saved** file confirmation window opens with “Data saved to file.” See Figure 32.

Figure 32. Saved File Confirmation Window



4. To save the file, click **OK** in the **Saved** file confirmation window to continue.
-

Closing the Connectivity Test Log Window

Procedure

1. Select **File > Close** in the **Connectivity Test Log** window, or click the close window button in the upper right hand corner of the **Connectivity Test Log** window. See Figure 29 on page 35. The **Connectivity Test Log** window closes.
-

Modifying an Existing STP Configuration Record

Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 5 on page 16. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 16.
2. Display the STP configuration record being modified. Go to the “Displaying an Existing STP Configuration Record” procedure on page 25.
3. Select and change the STP configuration record parameters. The **Modify** button is enabled when new data is entered into any of the fields, or when the **Use STP and FTP UserNames and Passwords for all STPs** box is checked.

NOTE: The STP name cannot be changed.

If the IP address, STP user name, or STP password is not entered correctly, an error message is displayed. See Figure 11 on page 22, Figure 12 on page 22, or Figure 13 on page 23. If the FTP user name and FTP password are not entered, an error message is displayed. See Figure 14 on page 23 or Figure 15 on page 24

4. To apply the changes, click the **Modify** button. See Figure 33 (FTRA 1.0) or Figure 34 on page 40 (FTRA 2.0 or greater). The displayed STP configuration record is modified, and all fields are cleared. To confirm that the STP configuration data has been modified, the **STP Data Modified** window is displayed (Figure 35 on page 41). Click **OK** in the **STP Data Modified** window to continue.



CAUTION: If the **Use STP and FTP UserNames and Passwords for all STPs** box is checked, then all user names and passwords for all STPs in the STP Configuration database are changed to the user name and password for the displayed STP.

Figure 33. Modifying STP Configuration Record Parameters (FTRA 1.0)

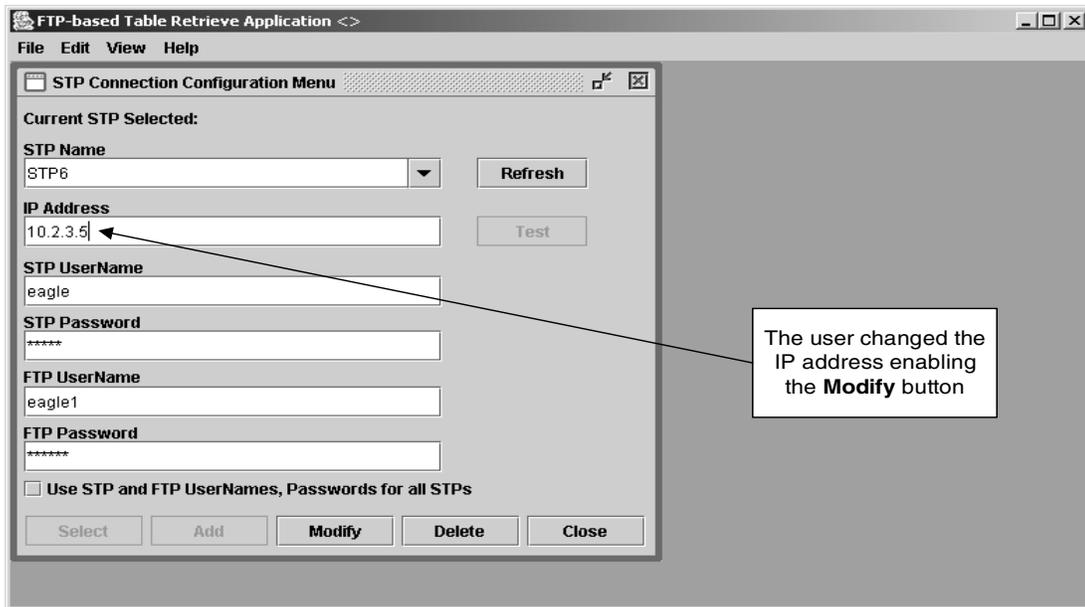


Figure 34. Modifying STP Configuration Record Parameters (FTRA 2.0 or greater)



CAUTION: If the Use STP and FTP UserNames and Passwords for all STPs box is checked, then all user names and passwords for all STPs in the STP Configuration database are changed to the user name and password for the displayed STP.



CAUTION: It is recommended that the setting for the Secure Connection box is not changed, unless you have verified that the new setting for the Secure Connection box will match the state of the Eagle OA&M IP Security Enhancements feature on the STP. The state of the Eagle OA&M IP Security Enhancements feature can be verified by entering the `rtrv-ctrl-feat` command at the EAGLE 5 SAS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, the Secure Connection box should be unchecked. If the Eagle OA&M IP Security Enhancements feature is enabled and activated, the Secure Connection box should be checked. To change the state of the Eagle OA&M IP Security Enhancements feature, perform the “Activating the Eagle OA&M IP Security Enhancements Controlled Feature” procedure in the *Database Administration Manual - System Management*.

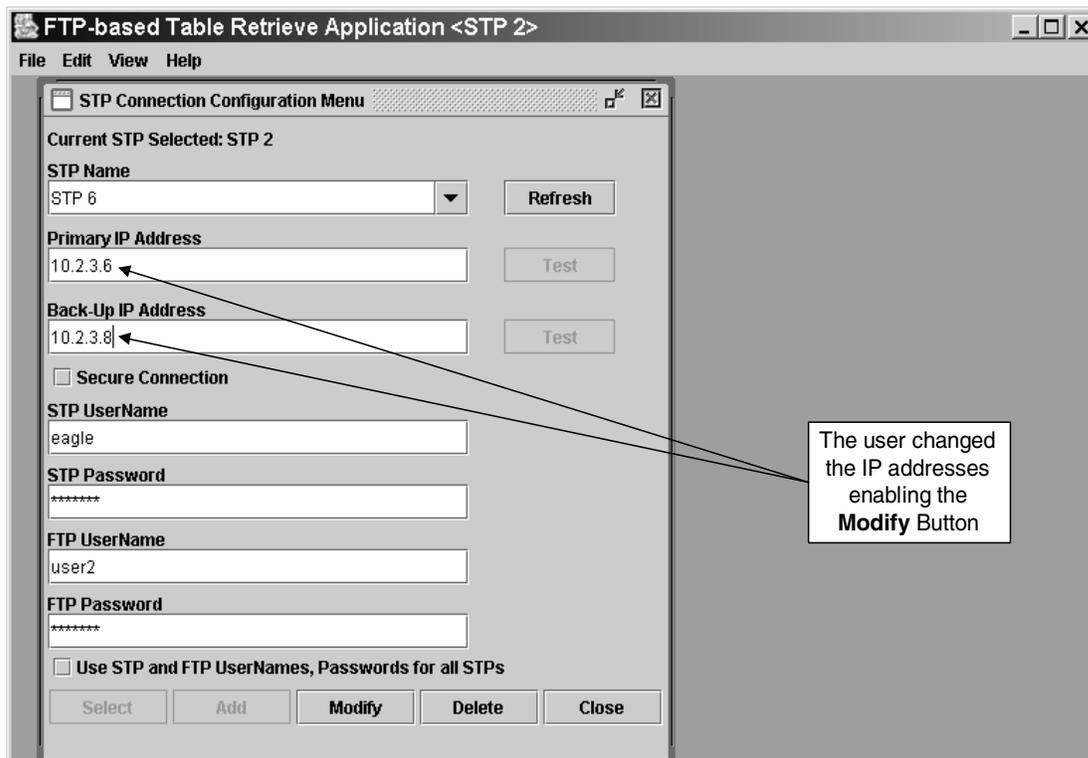
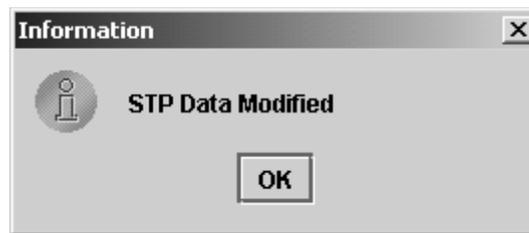
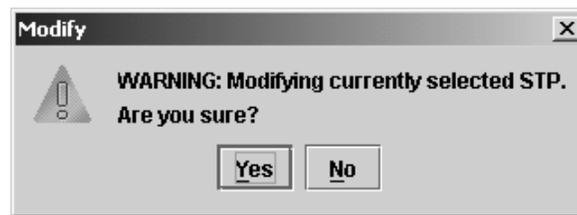


Figure 35. STP Data Modified Window



NOTE: If the STP configuration record being changed is shown in the **Current STP Selected:** field, a **Modify Warning** window is displayed. See Figure 36.

Figure 36. Modify Warning Window



Click **Yes** to continue.

If you do not wish to apply the changes, click the **Refresh** button in the **STP Connection Configuration Menu** window. This resets the STP configuration record values.

-
5. Verify that the changes were made. See the "Displaying an Existing STP Configuration Record" procedure on page 25.
-

Deleting an STP Configuration Record

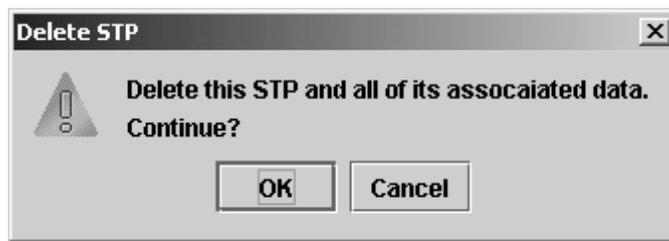
Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 5 on page 16. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 16.
-

2. Display the STP configuration record being deleted. Go to the “Displaying an Existing STP Configuration Record” procedure on page 25. The **Delete** button is enabled when an existing STP configuration record is displayed.

3. To delete the STP configuration record, click the **Delete** button. The **Delete STP** window opens. See Figure 37.

Figure 37. Delete STP Window



Click **OK**, to delete the STP configuration record. The STP configuration record is deleted.

If you do not wish to delete the STP configuration record, click **Cancel**.

4. Verify the STP name is no longer in the STP Connection Configuration database. Go to the “Displaying an Existing STP Configuration Record” procedure on page 25.

Selecting the Current STP

Before retrieving database tables from an EAGLE 5 SAS, or sending commands to an EAGLE 5 SAS, that STP name must be shown in the **STP Connection Configuration Menu** window as the current STP. The **Current STP Selected:** indicator in the **STP Connection Configuration Menu** window shows which STP is the current STP.

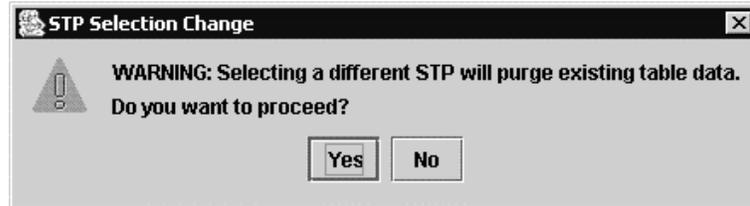
Procedure

1. Display an existing STP configuration record. Go to the “Displaying an Existing STP Configuration Record” procedure on page 25.

2. Click the **Select** button.

If the selected STP is different from the STP shown as the current STP, the **STP Selection Change** window opens and displays “Warning: Selecting a different STP will purge existing table data. Do you want to proceed?” See Figure 38.

Figure 38. STP Selection Change Window



3. To proceed and select the STP name as the current STP, click the **Yes** button in the **STP Selection Change** window. The existing data table is purged.

NOTE: To purge the data tables, a flag is set so that any of the existing table data already stored in the offline database will not be used.

The selected STP name appears in the title bar of the window, and **Current STP Selected: <STP Name>** appears in the **STP Connection Configuration Menu**. See Figure 39 (FTRA 1.0) or Figure 40 on page 44 (FTRA 2.0 or greater).

Figure 39. Current STP Selected (FTRA 1.0)

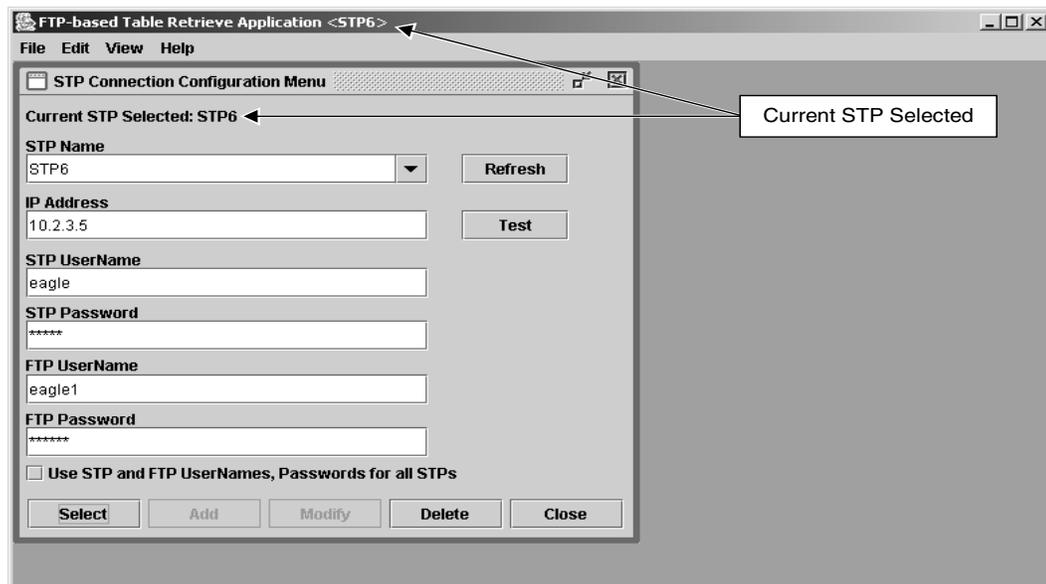
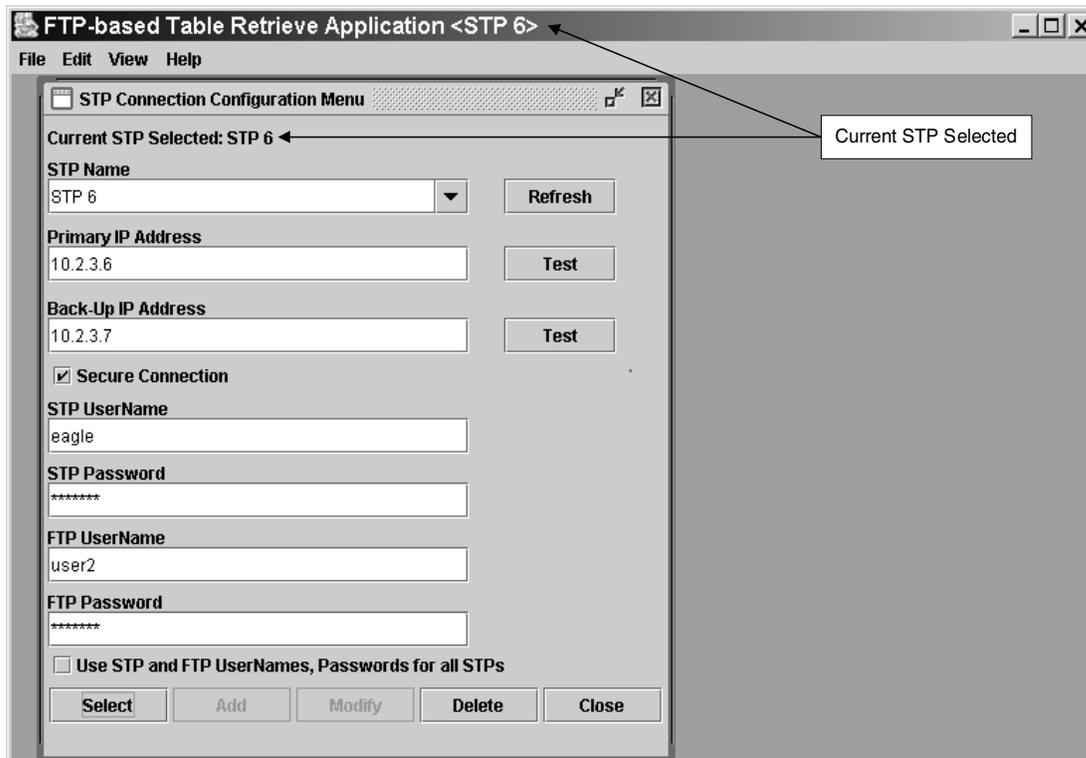


Figure 40. Current STP Selected (FTRA 2.0 or greater)



-
4. If you do not wish to use the STP name selected in step 2, click the **No** button in the **STP Selection Change** window. The current STP configuration record is displayed.
-

Secure EAGLE 5 SAS Host Key Provisioning

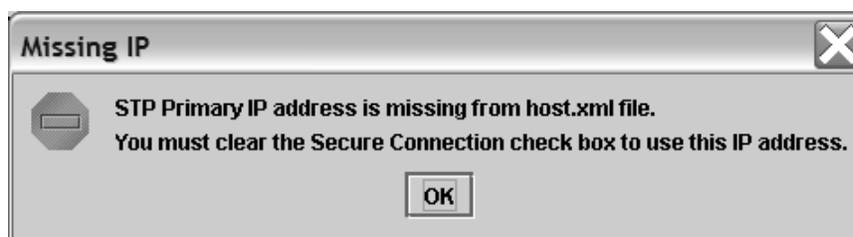
An EAGLE 5 SAS using secure connections has a unique host key for each IPSM in the EAGLE 5 SAS. This key is used by the FTRA (FTRA 2.0 or greater) to positively identify or authenticate each IPSM's telnet server on the EAGLE 5 SAS. The FTRA will not connect to an unauthenticated server. The FTRA authenticates the server by matching its pre-installed host key with the key received from the EAGLE 5 SAS when the connection between the EAGLE 5 SAS and the FTRA is made.

This procedure installs the public host key fingerprint, generated when the IPSM is installed into the EAGLE 5 SAS, reinitialized using the `init-card` command, or when the IPSM is brought into service with the `alw-card` or `rst-card` commands, into the FTRA. This procedure must be performed for each IPSM on each EAGLE 5 SAS that the FTRA will connect to, but only for EAGLE 5 SASs using secure connections to connect to the FTRA. This procedure must be performed before any secure connection between the EAGLE 5 SAS and the FTRA can be initiated.

NOTE: Once the IPSM is installed into the EAGLE 5 SAS, the public host key fingerprint for the IPSM will change only when power to the IPSM is disrupted by removing the IPSM from the shelf, then reinserting the IPSM into the shelf, or as the result of any event that interrupts power to the IPSM. Reinitializing the IPSM will not change the public host key fingerprint for the IPSM. This procedure will have to be performed for each public host key fingerprint on the EAGLE 5 SAS that has changed.

The public host key fingerprint is added to the FTRA's `hosts.xml` file. If the public host key fingerprint has not been added to the FTRA's `hosts.xml` file, and you try to initiate a secure connection to the EAGLE 5 SAS, you will receive the following warning message (Figure 41).

Figure 41. IP Address Warning Message



If the warning message shown in Figure 41 is received, either clear the **Secure Connection** check box in the STP Configuration Record for the STP (see the "Modifying an Existing STP Configuration Record" procedure on page 38), or add the public host key fingerprint to the FTRA's `hosts.xml` file using the procedure on page 47.

The verification that the keys are installed on the FTRA is called strict host key checking. By default, strict host key checking is on. This enforces server (EAGLE 5 SAS) strong authentication, designed to provide security between the FTRA and the EAGLE 5 SAS. This also prevents a hostile server from tricking the FTRA into exposing any EAGLE 5 SAS login and password combinations.



CAUTION: Do not set strict host key checking to off, unless your network is in a controlled and secure environment. If you set strict host key checking to off, the Connectivity Test Log will warn you each time you try to connect that the EAGLE 5 SAS public host key fingerprint has not been added to the hosts.xml file on the FTRA.

To set the strict host key flag:

1. Open the application start file using any text file editor. On the Windows platform, open the `ftra.bat` file. On the UNIX platform, open the `ftra` file.

2. Insert into the application start file, one of these text strings, depending on whether you want strict host key checking on or off.
 - `-DstrictHostKeyChecking=1` for setting strict host key checking to on (this is the default setting).
 - `-DstrictHostKeyChecking=0` for setting strict host key checking to off

This text string can be inserted anywhere between the `%JRE_HOME%\bin\java` and `-cp` text strings as shown in the following example.

```
%JRE_HOME%\bin\java -DstrictHostKeyChecking=1 -Ddebuglevel=2
-DsshTools.home=%FTRA2_HOME% -Dftra2rootdir=%FTRA2_HOME% -cp ftra3.jar
com.tekelec.ftra.gui.InterfaceSelector %1
```

3. Save the changes and close the application start file.

Procedure

1. On the EAGLE 5 SAS, enter the `rtrv-trm` command. The location of the IPSM is shown in the `LOC` column with the `TELNET` terminal type.

This is an example of the possible output.

```

rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
TRM  TYPE      COMM          FC      TMOUT  MXINV  DURAL
1    VT320      9600-7-E-1   SW      30     5     99:59:59
2    KSR        9600-7-E-1   HW      30     5     INDEF
3    PRINTER   4800-7-E-1   HW      30     0     00:00:00
4    VT320      2400-7-E-1   BOTH    30     5     00:30:00
5    VT320      9600-7-O-1   NONE    30     5     00:00:30
6    VT320      9600-7-E-2   SW      30     9     INDEF
7    PRINTER   9600-7-N-2   HW      30     5     00:30:00
8    KSR        19200-7-E-2  BOTH    30     5     00:30:00
9    VT320      9600-7-E-1   SW      30     7     00:30:00
10   VT320      9600-7-E-1   HW      30     5     00:30:00
11   VT320      4800-7-E-1   HW      30     5     00:30:00
12   PRINTER   9600-7-E-1   HW      30     4     00:30:00
13   VT320      9600-7-O-1   NONE    30     5     00:30:00
14   VT320      9600-7-E-2   SW      30     8     00:30:00
15   VT320      9600-7-N-2   HW      30     5     00:30:00
16   VT320      9600-7-E-2   BOTH    30     3     00:30:00

TRM  TYPE      LOC          TMOUT  MXINV  DURAL      SECURE
17   TELNET   1111         60     5     00:30:00  yes
18   TELNET   1111         60     5     00:30:00  yes
19   TELNET   1111         60     5     00:30:00  yes
20   TELNET   1111         60     5     00:30:00  yes
21   TELNET   1111         60     5     00:30:00  yes
22   TELNET   1111         60     5     00:30:00  yes
24   TELNET   1111         60     5     00:30:00  yes

TRM  TRAF  LINK  SA  SYS  PU  DB  UIMRD
1    NO   YES  NO  YES  NO  YES  YES
2    NO   NO   NO  NO  NO  NO  NO
3    YES  YES  YES  NO  YES  YES  YES
4    YES  NO   NO  NO  NO  NO  NO
5    NO   YES  NO  NO  NO  NO  YES
6    NO   NO   YES  NO  NO  NO  NO
7    YES  YES  YES  YES  YES  YES  YES
8    NO   NO   NO  NO  YES  NO  YES
9    NO   YES  NO  NO  NO  YES  NO
10   NO   NO   NO  NO  NO  NO  YES
11   YES  YES  YES  YES  YES  YES  YES
12   YES  YES  YES  YES  YES  YES  YES
13   NO   YES  NO  NO  NO  NO  YES
14   NO   NO   YES  NO  NO  NO  NO
15   YES  YES  YES  NO  YES  YES  YES
16   NO   NO   NO  NO  YES  NO  YES
17   NO   NO   NO  NO  NO  NO  NO
18   NO   NO   NO  NO  NO  NO  NO
19   NO   NO   NO  NO  NO  NO  NO
20   NO   NO   NO  NO  NO  NO  NO
21   NO   NO   NO  NO  NO  NO  NO
22   NO   NO   NO  NO  NO  NO  NO
23   NO   NO   NO  NO  NO  NO  NO
24   NO   NO   NO  NO  NO  NO  NO

```

2. Display the IP address assigned to the IPSM using the `rtrv-ip-lnk` command, specifying the card location of the IPSM shown in step 1 and the `port=a` parameter. For this example, enter this command.

```
rtrv-ip-lnk:loc=1111:port=a
```

The following is an example of the possible output.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
LOC  PORT IPADDR          SUBMASK          DUPLEX SPEED MACTYPE AUTO MCAST
1111  A    192.168.54.96        255.255.255.0   HALF   100   DIX    NO   NO
```

NOTE: If the Security Administration (SA) setting for all the terminals assigned to the IPSM specified in this procedure is set to **YES**, see the `rtrv-trm` output in step 1, skip this step and go to step 4.

3. Change the Security Administration setting on the terminals assigned to the IPSM with the `chg-trm` command and specifying the number of the terminals whose Security Administration setting is **NO**, and with the `sa=yes` parameter.

```
chg-trm:sa=yes:trm=<TELNET terminal number>
```

When the `chg-trm` command has successfully completed, this message should appear.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
CHG-TRM: MASP A - COMPLTD
```

NOTE: When the IPSM is installed into the EAGLE 5 SAS, UIM 1493 is generated. UIM 1493 contains the DSA key fingerprint to be added to the `hosts.xml` file. If you recorded the DSA key fingerprint for the IPSM when UIM 1493 was generated, skip step 4 and go to step 5.



CAUTION: If you are performing step 4 from a telnet terminal, make sure the step is being performed from a telnet terminal that is not assigned to the IPSM being initialized. When the IPSM is initialized, you will lose all telnet connections supported by the IPSM being initialized.

4. Obtain the DSA key fingerprint for the IPSM by performing the `init-card` command and specifying the location of the IPSM. For this example, enter this command.

```
init-card:loc=1111
```

After the `init-card` command has been executed, UIM 1494 is generated. The DSA key fingerprint is at the end of the output, in the hexadecimal format, and shown in bold in this output example.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
0021.1494   CARD 1111   INFO   SSH Host Keys Loaded
           DSA Server Host Key FTRA-formatted Fingerprint=
           84 7c 92 8b c 7c d8 19 1c 6 4b de 5c 8f c5 4d
           Report Date:05-03-17   Time:15:08:45
```

NOTE: If you wish to change the public host key fingerprint on the IPSM, remove and reinsert the IPSM. The public host key fingerprint does not change until the IPSM loses power. However, contact the Customer Care Center before removing and reinserting the IPSM. Refer to page 3 for the contact information.

5. Edit the FTRA **hosts.xml** file (in the **\$FTRA_HOME/cfg** directory on Unix or **%FTRA_HOME%\cfg** folder on Windows), using any text file editor. Add the:

- IPSM IP address from the **rtrv-ip-lnk** output shown in step 2
- DSA public key fingerprint, shown in either the output of UIM 1493, when the IPSM was installed, or from the output of UIM 1494 when the **init-card** command was performed in step 4 in the following format:

```
<AllowHost HostName="<IPSM IP Address>" Fingerprint="767: <DSA public key fingerprint>"/>
```

NOTE: The value 767 preceding the DSA public key fingerprint is the length of the key in bytes. On your EAGLE 5 SAS, this value may be different. refer to the FTRA Connectivity Test Log to verify this value. The outputs of UIM 1493 or 1494 do not contain this value.

The following is a sample **/ftra/cfg/hosts.xml** file before the new DSA fingerprint information is added.

```
=====
<?xml version="1.0" encoding="UTF-8"?>

<HostAuthorizations>
<AllowHost HostName="192.168.54.36" Fingerprint="767: 4a 9 ec d3 70 34 d2 91
f7 8b 75 a8 95 37 98 35"/>
<AllowHost HostName="192.168.54.216" Fingerprint="767: bc 76 ac 53 1e fd 72 16
3e 9c dc d7 23 25 6 59"/>
///-----
/// Add new fingerprints HERE, after last allowed host in the above list.
///-----
</HostAuthorizations>
=====
```

The sample **/ftra/cfg/hosts.xml** file after the new DSA fingerprint information is added.

```
=====
<?xml version="1.0" encoding="UTF-8"?>

<HostAuthorizations>
<AllowHost HostName="192.168.54.36" Fingerprint="767: 4a 9 ec d3 70 34 d2 91
f7 8b 75 a8 95 37 98 35"/>
<AllowHost HostName="192.168.54.216" Fingerprint="767: bc 76 ac 53 1e fd 72 16
3e 9c dc d7 23 25 6 59"/>
<AllowHost HostName="192.168.54.96" Fingerprint="767: 84 7c 92 8b c 7c d8 19
1c 6 4b de 5c 8f c5 4d"/>
///-----
/// Add new fingerprints HERE, after last allowed host in the above list.
///-----
</HostAuthorizations>
=====
```

NOTE: There should be no duplicate IP addresses in this file.

6. Save the file and exit the text editor.

-
7. A secure connection can now be established to the IP address used in this procedure. Either add the STP containing the IP address to the STP Configuration Record (see the “Adding an STP Configuration Record” procedure on page 20), or if the IP address is already defined in the STP Configuration Record, change the existing record for this STP with the IP address used in this procedure (see the “Modifying an Existing STP Configuration Record” procedure on page 38). Whether adding a new STP record, or changing an existing STP record, make sure the **Secure Connection** check box is checked.

-
8. After the STP record has been added or changed to use a secure connection, test the connection by performing the “Testing an STP Configuration Record” procedure on page 33. If the connection test is passed, the public host key fingerprint is successfully installed.

If the connection is refused, make sure that the key information for the EAGLE 5 SAS and the FTRA shown in the Connectivity Test Log match. The Connectivity Test Log shows both the key received from the EAGLE 5 SAS host and the key contained in the **hosts.xml** file for the EAGLE 5 SAS host. The following is an example from the Connectivity Test Log containing a host key mismatch. The key received from the EAGLE 5 SAS host is shown in bold. The key contained in the **hosts.xml** file is shown in bold underline.

```
2003-07-11 14:22:56.117: Stp Connectivity Test Process Manager: Testing STP11805011201
2003-07-11 14:22:56.227: Telnet Terminal Session Manager: Initiating Secure Telnet
Session with Eagle: 192.168.53.71:22
2003-07-11 14:22:56.808: HostKeyVerification: ERROR: Host 192.168.53.71 cannot be
authenticated due to a mismatched entry for this host in the hosts.xml file. The host key
supplied by 192.168.53.71 is: 768: bb 7d 79 a2 7d ae 5d 5a 45 e2 44 58 cd 8a bd 83.
The current allowed key for 192.168.53.71 is: 768: ab 7d 79 a2 7d ae 5d 5a 45 e2 44 58 cd
8a bd 83.
2003-07-11 14:22:56.828: HostKeyVerification: Connection rejected...onHostKeyMismatch
```

FTP Server Configuration

An FTP server must be configured on the EAGLE 5 SAS using the **FTP Server Configuration** menu before database tables can be retrieved from the EAGLE 5 SAS, or command files can be sent to the EAGLE 5 SAS.

NOTE: If the **Secure Connection** box in the **STP Connection Configuration Menu** window (applies only in FTRA 2.0 or greater) is checked, the IP address specified in the **FTP Server Configuration** menu must be the IP address of a secure FTP server. If the **Secure Connection** box in the **STP Connection Configuration Menu** window is not checked, the IP address specified in the **FTP Server Configuration** menu must be the IP address of a FTP server.

NOTE: Any firewall between the FTRA and the FTP server configured in the **FTP Server Configuration Menu** window (Figure 43 on page 52), must allow FTPs to the IP address specified in the **FTP Server Configuration Menu** window.

Procedure

1. Select **Edit > FTP Server Configuration** from the **FTP-based Table Retrieve Application** menu. See Figure 42.

Figure 42. FTP Server Configuration Menu in the FTP-Based Table Retrieve Application Window



The **FTP Server Configuration Menu** window opens. See Figure 43 on page 52 and Table 3 on page 52.

Figure 43. FTP Server Configuration Menu Window

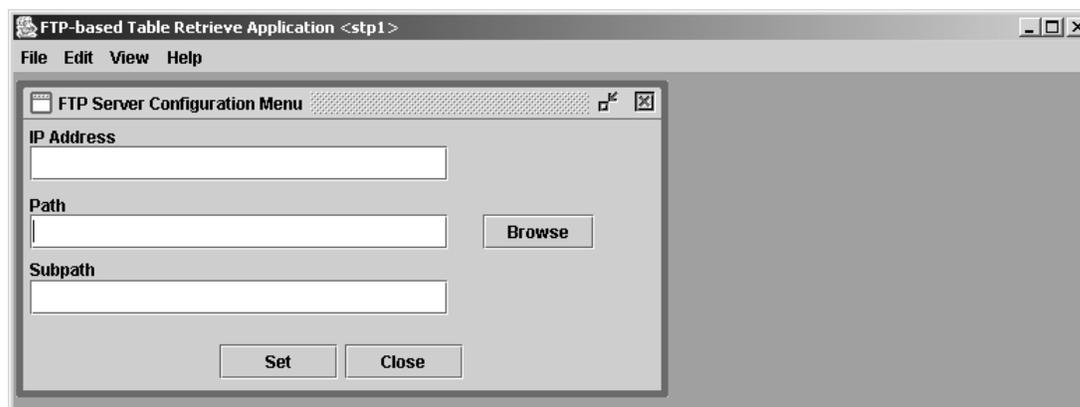


Table 3. FTP Server Configuration Menu Window Descriptions

Item	Description
Fields	
IP Address	The IP Address of the associated STP
Path	The complete path to the data tables transfer directory on the STP. This directory must be given complete read/write/execute permissions for all users. From Windows, this is commonly administered from within the FTP server software. From Unix, this is done with the chmod command. Please refer to your PC system documentation or Unix man pages for full details on setting directory permissions.
Subpath	The value used by the path parameter of the EAGLE 5 SAS ent-ftp-serv/chg-ftp-serv commands. The subpath is relative to the user's default directory upon FTP login. A file separator ('\ or '/') is not used to begin the subpath string.
Buttons	
Browse	Opens the Select Starting Directory window to initiate a directory/file selection dialog for the data tables.
Set	Stores the FTP server configuration data.
Close	Closes the FTP Server Configuration Menu window.

- Enter the IP address of the STP in the **IP Address** field. See .

NOTE: If the format is not entered correctly, the **Invalid IP Address** warning window is displayed. See Figure 44 on page 53.

Figure 44. Invalid IP Address Error Message



3. Enter the path for the FTP temporary data table storage area or click the **Browse** button.

If the **Browse** button is clicked, the **Select Starting Directory** window opens to select the location for the temporary data table storage area to be entered in **Path** field. See Figure 45 and Table 4 on page 54.

This directory must be given complete read/write/execute permissions for all users. From Windows, this is commonly administered from within the FTP server software. From Unix, this is done with the `chmod` command. Please refer to your PC system documentation or Unix `man` pages for full details on setting directory permissions.

Figure 45. Select Starting Directory Window

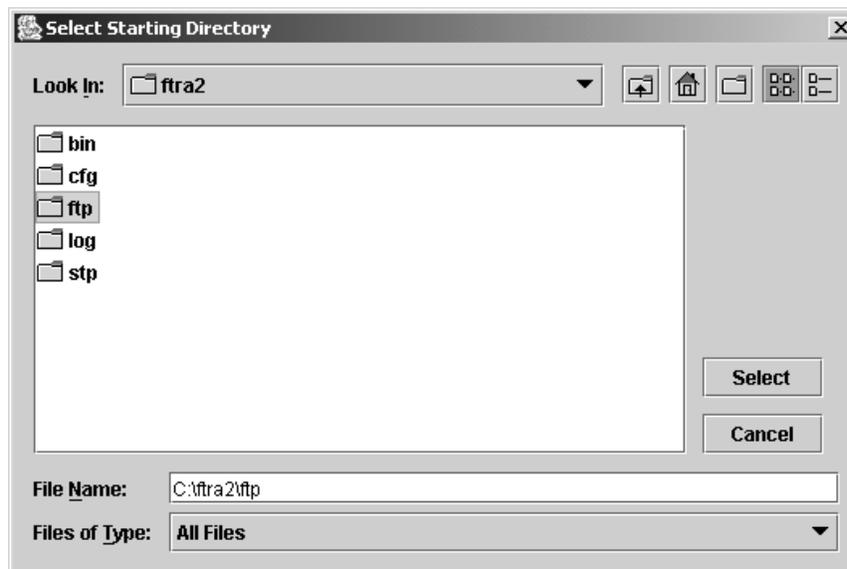
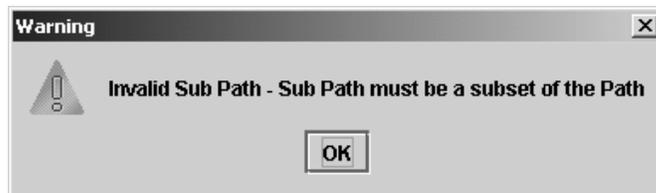


Table 4. Select Starting Directory Window Descriptions

Item	Description
Fields	
Look in:	A drop down menu that allows the user to browse through the directory structures.
File Name:	The name of the file to be selected.
Files of type:	A drop down menu that allows the user to select all files of a particular type.
Buttons	
Select	Takes the contents of the File Name field and loads it into the Path field of the menu
Cancel	Closes the Select Starting Directory window.

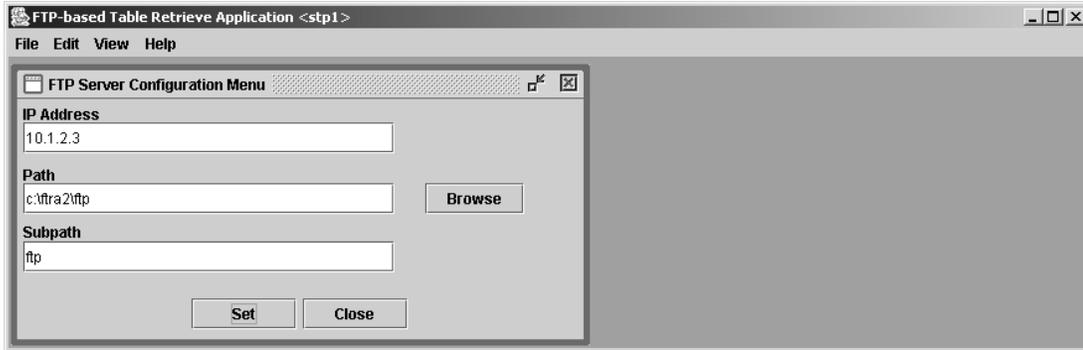
4. Enter the Subpath. The subpath must always be the last part of the path. The subpath is relative to the user's default directory upon FTP login. A file separator ('\ ' or '/') is not used to begin the subpath string. If an invalid Subpath is entered, a warning window opens. See Figure 46.

Figure 46. Invalid Subpath Window



5. Click the **Set** button. See Figure 47.

Figure 47. FTP Server Configuration Example



The **FTP Server Data Set** window opens. See Figure 48.

Figure 48. FTP Server Data Set Window



Click **OK** to continue.

Retrieve Database Tables from an STP

Retrieve Tables Window

The **Retrieve Tables** window (see Figure 50 on page 57) is used to select the database tables you wish to retrieve from the selected STP. The **Retrieve Tables** window contains a list of predefined retrieve commands. Any number of the retrieve commands can be selected from the **Command List** box and moved to the **Selected Commands** box. Clicking the **Retrieve** button causes the database tables associated with the selected retrieve commands to be transferred from the selected STP.

The **Retrieve from STP** and **Retrieve from Local Database** buttons determine whether new database tables are retrieved from the selected STP or if existing tables already retrieved from that STP will be used. If no tables exist for the selected STP, the **Retrieve from Local Database** button will be grayed out.

The output from the retrieve commands is converted to CSV files. When the retrieve operation is completed, the **Command Complete** window opens notifying the user if the retrieve was executed with or without errors. The Retrieve Tables Log opens allowing the user to view the events.



CAUTION: Starting with FTRA 2.0, if you attempt to retrieve and convert the database tables for these GTT commands (`rtrv-tt`, `rtrv-gtt`) and these EGTT commands (`rtrv-gttset1`, `rtrv-gttset`, `rtrv-gta`) in the same retrieve tables request, you will receive a warning (Figure 49) that errors can be caused by attempting to retrieve and convert the GTT and EGTT database tables from the same EAGLE 5 SAS.

You may only retrieve and convert the tables corresponding to which feature is on, GTT or EGTT. If the EGTT feature is on, shown in the `rtrv-feat` output, the database tables for the `rtrv-gttset1`, `rtrv-gttset`, and `rtrv-gta` commands can be retrieved and converted. If the EGTT feature is off, the database tables for the `rtrv-tt` and `rtrv-gtt` commands can be retrieved and converted.

The errors will be caused when the retrieved GTT and EGTT database tables are converted to CSV files. Because only one set of the database tables, GTT or EGTT, can be retrieved, only that set of the database tables can be converted. The error will occur when the attempt is made to convert that database tables that could not be retrieved.

Figure 49. GTT Warning Window

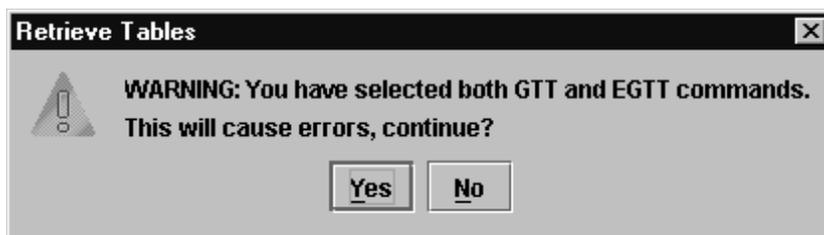


Figure 50. Retrieve Tables Window

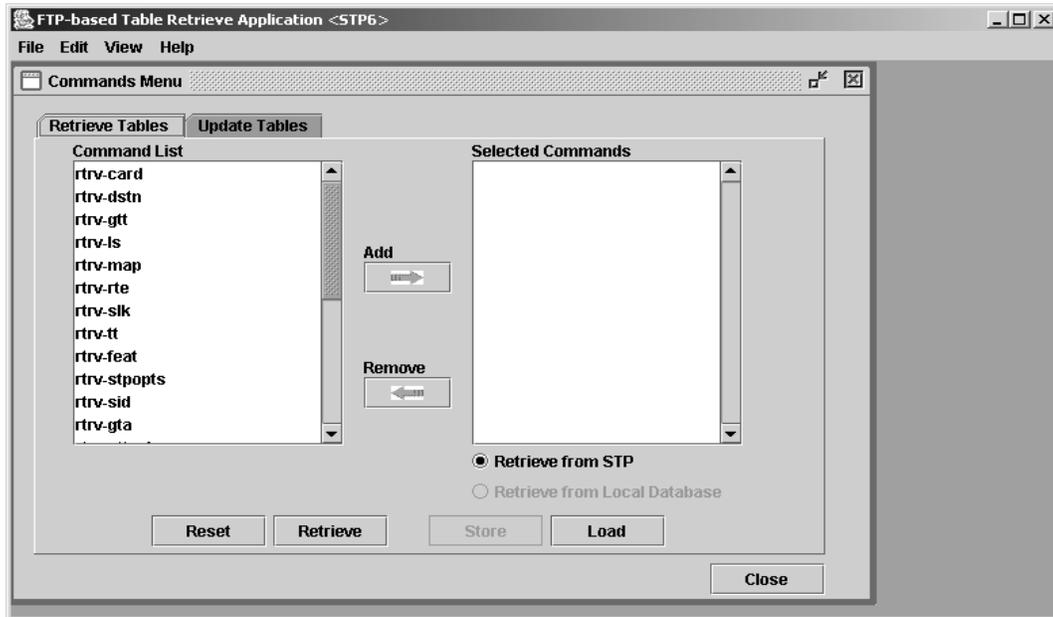


Table 5 on page 58 shows the description of the fields and buttons in the **Retrieve Tables** window.

Table 5. Retrieve Tables Window Description

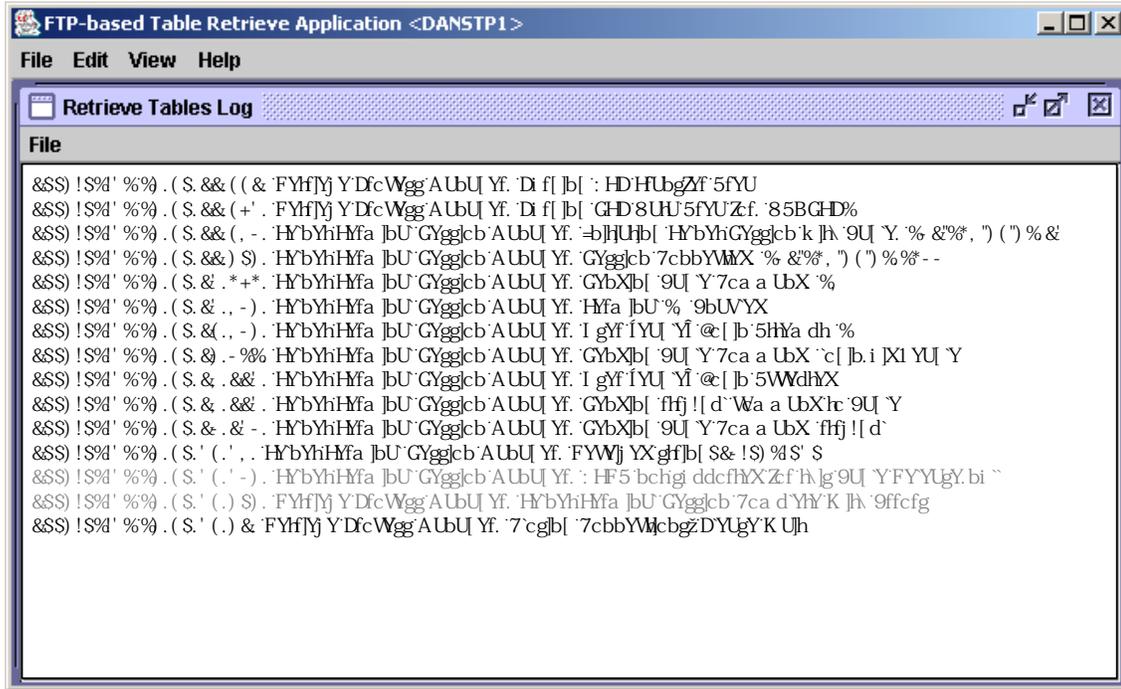
Item	Description
Fields	
Command List	Contains a predefined list of retrieve commands.
Selected Commands	These commands are used to determine which database tables are retrieved from the selected STP. From one to all of the retrieve commands can be selected for retrieval.
Buttons	
Add	Moves the highlighted commands from the Command List box to the Selected Commands box.
Remove	Moves any highlighted commands in the Selected Commands box back to the Command List box.
Reset	Moves all commands in the Command List box to the Selected Commands box. All highlights in the Selected Commands box are removed.
Retrieve	Initiates the retrieval of all the selected database tables represented by the selected retrieve commands. The database tables are transferred using an FTP connection and converted to CSV files.
Store	Stores the commands in the Selected Commands box which will be used by the Command Line Interface. This list is maintained even when the FTRA is shut down and restarted.
Load	Loads the commands into the Selected Commands box which are currently stored for Command Line Interface usage. This allows the user to verify rtrv commands which will be executed by the Command Line Interface.
Retrieve from STP	Retrieves the database tables, based on the selected retrieve commands, from the selected STP instead of using the tables previously retrieved.
Retrieve from Local Database	When selected, the FTRA uses the database table previously retrieved from the selected STP.
Close	Closes the Commands Menu window.

In FTRA releases 1.x and 2.x, the FTRA could operate only with one release of the EAGLE 5 SAS. Starting with FTRA 3.0, the FTRA can operate with any of these EAGLE 5 SAS releases: 29.0, 30.0, 30.2, 31.3, 31.6, 31.9, 32.0 and later. EAGLE 5 SAS releases 32.0 and later are supported if that release supports CSV file output.

FTP-Based Table Retrieve Application (FTRA) User Guide

When a Retrieve Tables command is performed, FTRA 3.0 verifies that the EAGLE 5 SAS is running one of the supported releases. If the EAGLE 5 SAS release is not supported, an error message is displayed and the Retrieve Tables command is terminated. See Figure 51.

Figure 51. Retrieve Table Log - Release Not Compatible Error



If the EAGLE 5 SAS release is supported, the Retrieve Tables command is performed and operations on the FTRA can continue.

Procedure

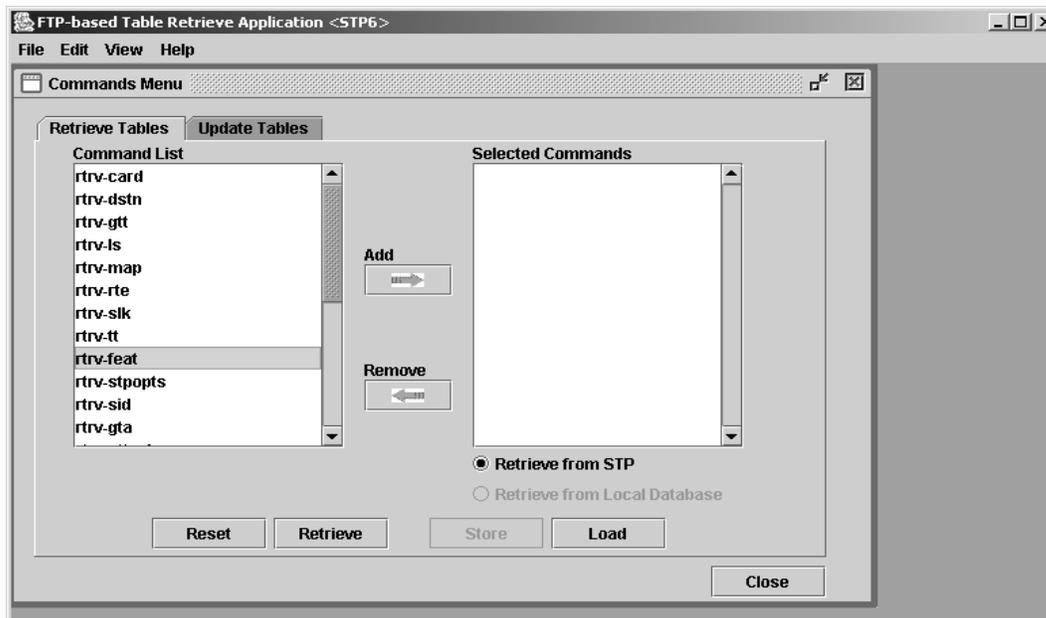
1. Select **Edit > Commands > Retrieve Tables** from the **FTP-Based Table Retrieve Application** window. See Figure 52. The **Retrieve Tables** window opens. See Figure 50 on page 57.

Figure 52. Commands Menu in the FTP-Based Table Retrieve Application Window



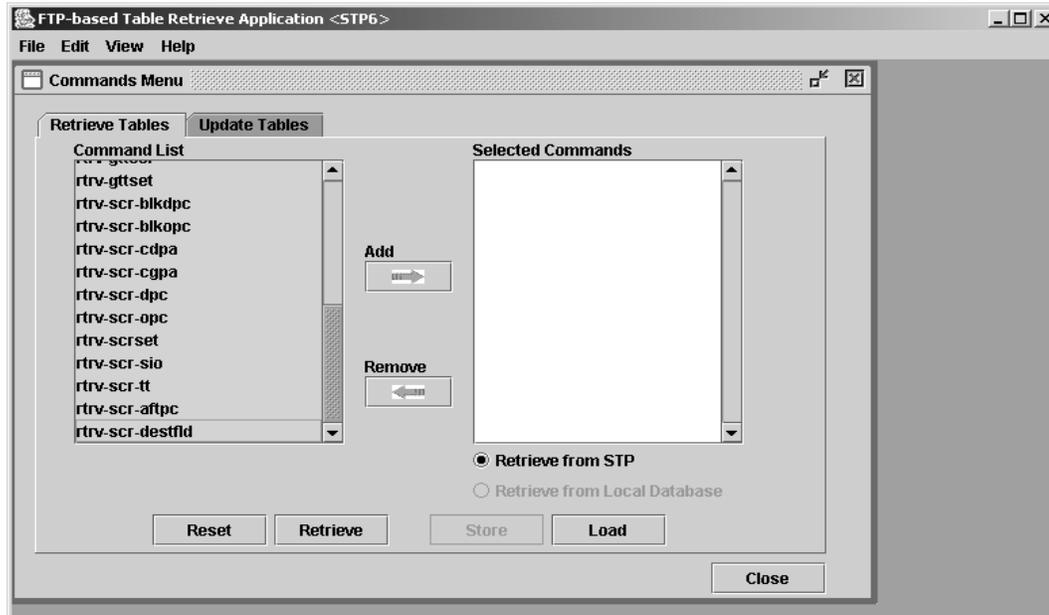
2. To select commands in the **Command List** box of the **Retrieve Tables** window, perform one of these steps:
 - a. To select a single command, click on the command and it is highlighted. See Figure 53.

Figure 53. Selecting a Command



- b. To select a range of commands, click on the first command and while holding down the Shift key, click on the last command to be selected. All the commands in between the selected commands are highlighted, along with the selected commands. See Figure 54.

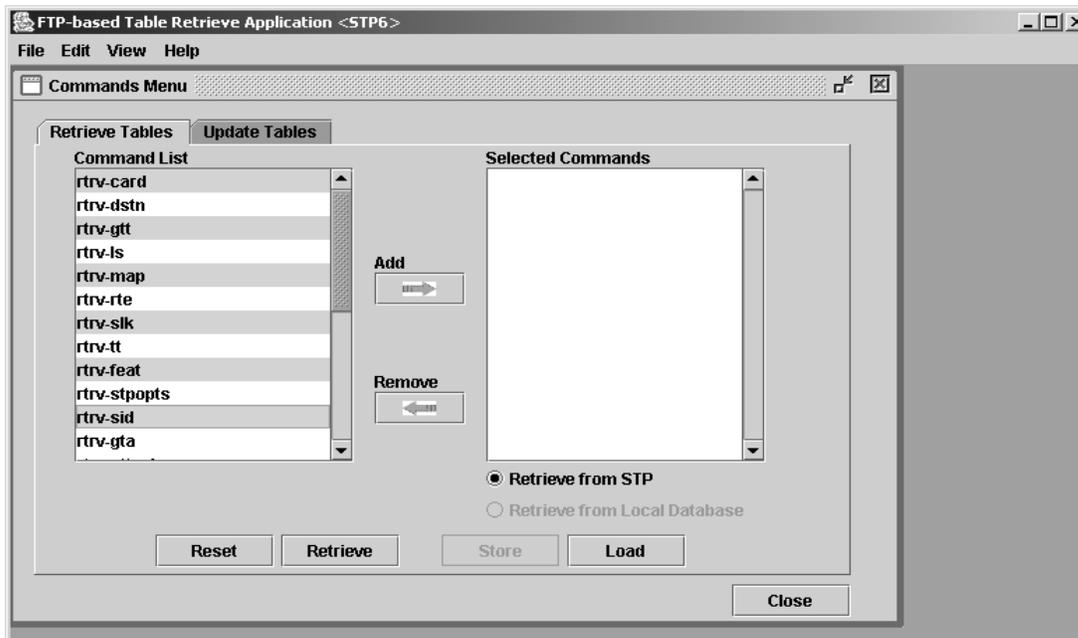
Figure 54. Selecting a Range of Commands



- c. To select multiple commands, select the first command, then hold down the Ctrl key and click on each of commands to be selected. The selected commands are highlighted. See Figure 55 on page 62.

NOTE: If you have selected any of these GTT commands (rtrv-tt, rtrv-gtt) and these EGTT commands (rtrv-gttset, rtrv-gttset, rtrv-gta) in substeps b or c, see the Caution on page 56.

Figure 55. Selecting Multiple Commands



- To move the commands selected in step 2 to the **Selected Commands** box, click the **Add** button. The commands are moved to **Selected Commands** box. See Figure 56, Figure 57 on page 63, and Figure 58 on page 63.

Figure 56. Adding a Command to the Selected Commands Box

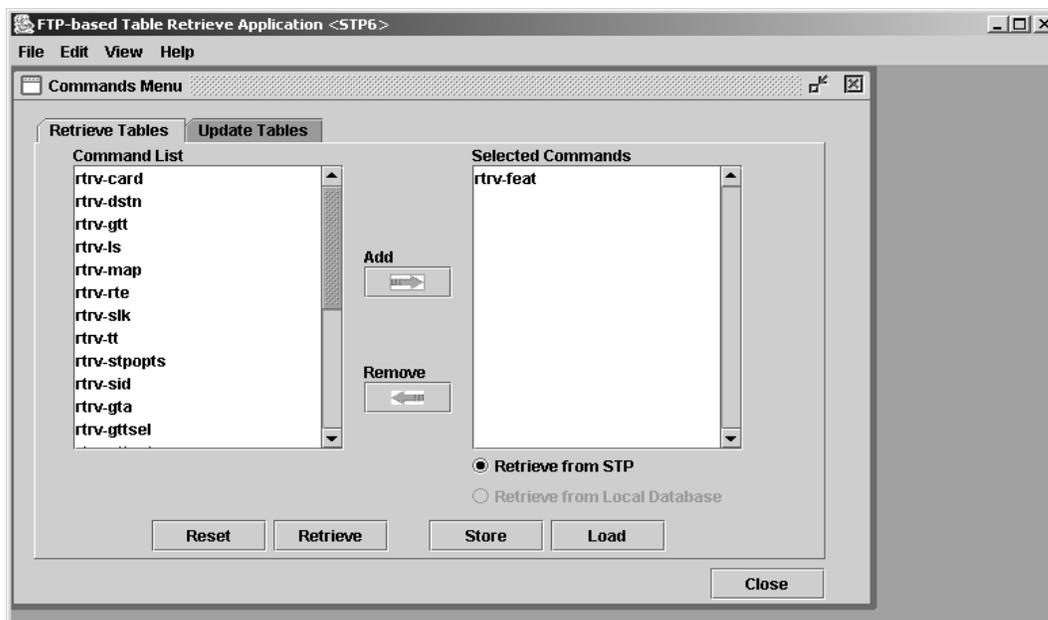


Figure 57. Adding a Range of Commands to the Selected Commands Box

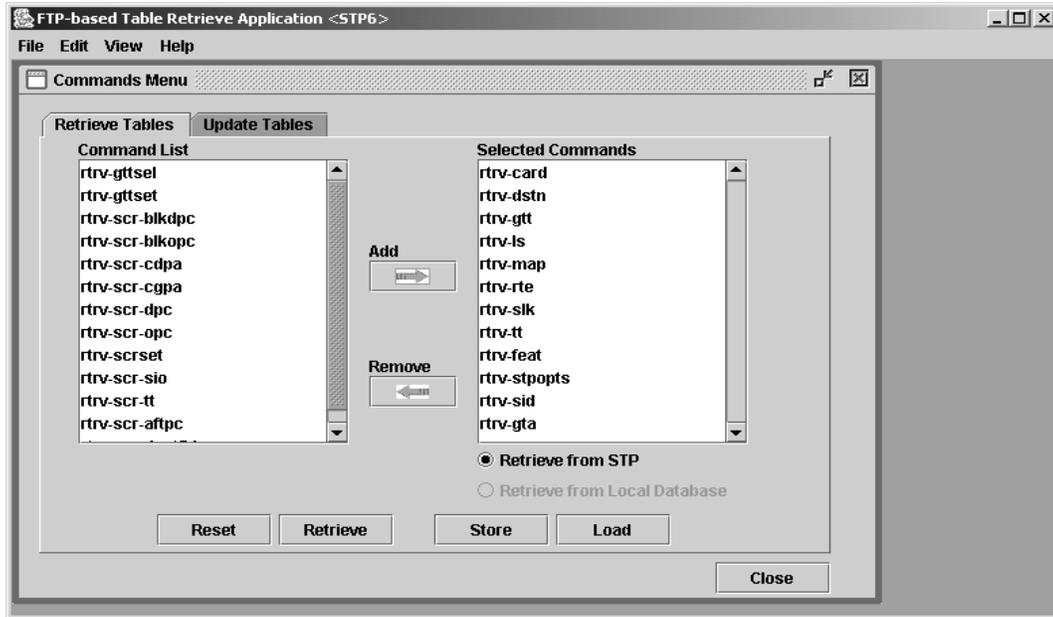
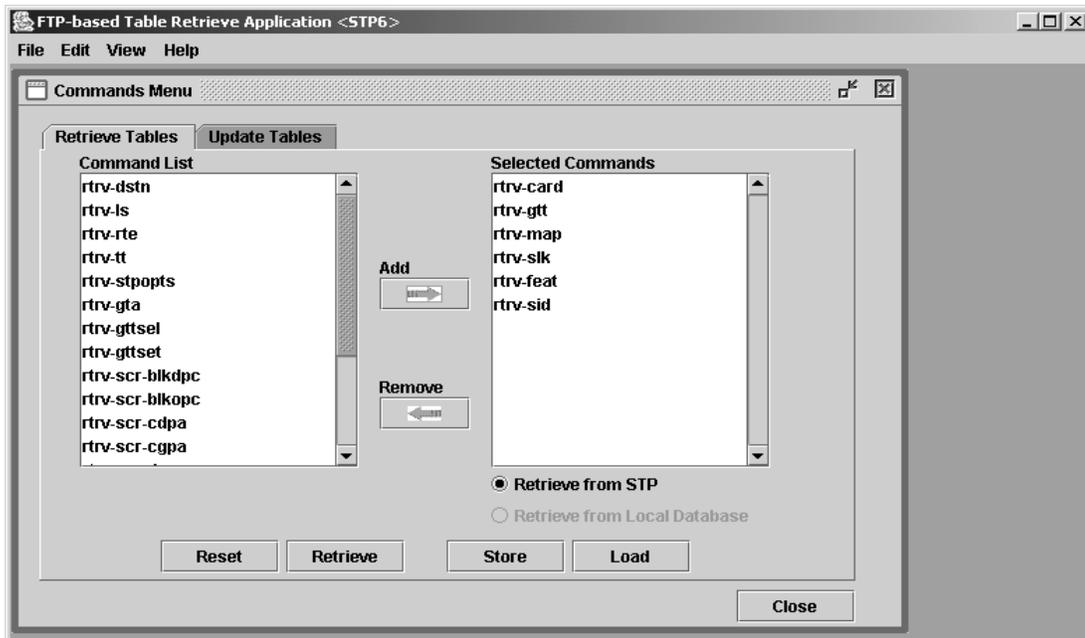


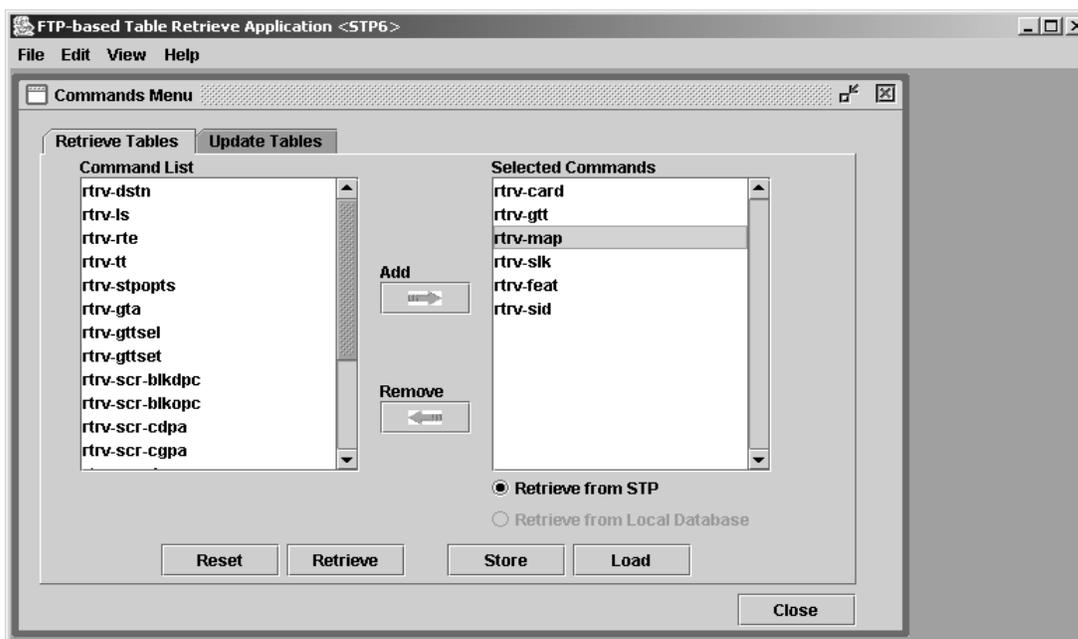
Figure 58. Adding Multiple Commands to Selected Commands Box



NOTE: If no commands are being moved from the **Selected Commands** box to the **Command List** box, skip step 4 and go to step 5.

4. To remove commands from the **Selected Commands** box, perform one of these steps:
 - a. In the **Selected Commands** box, click on the command to be removed and it is highlighted. Click the **Remove** button. The highlighted command is moved to the **Command List** box. See Figure 59.

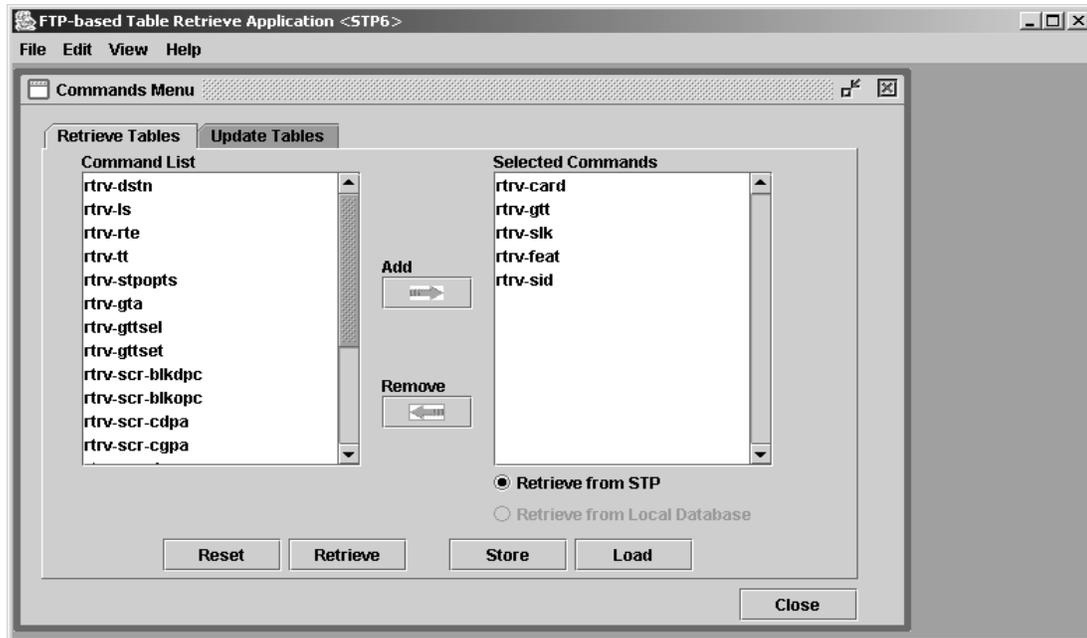
Figure 59. Command Selected to be Removed in the Selected Commands Box



- b. To select a range of multiple commands to be removed, click on the first command and while holding down the Shift key, click on the last command to be removed. Click the **Remove** button. All highlighted commands are moved to the **Command List** box.
- c. Hold down the Ctrl key and click on each of commands to be removed. Click the **Remove** button. Only the highlighted commands are moved to **Command List** side. See Figure 60 on page 65.

NOTE: When a command is removed it is placed at the bottom of the **Command List** box.

Figure 60. Command Removed from the Selected Commands Box



- d. Click the **Reset** button. All commands in the **Command List** box are moved to the **Selected Commands** box. All highlights in the **Selected Commands** box are removed.

NOTE: If command information from only the selected STP is being retrieved, and the Command Line Interface is not being used, skip step 5 and go to step 6.

5. To store the selected commands for the Command Line Interface, click the **Store** button on the **Commands Menu** window. The **Command Data Stored** window opens. See Figure 61.

Figure 61. Command Data Stored Window



Click **OK** to continue.

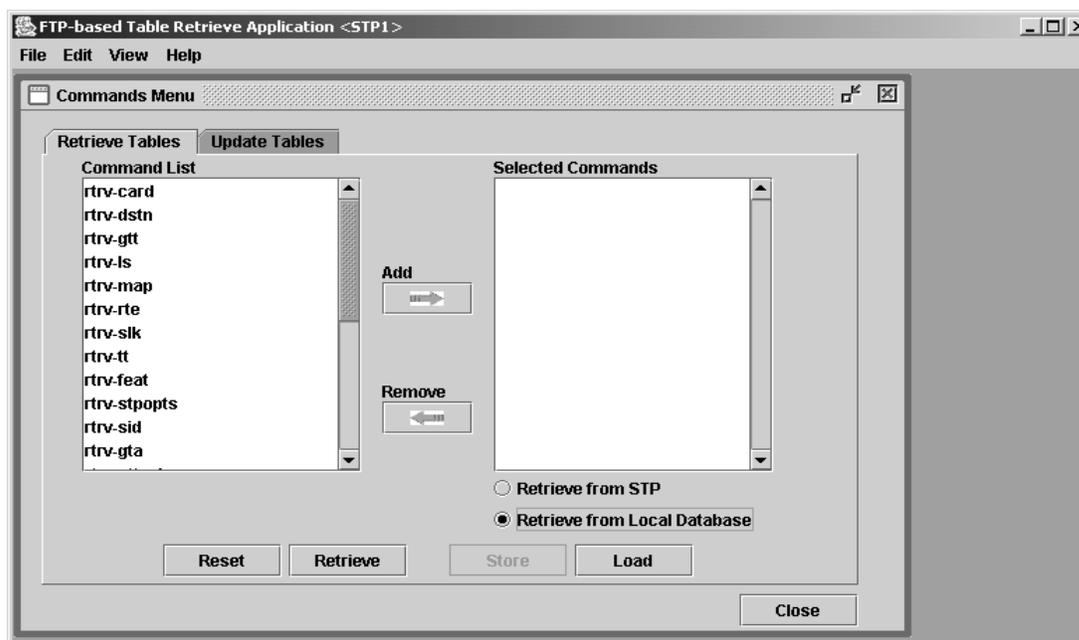
To verify what retrieve commands are stored, click the **Load** button. The stored commands appear in the **Selected Commands** box, as shown in Figure 56 on page 62, Figure 57 on page 63, or Figure 58 on page 63.

To use the Command Line Interface, go to the “Command Line Interface” section on page 75.

NOTE: If database tables are to be retrieved from the selected STP, skip step 6 and go to step 7.

6. To generate CSV files from database tables already retrieved from the selected STP, select the **Retrieve from Local Database** button after selecting the desired commands. See Figure 62. Click the **Retrieve** button.

Figure 62. Retrieving Database Tables from the Local Database



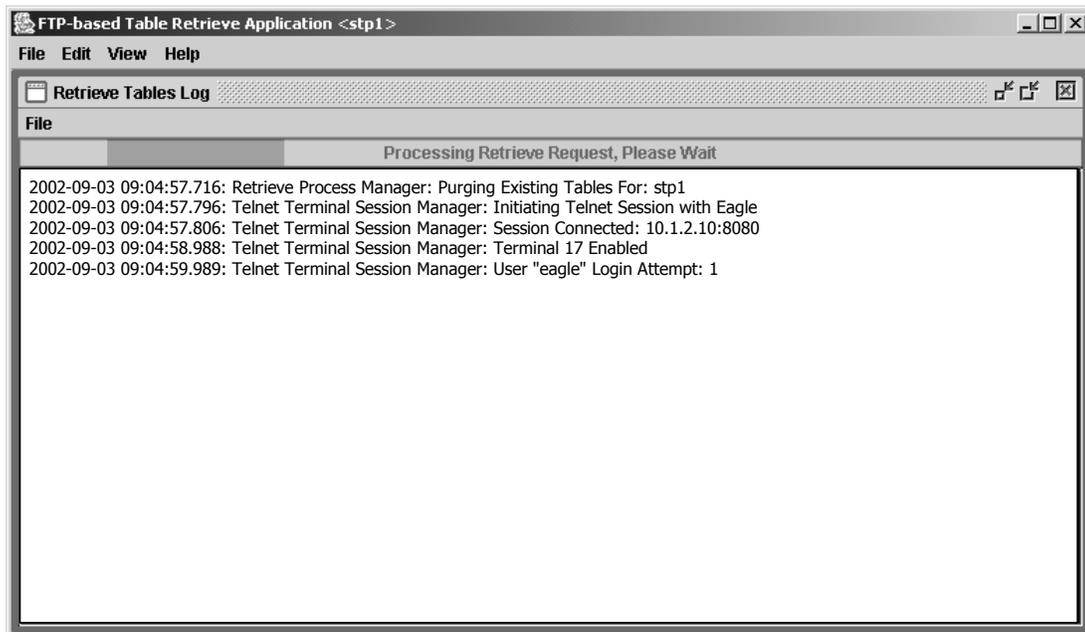
NOTE: If step 6 was performed, skip step 7. This procedure is finished.

7. Retrieve the database tables from the selected STP corresponding to the commands selected in step 2 by selecting the **Retrieve from STP** button, then click the **Retrieve** button. The **Retrieve Tables Log** window opens (see Figure 63) and displays the message "Processing Retrieve Request, Please Wait" until the retrieve process completes.

NOTE: The telnet terminals on the EAGLE 5 SAS to which FTRA will be connecting should have their terminal settings set to `all=no` (use the EAGLE 5 SAS command `chg-trm:trm=<telnet terminal>:all=no` to make this setting; use the EAGLE 5 SAS command `rtrv-trm` to verify the EAGLE 5 SAS terminal settings). On an STP with heavy UIM output, this prevents the FTRA's terminal from being flooded with unrelated output, which could unnecessarily backlog command responses during FTRA operation.

NOTE: If you are retrieving the database tables for any of these GTT commands (`rtrv-tt`, `rtrv-gtt`) and any of these EGTT commands (`rtrv-gttset`, `rtrv-gttset`, `rtrv-gta`), see the Caution on page 56.

Figure 63. Retrieve Tables Log Window - Processing Retrieve Request



This message is displayed until the retrieve process completes. The **Command Complete** window opens.

- a. If no errors occurred, the text "Retrieve Tables processing completed without errors." "Please check Retrieve Tables Log for Results." appears in the **Command Complete** window. See Figure 64 on page 68.

Figure 64. Command Complete Window Without Errors



Click **OK**, to continue.

- b. If errors occurred, the text "Retrieve Tables processing completed with errors." "Please check Retrieve Tables Log for Results." appears in the **Command Complete** window. See Figure 65.

Figure 65. Command Complete Window With Errors



The **Retrieve Table Log** window opens. See Figure 66 on page 69 and Figure 67 on page 70. Click **OK**, to continue.

Retrieve Tables Log

The Retrieve Tables Log contains the events of the retrieve processing and any error messages that may have occurred. The **Retrieve Tables Log** window is opened after database tables have been retrieved from an STP and is displayed until the retrieve processing is complete (see Figure 63 on page 67).

The log is automatically cleared when the next set of database tables are retrieved from an STP. Selecting **View > Retrieve Tables Log** from the menu also opens the **Retrieve Tables Log** window. See Figure 66 and Figure 67 on page 70.

Figure 66. Retrieve Tables Log Window without Errors

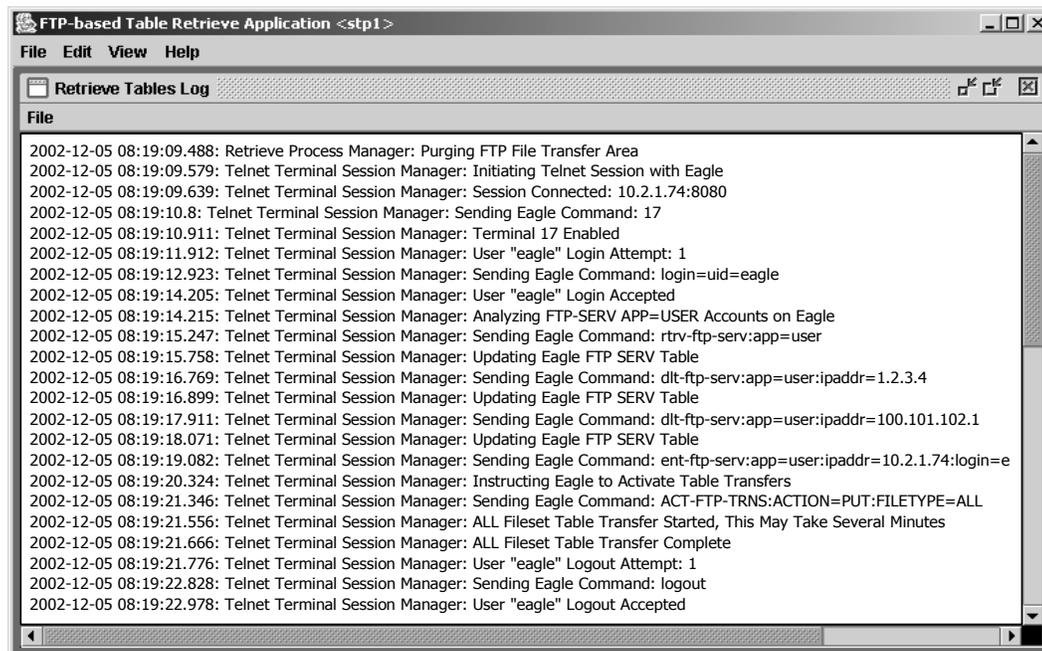
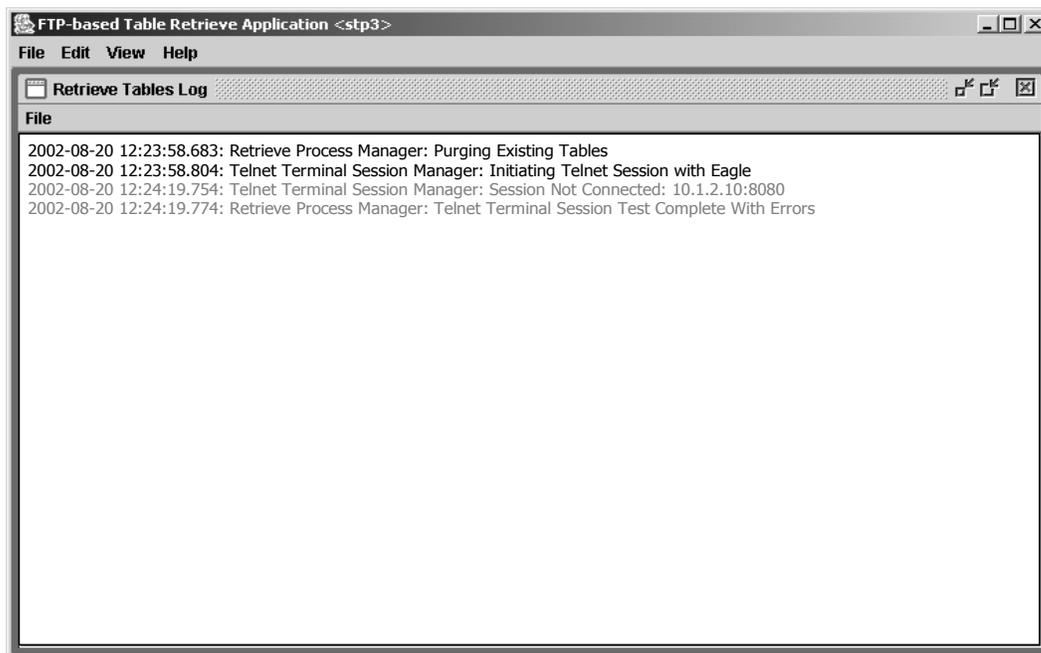


Figure 67. Retrieve Table Log with Errors

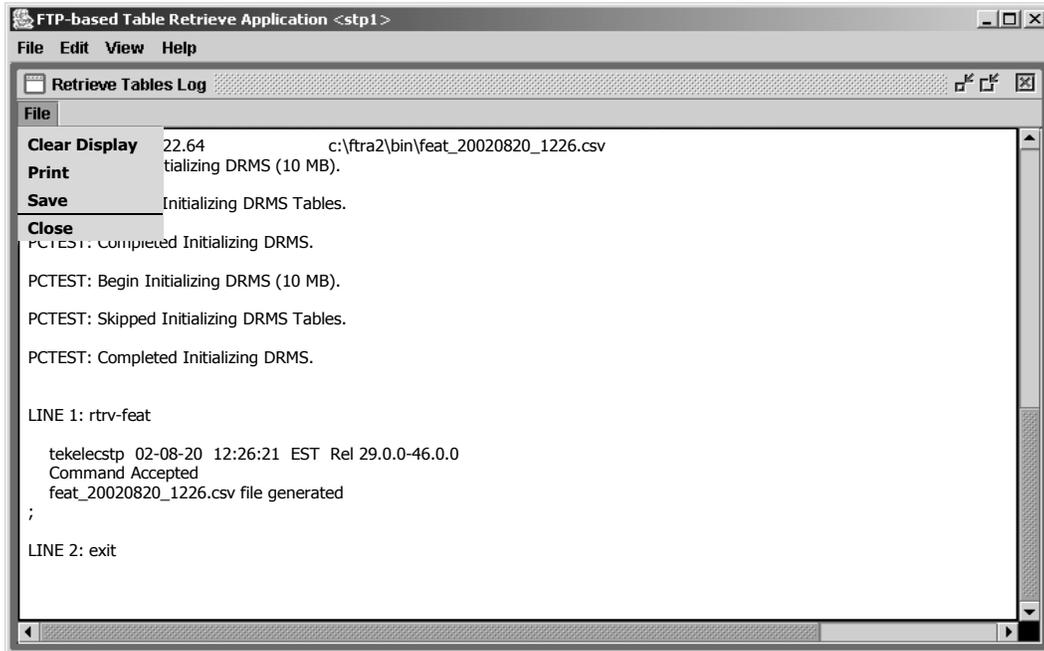


Retrieve Tables Log File Menu

The **File** menu in the **Retrieve Tables Log** window, shown in Figure 68 on page 71, provides these selections:

- Clearing the Retrieve Tables Log display
- Printing the Retrieve Tables Log
- Saving the Retrieve Tables Log to a file
- Closing the **Retrieve Tables Log** window.

Figure 68. File Menu in the Retrieve Tables Log Window



Clearing the Retrieve Tables Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is save to a file or printed before the display is cleared.

Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Clear Display** in the **Retrieve Tables Log** window. See Figure 68.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 69 on page 72. The **Retrieve Tables Log** window opens.

Figure 69. View Menu



3. Select **File > Clear Display** in the **Retrieve Tables Log** window. The Retrieve Tables Log display clears.

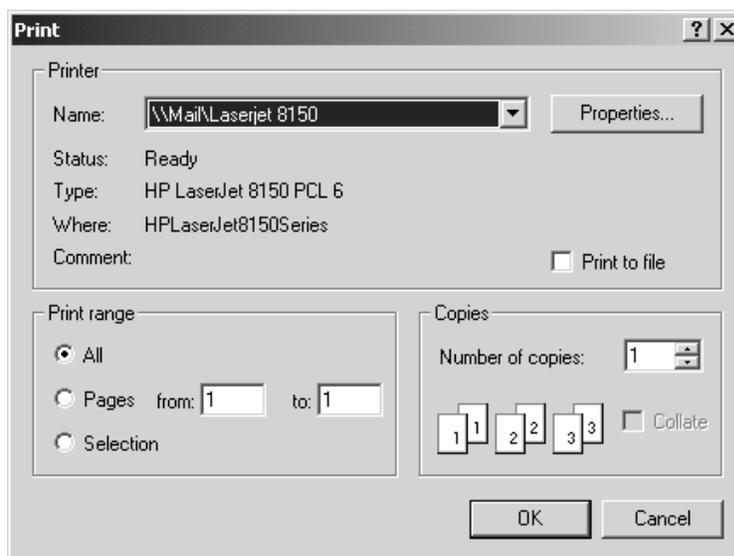
Printing the Retrieve Tables Log

Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Print** in the **Retrieve Tables Log** window. See Figure 68 on page 71.
2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 69. The Retrieve Tables Log opens.
3. Select **File > Print** in the **Retrieve Tables Log** window. The **Print** window opens. See Figure 70.

Figure 70. Print Window



4. Configure the printer settings.

5. To print the Retrieve Tables Log, click the **OK** button in the **Print** window. The current contents of the Retrieve Tables Log are printed.

6. If you decide not to print the Retrieve Tables Log, click the **Cancel** button in the **Print** window.

Saving the Retrieve Tables Log to a File

Procedure

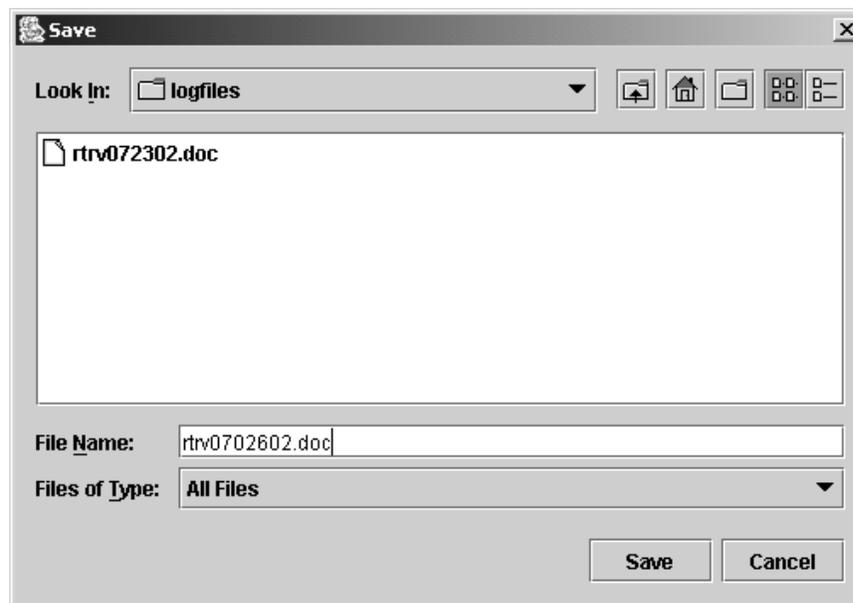
NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Save** in the **Retrieve Tables Log** window. See Figure 68 on page 71.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 69 on page 72. The **Retrieve Tables Log** window opens.

3. Select **File > Save** in the **Retrieve Tables Log** window. The **Save** window opens. See Figure 71.

Figure 71. Save Window



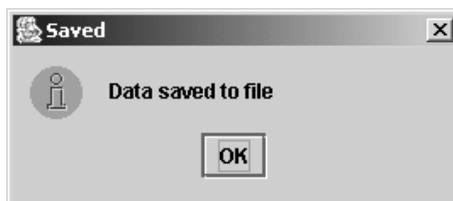
4. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.

NOTE: If you decide not to save the file, do not perform steps 5 and 6, but click **Cancel** in the **Save** window.

5. Click the **Save** button. A **Saved** file confirmation window opens with “Data saved to file.” See Figure 72.

Figure 72. Saved File Confirmation Window



6. To save the file, click **OK** in the **Saved** file confirmation window to continue.
-

Closing the Retrieve Tables Log Window

Procedure

1. Select **File > Close** in the **Retrieve Tables Log** window, or click the close window button in the upper right hand corner of the **Retrieve Tables Log** window. See Figure 68 on page 71. The **Retrieve Tables Log** window closes.
-

Command Line Interface

The FTRA Command Line Interface allows the user to retrieve the same database tables, using the EAGLE 5 SAS's retrieve commands, from all configured STPs in the STP configuration database. The **Store** and **Load** buttons in the **Retrieve Tables** window are used to select these retrieve commands. See "Retrieve Database Tables from an STP" on page 56.

Before the Command Line Interface can be started, you must exit the FTRA application. To start the Command Line Interface retrieve process, enter the `ftra -c` command at the DOS command prompt (in Windows) or at a shell command prompt (in UNIX).

The user can automate this retrieve process through the use of external scheduling software such as Task Scheduler (on the Windows platform) and "cron" (on the Unix platform). Please refer to the platform's scheduling program for specifics on how to use the external scheduling software. For example, on the Unix platform, enter the `man crontab` command.

Procedure – Command Line Interface Manual Start

1. Exit the FTRA application. See "Exit the FTRA" on page 14.

2. On the Windows platform, at a DOS prompt, go to the `\bin` directory of the FTRA `<install_directory>` location.

3. On the Unix platform, at a shell prompt, go to the `/bin` directory of the FTRA `<install_directory>` location.

4. Enter the `ftra -c` command (see Figure 73 on page 76 or Figure 74 on page 76). The stored `rtrv` commands are sent to all provisioned STPs. The data tables are retrieved and converted to the CSV file format.

Figure 73. FTRA Windows Command Line Interface



Figure 74. FTRA UNIX Command Line Interface



Procedure – Command Line Interface Automatic Start

1. Enter the `ftra -c` command, the path to the `bin` directory of the FTRA *<install_directory>*, the start time of the external scheduling software such as Task Scheduler (in Windows, see Figure 75) and “cron” (in Unix, see Figure 76 on page 78).

When the start time is reached, The stored `rtrv` commands are sent to all provisioned STPs. The data tables are retrieved and converted to CSV file format.

NOTE: If you are using “cron” on the Unix workstation, it might be necessary to create a wrapper script for FTRA, in order to correctly set environment variables. For an example of the wrapper script, see Figure 77 on page 78.

Figure 75. FTRA Windows Task Scheduler

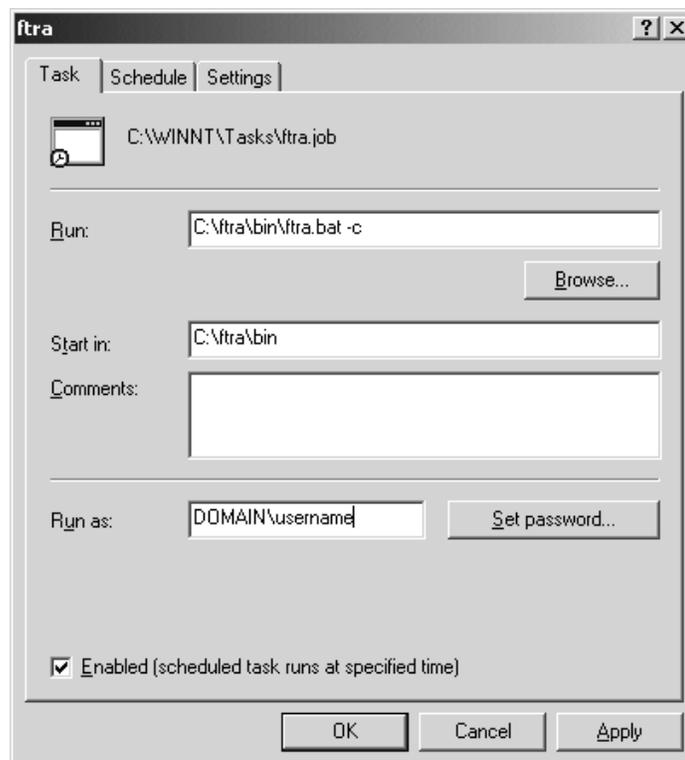


Figure 76. UNIX cron Job Scheduled using crontab

NOTE: The last line shows that the FTRA is scheduled to run at 3:00 AM Monday through Friday.

```

Text Editor - crontabjia1
File Edit Format Options Help
#ident "@(#)root 1.19 03/07/06 SMI" /* SVr4.0 1.1.3.1
#
# The rtc command is run to adjust the real-time clock if and when
# daylight savings time changes.
#
10 3 * * 0,4 /etc/cron.d/logchecker
10 3 * * 0 /usr/lib/newsyslog
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
0 3 * * 1-5 [ /tekelec/ftra/bin/ftra_wrapper > /tmp/wanda.log 2>1&
    
```

Figure 77. CRON FTRA Wrapper Script

```

Text Editor - ftra_wrapper
File Edit Format Options Help
[FTRA_HOME=/tekelec/ftra
JRE_HOME=/tekelec/java/j2re1.4.0_01
export FTRA_HOME
export JRE_HOME
/tekelec/ftra/bin/ftra -c
    
```

Updating Database Tables in the Selected STP

The **Update Tables** window (see Figure 78) is used to send EAGLE 5 SAS commands to the selected STP. The commands, in the form of a command file, are validated before being sent.

To send the command file to the selected STP, the command file is selected by entering the path and file name of the command file, or by selecting the file name of the command file from the **Select** window. The command file is then validated by clicking the **Validate** button in the **Update Tables** window. When the validation is completed, the **Update Validation Complete** window appears. From the **Update Validation Complete** window the command file can be edited, sent to the selected STP, or the **Update Validation Complete** window can be closed without sending the command file to the selected STP. The Update Tables Log contains the events of the command validation and any error messages that may have occurred.

Figure 78. Update Tables Window

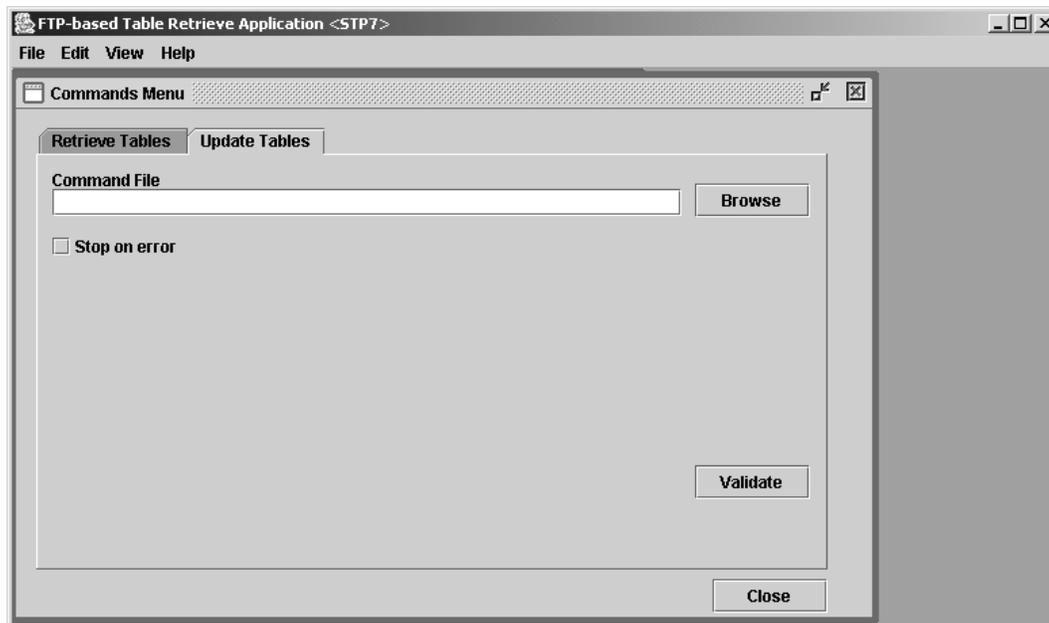


Table 6 shows the description of the fields and buttons in the **Update Tables** window.

Table 6. Update Tables Window Description

Item	Description
Fields	
Command File	The path and file name of the command file are entered here. A command file contains the EAGLE 5 SAS commands used to modify database tables of the STP.
Stop on error box	If the box is checked, and an error is found during the validation of the commands, the validation stops and no further commands are validated. If the box is not checked, all commands are processed regardless of errors. The error results are displayed in the Update Tables Log.
Buttons	
Browse	Opens the Select window to select the command file to send to the selected STP.
Validate	Validates the EAGLE 5 SAS commands using the offline database.
Close	Closes the Commands Menu window.

Validating a Command File

Procedure

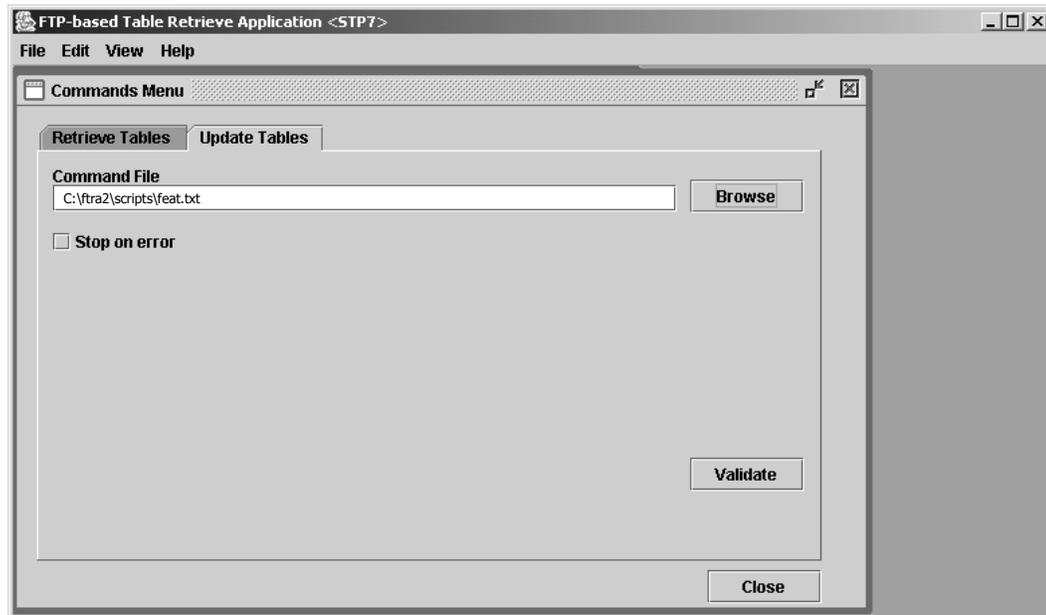
1. Select **Edit > Commands > Update Tables** in the **FTP-based Table Retrieve Application** window. See Figure 79. The **Update Tables** window opens. See Figure 78 on page 79.

Figure 79. Edit Menu



2. Perform one of these steps.
 - a. Enter the path and name of the command file in the **Command File** field. See Figure 80.

Figure 80. Update Tables with a Command File Selected



- b. Click the **Browse** button. The **Select** window is opened. See Figure 81 on page 82. Find the folder containing the command file and click on the command file name. The command file name is highlighted. Click the **Select** button. The **Select** window disappears and the **Update Tables** window appears with the path and file name of the selected command file entered in the **Command File** field.

If you wish to cancel the command file selection process in the **Select** window, click the **Cancel** button.

Table 7 on page 82 shows the description of the buttons in the **Select** window.

Figure 81. Select Window

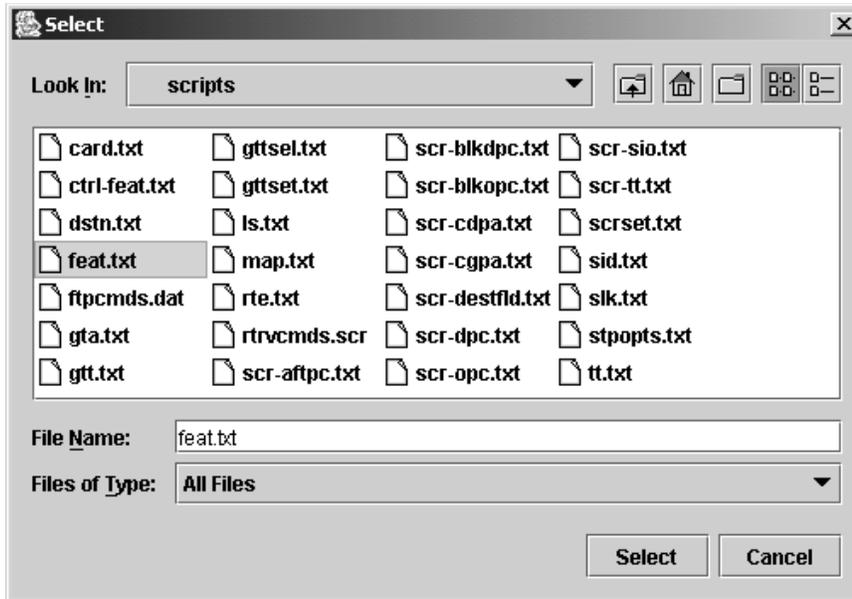
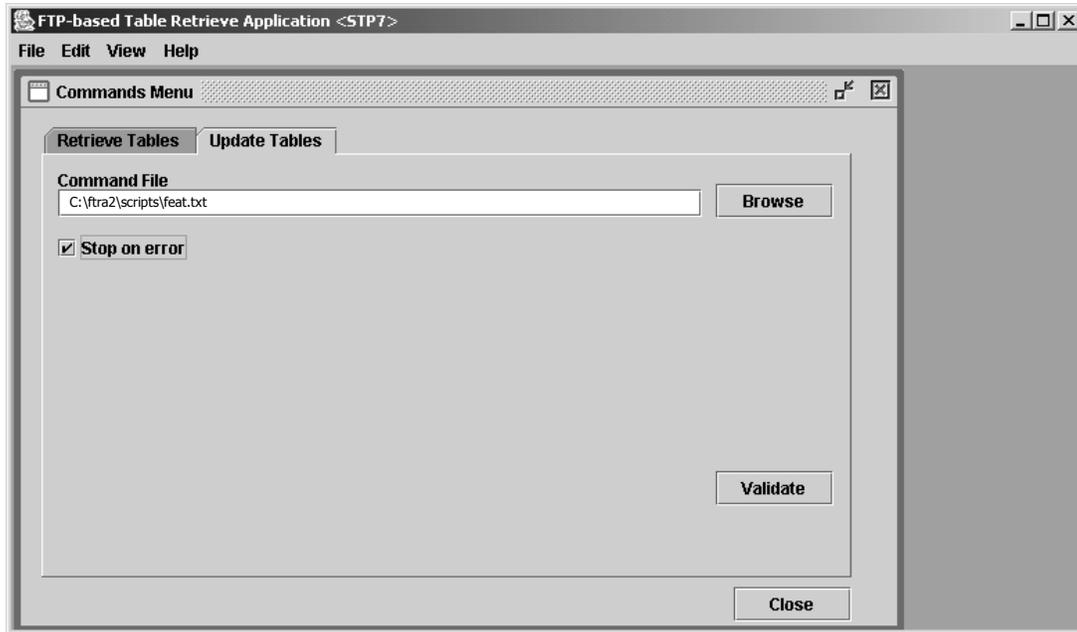


Table 7. Select Window Descriptions

Item	Description
Fields	
Look in:	A drop down menu allowing the user to browse through the directory structures.
File Name:	The name of the file to be selected.
Files of type:	A drop down menu that selects all files.
Buttons	
Select	The contents of the File Name field and the path to the filename is loaded into the Command File field of the Update Tables window.
Cancel	Closes the Select window.

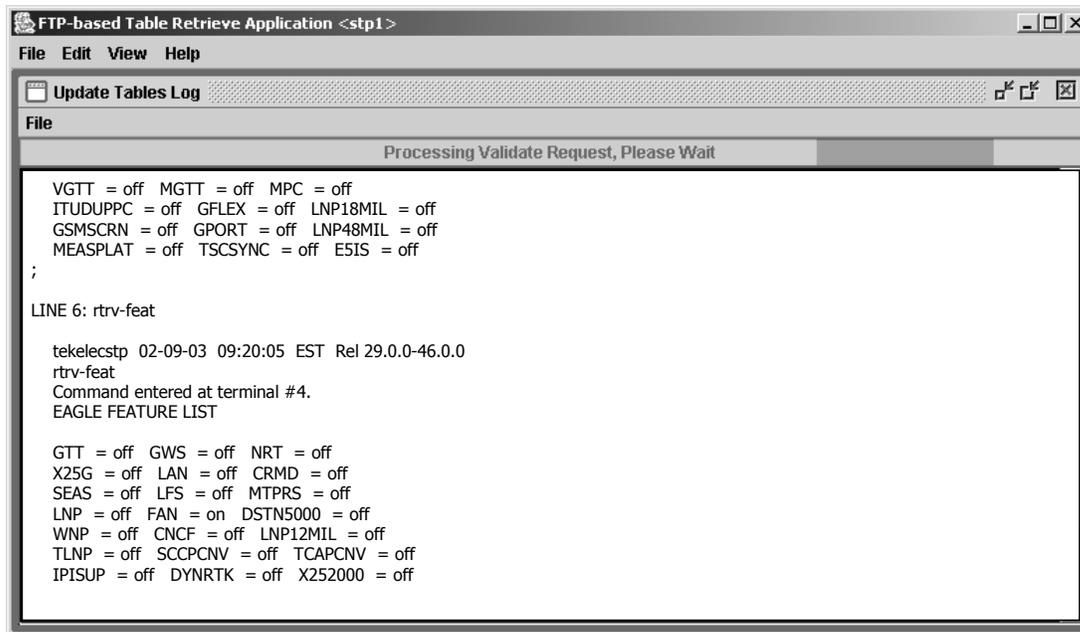
3. If you wish to have the command validation stop if any errors are found, check the **Stop on error** box in the **Update Tables** window. See Figure 82. If you wish to have the command validation processed regardless of any errors, uncheck the **Stop on error** box. The error results are displayed in the Update Tables Log.

Figure 82. Update Tables Window with a Command File Selected and Stop on Error Box Checked



- Click the **Validate** button. The **Update Tables Log** window opens at the beginning of the validate process and displays the “Processing Validate Request, Please Wait” message until the validation of the command file is complete. See Figure 83.

Figure 83. Update Tables Log Window - Processing Retrieve Request



The **Update Validation Complete** window opens. See the “Update Validation Complete Window” section on page 85.

- The **Update Tables Log** window opens. It contains the events and error messages generated during the validation. See Figure 93 on page 90, Figure 94 on page 91, and Figure 95 on page 92 for Update Tables Log examples.

NOTE: If there is no entry in the **Command File** field and the **Validate** button is clicked, a warning message is displayed stating that a command file name must be entered. See Figure 84.

Figure 84. Must Enter Command Script File Name Message



Update Validation Complete Window

When the command validation has completed, the **Update Validation Complete** window opens notifying the user if the commands validated with or without errors. From the **Update Validation Complete** window, the command file can be edited, sent to the selected STP, or the window can be closed without sending the command file to the selected STP. See Figure 85.

Figure 85. Update Validation Complete Window without Errors

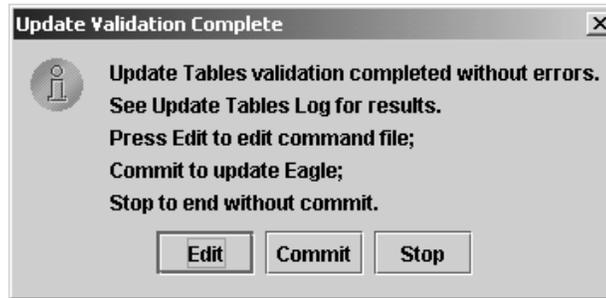


Table 8 shows the description of the buttons in the **Update Validation Complete** window.

Table 8. Update Validation Complete Window Description

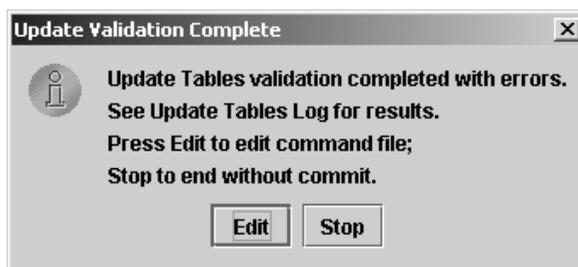
Item	Description
Edit	Opens the Command File Editor window and allows the user to make changes to the command file. To edit a command file, go to the “Editing a Command File” section on page 87.
Commit	Sends the commands in the command file to the STP. A Command Complete window opens and the Update Tables Log is updated. See the “Sending a Command File to the Selected STP” section on page 86. If the Update Tables validation completed with errors the Commit button is not displayed.
Stop	Closes the Update Validation Complete window without sending the commands in the command file to the STP.

Update Validation Complete Window with Errors

If the **Update Validation Complete** window shows that errors have occurred, the command file can be edited or the window can be closed without sending the command file to the selected STP. See Figure 86. There is no **Commit** button in this window; this prevents the sending of invalid commands.

To fix the errors in the command file, click the **Edit** button, then go to the “Editing a Command File” section on page 87.

Figure 86. Update Validation Complete Window with Errors



Sending a Command File to the Selected STP

To send the command file, click the **Commit** button in the **Update Validation Complete** window. The **Commit** button is shown only on the **Update Validation Complete without Errors** window. See Figure 85 on page 85. The validated command file is sent to the selected STP.

The **Command Complete** window opens and displays: “Update Tables processing completed without errors” and “Please check Update Tables Log for results.” See Figure 87. Click **OK**, to continue. The Update Tables Log contains the commit processing events. See Figure 93 on page 90.

Figure 87. Command Complete Window



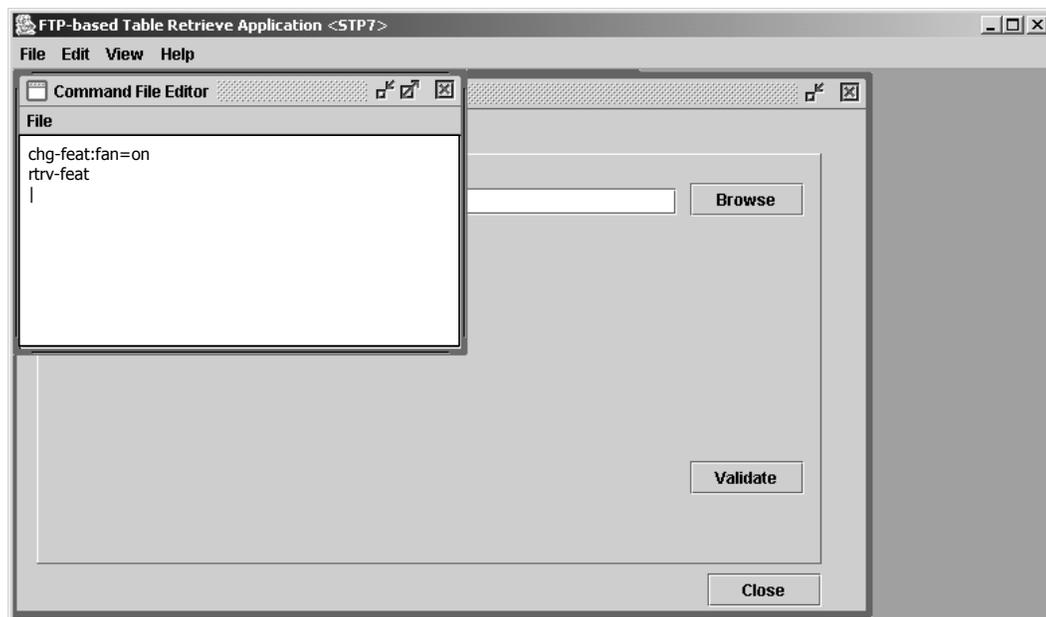
Stop Without Sending or Editing a Command File

To stop the process without sending or editing a command file, click the **Stop** button in the **Update Validation Complete** window. See Figure 85 on page 85. The **Update Validation Complete** window is closed. No changes are made to the command file and the command file is not sent to the selected STP.

Editing a Command File

To edit a command file, click the **Edit** button in the **Update Validation Complete** window. The **Command File Editor** window is opened. See Figure 88.

Figure 88. Command File Editor Window



When the editing is complete, the command file can be saved without sending the command file to the selected STP, saved and sent to the selected STP without any further validation, or the command file can be closed without saving the changes to the command file.

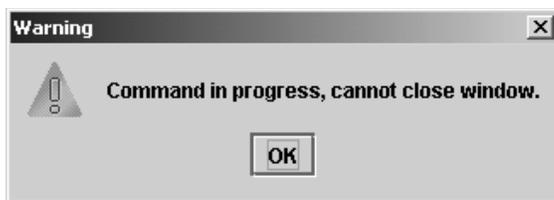
Procedure

1. Click the **Edit** button in the **Update Validation Complete** window. See Figure 85 on page 85. The **Command File Editor** window opens. See Figure 88 on page 87.

NOTE: The hourglass is displayed until the **Command File Editor** window is closed.

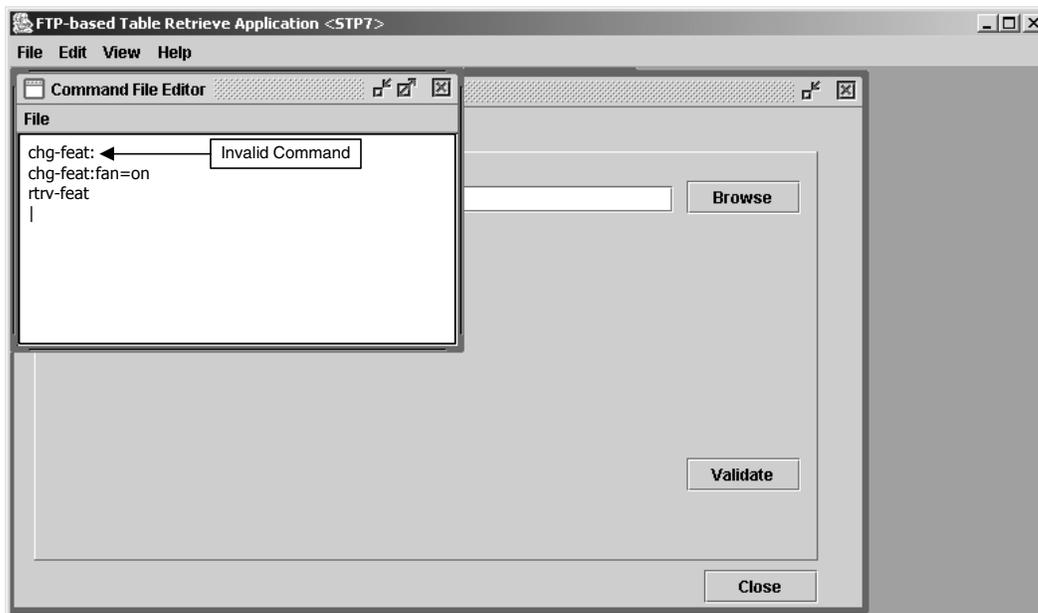
NOTE: If an attempt is made to close the **Update Tables** window while the **Command File Editor** window is opened, the **Command In progress, Cannot Close Window** warning message is displayed. See Figure 89.

Figure 89. Command In progress, Cannot Close Window



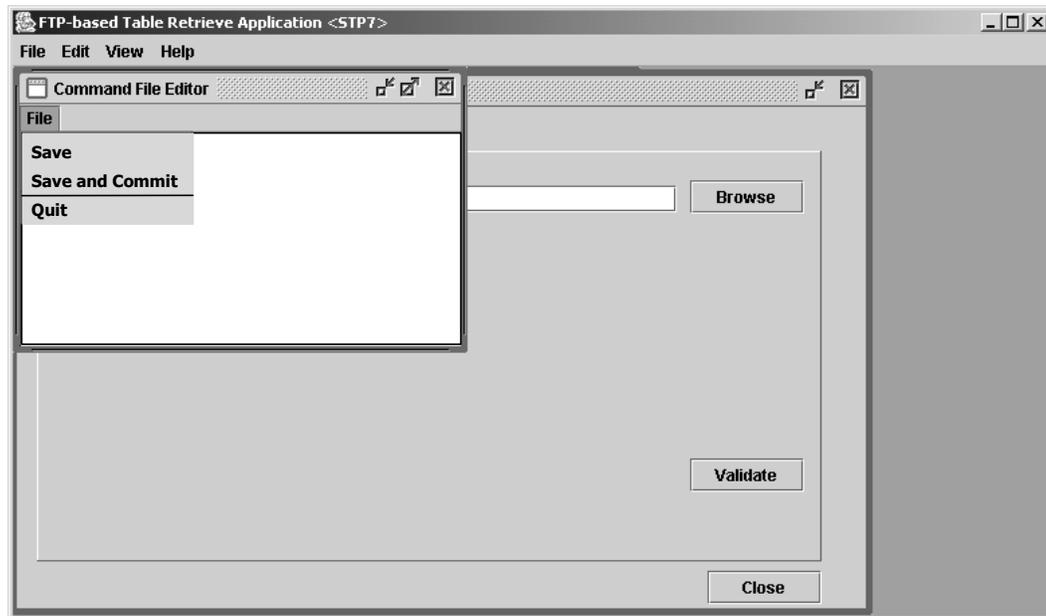
2. Edit the command file. Figure 90 shows a command file with an invalid command. In this example, the invalid command is `chg-feat:.`. This command should be removed from the command file, or have a correct parameter and value added to it.

Figure 90. Command File Editor with Invalid Command



3. When the editing is complete, perform one of these steps.
 - a. Select **File > Save** from the **Command File Editor** window (see Figure 91). The command file is saved and the **Command File Editor** window remains open. The command file is not sent to the selected STP. The command file can be validated again in the **Update Tables** window.

Figure 91. File Menu in the Command File Editor Window



- b. Select **File > Save and Commit** from the **Command File Editor** window (see Figure 91). The command file is saved and the **Command File Editor** window closes. The **Command Complete** window opens and displays: "Update Tables processing completed without errors. Please check Update Tables Log for results." Click **OK**, to continue. See Figure 92. The command file is sent to the selected STP. The Update Tables Log contains the commit processing events. See Figure 93 on page 90

Figure 92. Command Complete Window



- c. Select **File > Quit** from the **Command File Editor** window (see Figure 91). The **Command File Editor** window closes. The command file is not sent to the selected STP. If changes to the command file have been made, a window is displayed asking if you want to save the changes.

Update Tables Log Window

The Update Tables Log contains the processing events and any error messages that may have occurred during the validation and sending of a command file. The **Update Tables Log** window is opened at the beginning of the validation process and displays "Processing Validate Request, Please Wait" (Figure 83 on page 84) until the command file validation is completed. The **Update Tables Log** window is automatically cleared when the next command file validation is started. Selecting **View > Update Tables Log** from the menu can also open the **Update Tables Log** window.

See Figure 93, Figure 94 on page 91, Figure 95 on page 92, and Figure 96 on page 93 for the **Update Tables Log** window examples.

Figure 93. Update Tables Log Window after the Commit Command Completed

```

File
ITUMTPRS = off SLSOCB = off EGTT = off
VGTT = off MGTT = off MPC = off
ITUDUPPC = off GFLEX = off LNP18MIL = off
GSMSCRN = off GPORT = off LNP48MIL = off
MEASPLAT = off TSCSYN = off E5IS = off
;
LINE 4: exit
2002-08-21 09:17:50.844: Telnet Terminal Session Manager: Initiating Telnet Session with Eagle
2002-08-21 09:17:51.034: Telnet Terminal Session Manager: Session Conncted: 66.26.93.175:8080
2002-08-21 09:17:52.276: Telnet Terminal Session Manager: Terminal 17 Enabled
2002-08-21 09:17:53.287: Telnet Terminal Session Manager: User "eagle" Login Attempt: 1
2002-08-21 09:17:55.521: Telnet Terminal Session Manager: User "eagle" Login Accepted
2002-08-21 09:17:55.651: Telnet Terminal Session Manager: Sending Command Updates to Eagle
2002-08-21 09:17:55.781: Telnet Terminal Session Manager: Sending Eagle Command:
2002-08-21 09:17:56.913: Telnet Terminal Session Manager: Sending Eagle Command: chg-feat:fan=on
2002-08-21 09:17:58.044: Telnet Terminal Session Manager: Sending Eagle Command: rtrv-feat
2002-08-21 09:17:59.176: Telnet Terminal Session Manager: Sending Eagle Command: exit
2002-08-21 09:18:00.308: Telnet Terminal Session Manager: Sending Eagle Command: exit
2002-08-21 09:18:01.439: Telnet Terminal Session Manager: Sending Eagle Command: exit
2002-08-21 09:18:02.571: Telnet Terminal Session Manager: User "eagle" Logout Attempt: 1
2002-08-21 09:18:03.703: Telnet Terminal Session Manager: User "eagle" Logout Accepted
2002-08-21 09:18:04.103: Commit Process Manager: Telnet Terminal Session Complete Without Errors

```

Figure 94. Update Tables Log

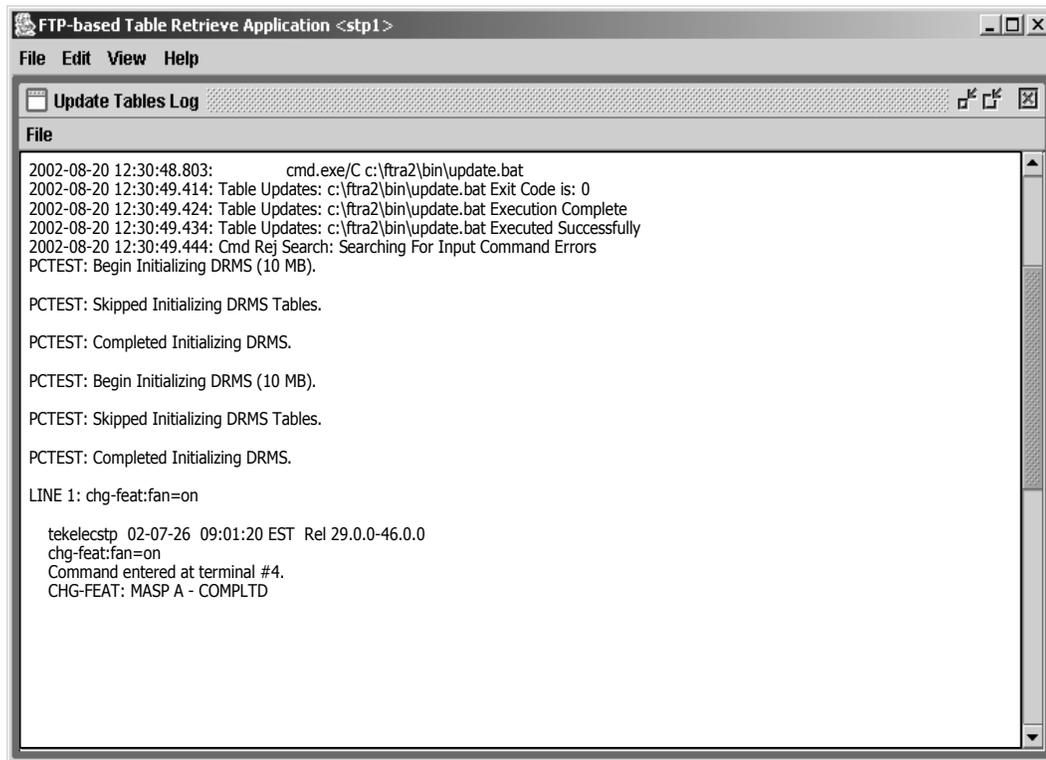


Figure 95. Update Tables Log with Stop on Error Box Checked in the Update Tables Window

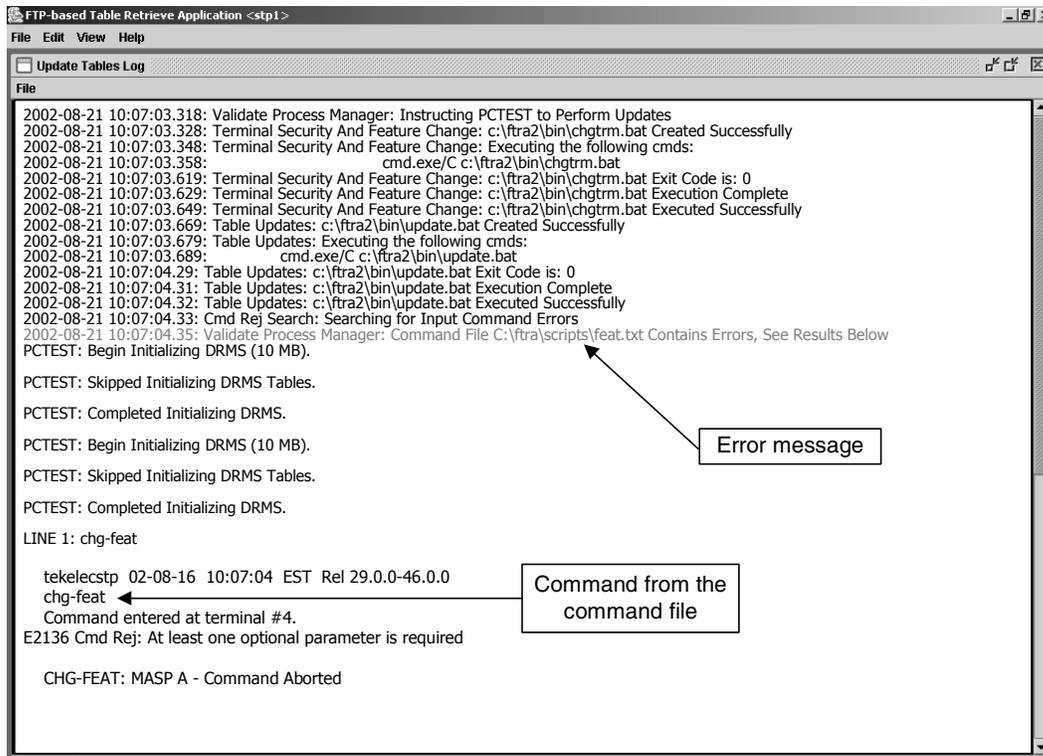


Figure 96. Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window

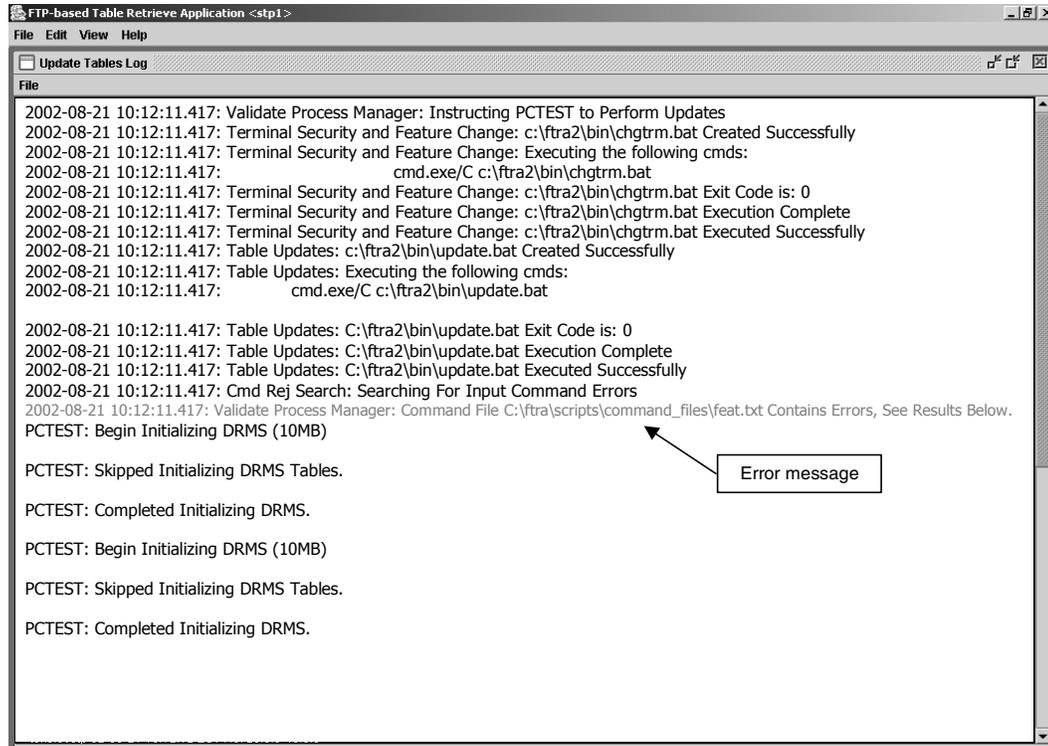
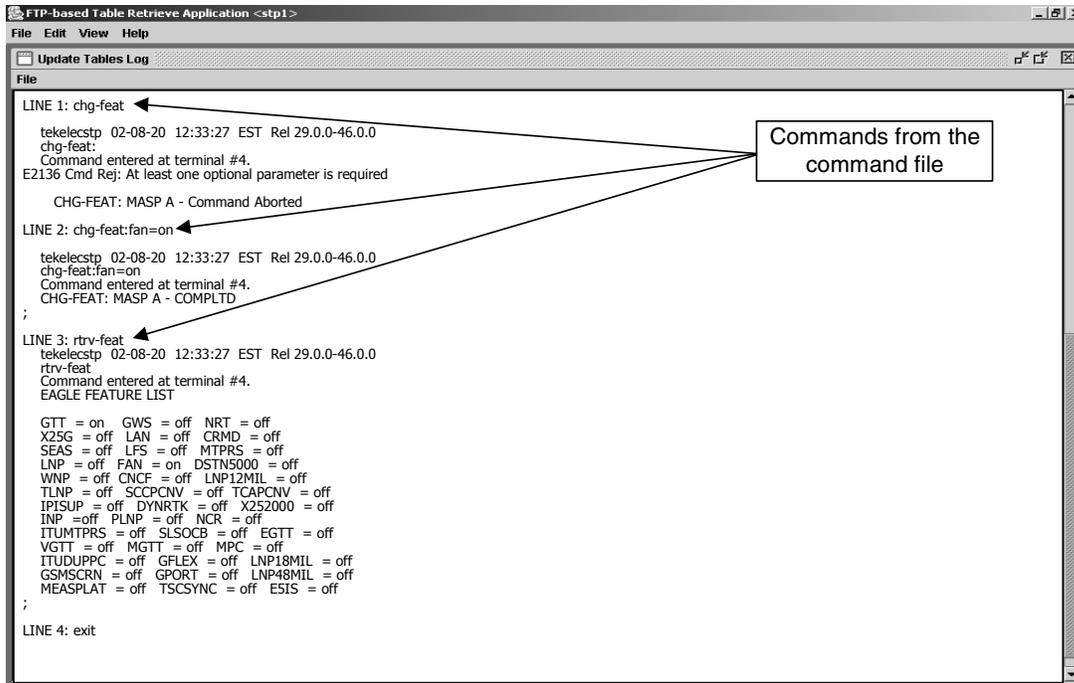


Figure 90 on page 88 shows an example of a command file that produced the error shown in Figure 96.

Figure 96. Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window (Continued)

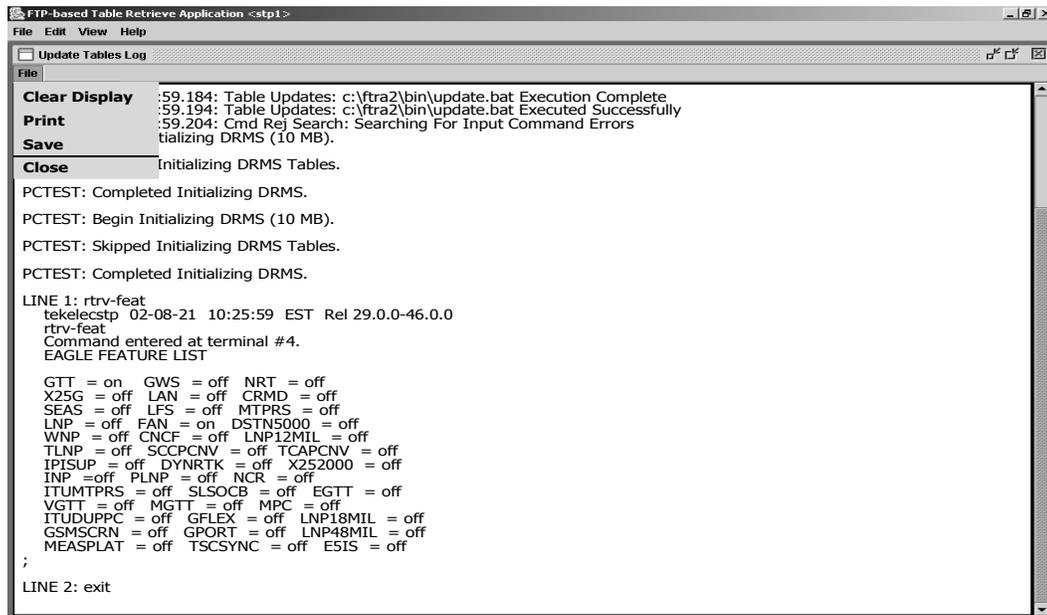


File Menu in the Update Tables Log Window

The **File** menu in the **Update Tables Log** window, shown in Figure 97 on page 95, provides the user with the following selections:

- Clearing the Update Tables Log display.
- Printing the Update Tables Log.
- Saving the Update Tables Log to a file.
- Closing the **Update Tables Log** window.

Figure 97. File Menu in the Update Tables Log Window



Clearing the Update Tables Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is save to a file or printed before the display is cleared.

Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Clear Display** in the **Update Tables Log** window. See Figure 97.
2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 98. The **Update Tables Log** window opens.

Figure 98. View Menu



3. Select **File > Clear Display** in the **Update Tables Log** window. The Update Tables Log display clears.
-

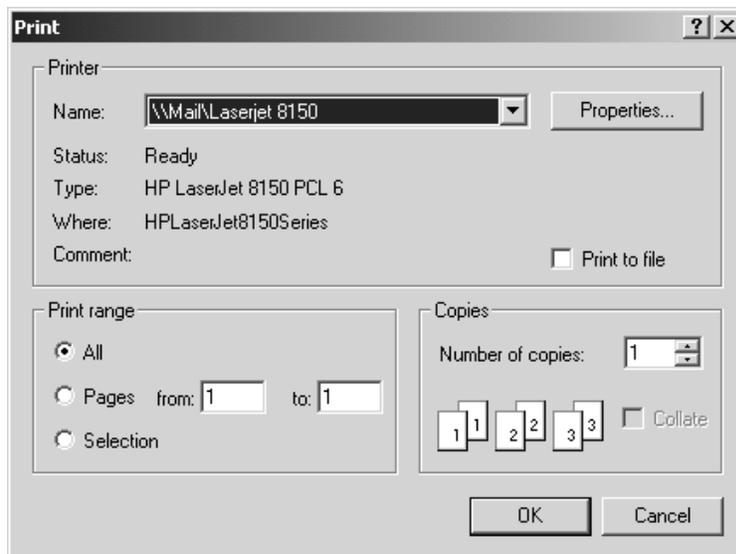
Printing the Update Tables Log

Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Print** from the **Update Tables Log** window. See Figure 97 on page 95.
-
2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 98 on page 95. The Update Tables Log opens.
-
3. Select **File > Print** from the **Update Tables Log** window. The **Print** window opens. See Figure 99.

Figure 99. Print Window



4. Configure the printer settings.
-

5. To print the Update Tables Log, click the **OK** button. The current contents of the Update Tables Log are printed.
6. If you do not wish to print the Update Tables Log, click the **Cancel** button.

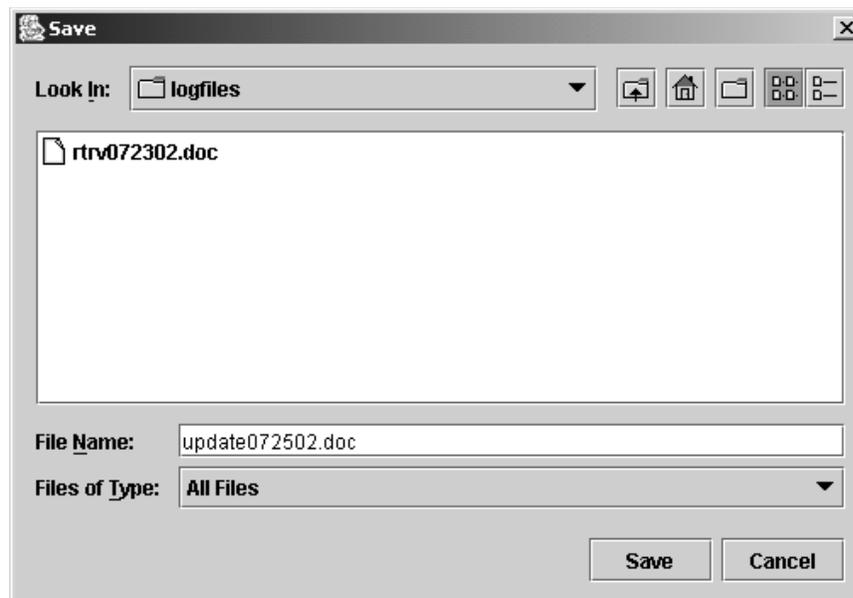
Saving the Update Tables Log to a File

Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Save** from the **Update Tables Log** window. See Figure 97 on page 95.
2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 98 on page 95. The Update Tables Log opens.
3. Select **File > Save** in the **Update Tables Log** window. The **Save** window opens. See Figure 100.

Figure 100. Save Window

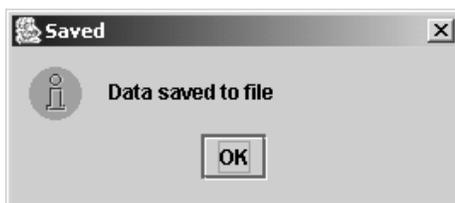


4. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file even if it was saved as a .txt file.

5. To save the file, click the **Save** button. A **Saved** file confirmation window opens with “Data saved to file.” See Figure 101. Click **OK**, to continue.

Figure 101. Saved Confirmation Window



6. If you do not wish to save the file, click the **Cancel** button in the **Save** window.
-

Closing the Update Tables Log Window

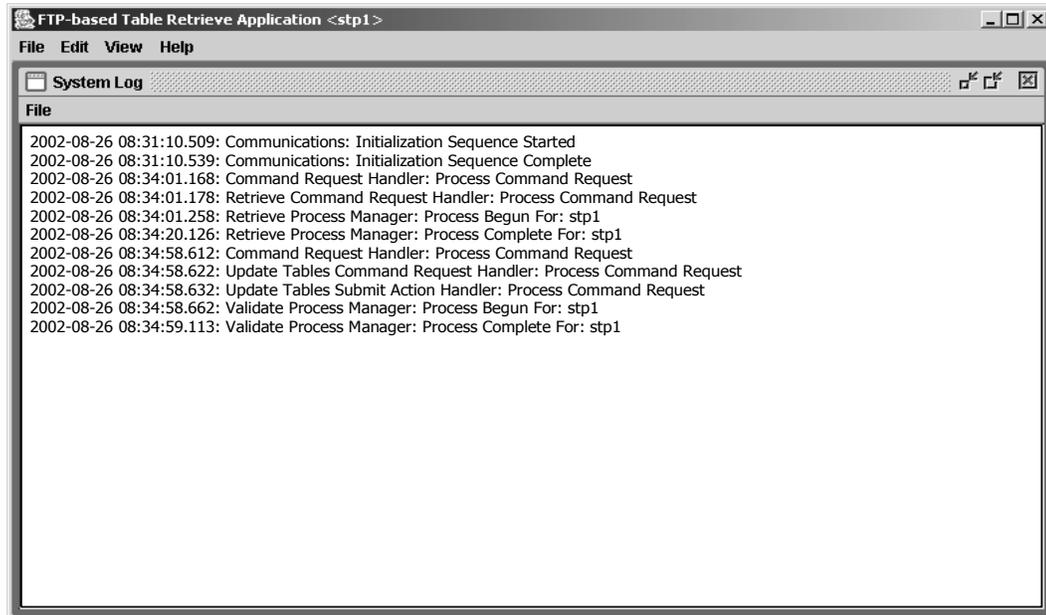
Procedure

1. Select **File > Close** in the **Update Tables Log** window, or click the close window button in the upper right hand corner of the **Update Tables Log** window. See Figure 97 on page 95. The **Update Tables Log** window closes.
-

The System Log

The System Log contains an event history and any errors that have occurred when database tables are retrieved from an STP, or command files are sent to an STP. See Figure 102.

Figure 102. System Log Window

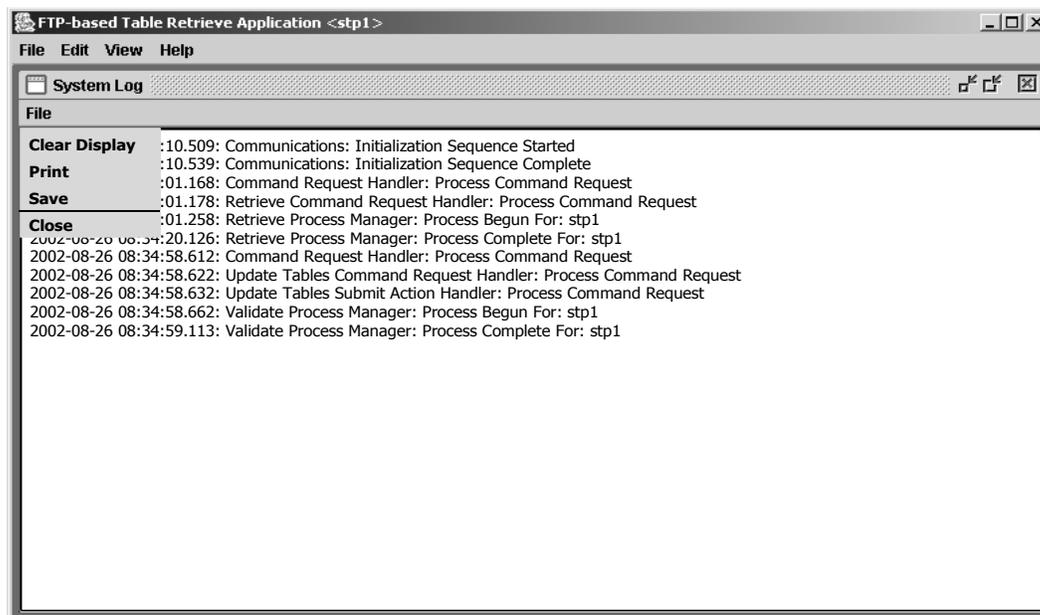


File Menu in the System Log Window

The **File** menu in the **System Log** window, shown in Figure 103 on page 100, provides these selections:

- Clearing the System Log display.
- Printing the System Log.
- Saving the System Log to a file.
- Closing the **System Log** window.

Figure 103. File Menu in the System Log Window



Clearing the System Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is saved to a file or printed before the display is cleared.

Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 104. The **System Log** window opens.

Figure 104. View Menu



2. Select **File > Clear Display** in the **System Log** window. See Figure 103. The System Log display clears.
-

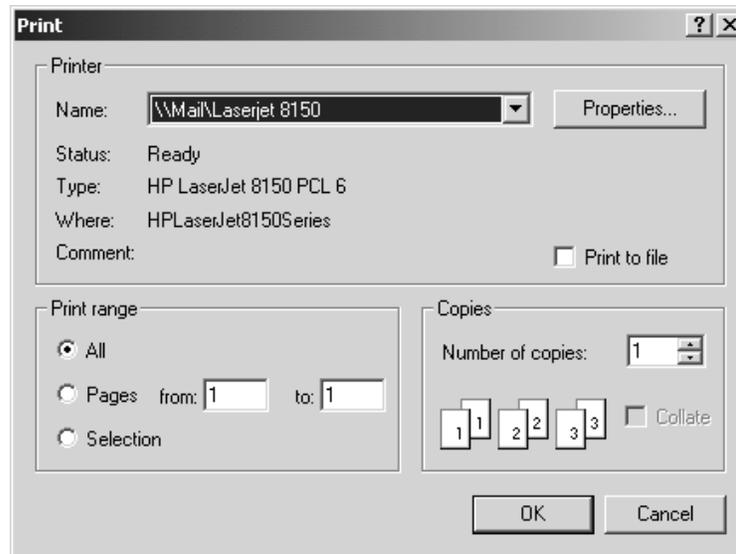
Printing the System Log

Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 104 on page 100. The **System Log** window opens.

2. Select **File > Print** in the **System Log** window. The **Print** window opens. See Figure 105.

Figure 105. Print Window



3. Configure the printer settings.

 4. To print the System Log, click the **OK** button. The current contents of the System Log are printed.

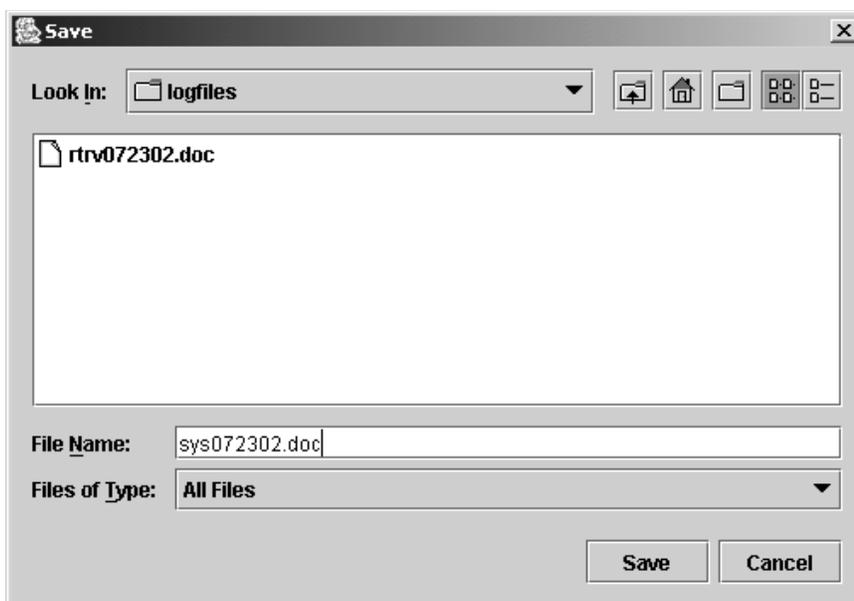
 5. If you decide not to print the System Log, click the **Cancel** button.
-

Saving the System Log to a File

Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 104 on page 100. The System Log opens.
 2. Select **File > Save** in the **System Log** window. The **Save** window opens. See Figure 106.
-

Figure 106. Save Window

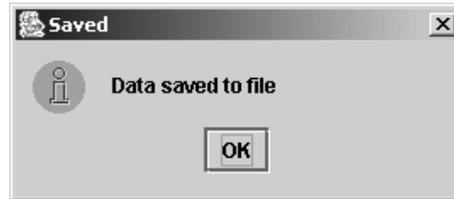


3. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file even if it was saved as a .txt file.

4. To save the System Log to a file, click the **Save** button. A **Saved** file confirmation opens with “Data saved to file”. See Figure 107. Click **OK** to continue.

Figure 107. Saved Confirmation Window



-
5. If you do not wish to save the System Log to a file, click the **Cancel** button in the **Save** window.
-

Closing the System Log Window

Procedure

1. Select **File > Close** in the **System Log** window, or click the close window button in the upper right hand corner of the **System Log** window. The **System Log** window closes.
-

About FTRA Window

The **About FTRA** window displays the version level of the FTRA and copyright information. To display the **About FTRA** window, select **Help > About** in the **FTP-based Table Retrieve Application** window. See Figure 108.

Figure 108. Help Menu



The **About FTRA** window opens. See Figure 109. Click **OK**, to continue.

Figure 109. Typical About FTRA Window



SSH/SFTP Error Codes

Table 9 and Table 10 on page 119 contain a list of the error codes that can be generated when making a secure connection between the FTRA, version 2.0 or greater, and the EAGLE 5 SAS. Each error code contains a brief description of the error and the suggested recovery action.

This section also contains procedures, following Tables 9 and 10, for testing connectivity and network problems, and to verify that the setup for making secure connections is correct.

If secure connections to the EAGLE 5 SAS cannot be made, verify that the Eagle OA&M IP Security Enhancements feature is enabled and activated by entering the `rtrv-ctrl-feat` command at the EAGLE 5 SAS before performing any of the actions in Tables 9 and 10. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the “Activating the Eagle O&AM IP Security Enhancements Controlled Feature” procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature.

If any of the errors shown in Table 9 or Table 10 on page 119 are encountered after the recovery procedure is verified, contact the Customer Care Center. Refer to page 3 for the contact information.

Table 9. FTP/SFTP/SSH Error Codes

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
User Errors		
594	Invalid Path	Verify that the path is valid in the FTP Server Configuration Menu window (see Figure 43 on page 52).
598	The SSHD daemon is not running on the destination system or the server IP address unavailable.	Verify that the IP address exists on network with a ping (Refer to the “Connectivity Test - I” section on page 122 and the “Connectivity Test - II” section on page 123). If the IP address exists on network then verify that SSHD daemon is running on the destination machine using the <code>ps -ef grep sshd</code> command.
629	The SFTP daemon is not running	Verify that the subsystem entry in the <code>sshd_config</code> file on the destination station is specified and points to the SFTP daemon.

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
633	User login failure.	Verify that the Username and Password in the STP Connection Configuration Menu window, (see Table 2 on page 17) is valid and an account exists for the username and password on the SSHD server host.
SFTP Errors		
595	File open failed.	Invalid file name in the download list, or out of resources. Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
596	The file name is already specified.	Report this issue to the Customer Care Center immediately. (Internal SFTP implementation error). Refer to page 3 for the contact information.
SFTP Client Errors		
597	SFTP client packet send failure	Perform these tests:
598	The SFTP connection is closed.	<ul style="list-style-type: none"> • “FTP Server Verification” on page 122
599	SFTP packet read failure	<ul style="list-style-type: none"> • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
600	SFTP protocol error. The received message is larger than the expected packet size.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 124. If the error persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.
601	Undefined	Notify the Customer Care Center. Refer to page 3 for the contact information.
608	SFTP received a invalid ID in the response received during a read operation on remote directory.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 124. If the error persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.
609	SFTP: Handle mismatch error. This error is displayed when there is a failure to receive an expected handle upon successful READ/WRITE/CREAT/TRUNC/EXCL of a file using SSH_FXP_OPEN on remote server.	
610	Unexpected SSH2_FXP_ATTRS.	
611	Unexpected SSH_FXP_NAME. SFTP using the SSH_FXP_OPENDIR opens a directory for reading. The server responds to this request with either a SSH_FXP_NAME or a SSH_FXP_STATUS message. This error code implies that an unexpected SSH_FXP_NAME is received.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 124.

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
612	The SFTP client uses the SSH_FXP_REALPATH request to have the server localize any given path name to an absolute path. This is useful for converting path names containing “..” components or relative pathnames without a leading slash into absolute paths. This error implies that there is a failure during this operation	Check if the access to the path specified in the FTP Server Configuration Menu window (see Figure 43 on page 52) is accessible and re-try the connection.
613	The SSH_FXP_READLINK request is used by the SFTP client to read the target of a symbolic link. The server will respond with a SSH_FXP_NAME packet containing only one name and a dummy attributes value. The name in the returned packet contains the target of the link. This failure implies that there is a failure during the READLINK operation.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing the tests in “Network Outage Trouble Shooting” section on page 124.
614	The SFTP client receives SSH_FXP_DATA as a response to any file operations from the server. This error implies that the client received an unexpected SSH_FXP_NAME from the server.	
615	The SFTP client received more data than expected.	
616	The SFTP client failed to read the data from the file descriptor of the file specified for transfer.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
SSH Client Errors		
617	Excessive identity files. This error means that there are excessive identity files. OpenSSH implementation contains the maximum of 100 identity files or the client configuration file is corrupted.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
624	The debug levels allowed for SSH protocol in openSSH is 0-9. There is either an error in the client configuration file, or the client configuration file is corrupted.	
625	Failure to read the client configuration file.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
626	Invalid compression level is specified in the client configuration file.	
627	SSH failure to setup the IO with the server.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing these tests: <ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.
628	SSH failure to open the channel for the SSH connection with the server.	
629	SSH failure to setup the channel for the SSH connection with the server.	
630	SSH failure to verify the SSH client host key.	

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
631	SSH user authentication failure. Please verify that only the password authentication is set to "yes" in the SSH server configuration file. Refer to the SSHD server configuration provided by vendor of the product. The FTRA and the EAGLE 5 SAS is compatible with openSSH 3.0.2p1 .	Report the issue to the Customer Care Center if the problem persists after the SSHD configuration file is verified. Refer to page 3 for the contact information.
632	The authentication method is NULL in the client software. This error is a failure to set the null authentication method.	Report this issue to the Customer Care Center. Refer to page 3 for the contact information.
633	Permission is denied by the server due to authentication failure.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing these tests:
640	A bad message was received during the SSH authentication.	<ul style="list-style-type: none"> • "FTP Server Verification" on page 122 • "SFTP /SSHD Server Verification" on page 122 • "Connectivity Test - I" on page 122 • "Connectivity Test - II" on page 123 • "Network Outage Trouble Shooting" on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
641	Missing authentication context, encountered during the SSH user authorization.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
642	Failure during the public key read/verification operation.	
643	Undefined SFTP/SSH error.	
644	Unexpected SSH_FXP_STATUS error. An invalid status was received by the SFTP server.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing these tests: <ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.
645	A bad option was specified in the SSH client on the EAGLE 5 SAS.	
646	An unsupported escape character was used in the SSH client on the EAGLE 5 SAS.	
647	An unsupported cipher type was used in the SSH client on the EAGLE 5 SAS.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
648	An unsupported MAC type was used in the SSH client on the EAGLE 5 SAS.	<p>Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1. Verify there is no network outage by performing these tests:</p> <ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
649	A bad port was used in the SSH client on the EAGLE 5 SAS.	<p>Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.</p>
656	Bad forwarding was used in the SSH client on the EAGLE 5 SAS.	
657	Bad forwarding ports were specified in the SSH client on the EAGLE 5 SAS.	
658	A bad dynamic port was specified in the SSH client on the EAGLE 5 SAS.	

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
659	The host was not specified in the SSH client on the EAGLE 5 SAS.	<p>Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1. Verify there is no network outage by performing these tests:</p> <ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
660	An invalid option or argument was specified in the SSH client on the EAGLE 5 SAS.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
661	The hostname was not specified in the SSH client on the EAGLE 5 SAS.	
663	The SSH client was unable to load the cipher type on the EAGLE 5 SAS.	
664	Asynchronous IO is not supported on IPSM, SSH client error.	
665	Compression is already enabled in the SSH client on the EAGLE 5 SAS.	
666	Unknown cipher number on the SSH client on the EAGLE 5 SAS.	
667	The SSH client key length is invalid.	
668	No key is available on the SSH client on the EAGLE 5 SAS.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
669	The secure connection was closed by the remote server, refer to the error on the SFTP/SSHD server side.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing these tests:
670	Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network.	<ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122
671	An unexpected packet type was received from the SFTP/SSHD server.	<ul style="list-style-type: none"> • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124.
672	A bad packet length was received from the SSHD/SFTP server.	<p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
673	A cryptographic attack was detected by the SSH client. Please notify the local system administrator.	Report the issue to the Customer Care Center. Refer to page 3 for the contact information. This is not a software problem but there is a security threat. The keys/authentication may have to be updated immediately.

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
674	The SSH/SFTP client on the EAGLE 5 SAS failed to read from the remote side.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing these tests:
675	Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 SAS.	<ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
676	Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 SAS.	<p>Verify that the <code>sshtools.xml</code> file provided with FTRA software has the field as shown:</p> <pre><!-- The Message Authentication Code configuration, add or override default mac implementations --> <MacConfiguration> <DefaultAlgorithm>hmac-md5</DefaultAlgorithm> </MacConfiguration></pre>
677	Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 SAS.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
678	SSH/SFTP tried to close a connection that is already closed.	

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
679	The SSH/SFTP client on the EAGLE 5 SAS failed to write to the remote side.	<p>Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1. Verify there is no network outage by performing these tests:</p> <ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
680	SSH/SFTP tried to set the packet size twice.	Report this issue to the Customer Care Center immediately. Refer to page 3 for the contact information.
681	A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 SAS.	

Table 9. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
SSH/SFTP Connection/Setup Errors		
682	The connection timed out when SSH tried to connect to SSHD.	Verify that the SFTP/SSHD version is compatible with openSSH 3.0.2p1 . Verify there is no network outage by performing these tests: <ul style="list-style-type: none"> • “FTP Server Verification” on page 122 • “SFTP /SSHD Server Verification” on page 122 • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.
683	The SSH connection was refused by the remote server.	
684	The SSHD server is unreachable.	
685	The network has reset.	
686	The SSH/SFTP connection has been aborted.	
687	The SFTP/SSH connection has been reset by the peer.	
688	Failed to allocate network buffers.	
689	The SSH/SFTP socket is already connected.	
690	The SSH/SFTP socket is not connected.	
691	The network channel is down.	
692	The SSHD/SFTP server connection host is down.	
693	SFTP client channel read failure.	
694	SFTP client channel write failure.	
695	SFTP client channel open failure.	

Table 10. Generic Network Error Codes

SFTP/SSH/ Generic Network Client Error Code	Description	Action/Recovery
40	A destination address is required.	Verify that there is an FTP server entry on the EAGLE 5 SAS using the <code>rtrv-ftp-serv</code> command, and re-try the connection
41	Protocol wrong type for socket	Report this issue to the Customer Care Center. Refer to page 3 for the contact information.
42	The protocol is not available.	
43	The protocol is not supported.	
44	The socket type is not supported.	
45	The operation is not supported on the socket.	
46	The protocol family is not supported.	
47	The address family is not supported.	
48	The address is already in use.	
49	The requested address cannot be assigned.	
50	Socket operation on non-socket	
51	The network is unreachable.	Verify that the connection tests and network outage numbers match as shown in these sections: <ul style="list-style-type: none"> • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
52	The network dropped the connection on reset.	
53	Software caused the connection to abort.	Report this issue to the Customer Care Center. Refer to page 3 for the contact information.

Table 10. Generic Network Error Codes (Continued)

SFTP/SSH/ Generic Network Client Error Code	Description	Action/Recovery
54	The connection was reset by the peer.	<p>Verify that the connection tests pass and network outage numbers are within the allowed limits as shown in these sections:</p> <ul style="list-style-type: none"> • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
55	No buffer space available.	Report this issue to the Customer Care Center. Refer to page 3 for the contact information.
56	The socket is already connected.	
57	The socket is not connected.	
58	Can't send after socket shutdown	
59	Too many references: can't splice	
60	The connection timed out.	<p>Perform these tests and verify that the FTP server address responds to the ping command from the ISPM.</p> <ul style="list-style-type: none"> • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123
61	The connection was refused.	Verify that there is a FTP server daemon is running on the remote station by performing the “FTP Server Verification” test on page 122.

Table 10. Generic Network Error Codes (Continued)

SFTP/SSH/ Generic Network Client Error Code	Description	Action/Recovery
62	The network is down.	Verify that the connection tests pass and network outage numbers are within the allowed limits as shown in these sections:
65	There is no route to the host.	
67	The host is down.	
30	Read-only file system	<ul style="list-style-type: none"> • “Connectivity Test – I” on page 122 • “Connectivity Test - II” on page 123 • “Network Outage Trouble Shooting” on page 124. <p>Make any fixes necessary and retry the connection.</p> <p>If the problem persists, report the issue to the Customer Care Center. Refer to page 3 for the contact information.</p>
32	Broken pipe	Report the issue to the Customer Care Center. Refer to page 3 for the contact information.
35	Unsupported value	

Troubleshooting Procedures

FTP Server Verification

Component: The FTP server IP address shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 52).

Supported Version/Specification: Any FTP server compliant with IETF RFC 959.

Test: On the Unix platform, execute the `netstat -a | grep 21` command to verify that the FTP server is running on the machine with the IP address shown in the **FTP Server Configuration Menu** window (Figure 43 on page 52).

Expected Result:

```
Unix> netstat -a | grep 21
*.32821          *.*                0          0          0          0 LISTEN
f5e15218 stream-ord f5ee8880      0 /var/adm/atria/almd , The system and
process specific variable will change.
```

On the Windows platform, check the Task Manager to verify that the FTP daemon is running.

SFTP/SSHD Server Verification

Component: The SSHD/SFTP server IP address shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 52).

Supported Version/Specification: Version compatible with openSSH 3.0.2p1.

Test: On the Unix platform, execute the `ps -f | grep sshd` command. Please refer to Unix MAN pages for help with `ps` command.

On the Windows platform, use the Task Manager to verify that the sshd daemon process is running.

Expected Result:

```
Unix> ps -ef | grep sshd
user  26912 26886  0 13:28:07 pts/5    0:00 grep sshd
root  411    1  0   Jul 24 ?          4:35 /usr/local/sbin/sshd Note: The
user/system/path variables depends on the server.
```

On the Windows platform, check the Task Manager to verify that the FTP daemon is running.

Connectivity Test – I

Component: Connectivity Test - I.

Supported Version/Specification: N/A

Test: To verify that there is a network connection available between the EAGLE 5 SAS and the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 52).

On an EAGLE 5 SAS terminal, enter the `pass:loc=xxxx:cmd="ping yy.yy.yy.yy"` command, where `xxxx` is location of IPSM associated with the IP address entered in the **STP Connection Configuration Menu** window, (see Table 2 on page 17), and `yy.yy.yy.yy` is the IP address of the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 52).

Expected Result:

NOTE: The RTT time and data sizes may vary.

```
> pass:loc=xxxx:cmd="ping yy.yy.yy.yy"
Command Accepted - Processing
  rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
  pass:loc=xxxx:cmd="ping yy.yy.yy.yy"
  Command entered at terminal #5.
;
  rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
  PASS: Command sent to card
;
  rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
  PING command in progress
;
  rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
;
  rlghncxa03w 05-09-31 13:58:01 GMT  EAGLE5 34.0.0
  PING yy.yy.yy.yy: 56 data bytes
  64 bytes from yy.yy.yy.yy: icmp_seq=0. time=10. ms
  64 bytes from yy.yy.yy.yy: icmp_seq=1. time=5. ms
  64 bytes from yy.yy.yy.yy: icmp_seq=2. time=5. ms
  ---yy.yy.yy.yy PING Statistics---
  3 packets transmitted, 3 packets received, 0% packet loss
  round-trip (ms)  min/avg/max = 5/6/10
  PING command complete
```

Connectivity Test - II

Component: Connectivity Test - II.

Supported Version/Specification: N/A.

Test: To verify that there is a network connection available between the EAGLE 5 SAS and FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 52).

Execute the `ping -s zz.zz.zz.zz` command on the FTP server machine where `zz.zz.zz.zz` is the IP address of the EAGLE 5 SAS shown in the **STP Connection Configuration Menu** window (see Table 2 on page 17).

Expected Result:

```
ping -s zz.zz.zz.zz
PING zz.zz.zz.zz: 56 data bytes
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=0. time=5. ms
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=1. time=4. ms
```

```
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=2. time=5. ms
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=3. time=4. ms

----zz.zz.zz.zz PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 4/4/5
```

Network Outage Trouble Shooting

Component: Network Outage Troubleshooting

Supported Version/Specification: N/A.

Test: To verify the TCP/IP traffic/network statistics are within the Tekelec supported network statistics.

At the EAGLE 5 SAS, enter the **pass:loc=xxxx:cmd="netstat -p tcp"** command at the EAGLE 5 SAS terminal, where **xxxx** is location of the IPSM associated with the IP address entered in the **STP Connection Configuration Menu** window, (see Table 2 on page 17), and analyze the data from output which is similar to the following example output.

NOTE: The specific information for the command may vary depending upon the system used.

```
> pass:loc=3102:cmd="netstat -p tcp"
Command Accepted - Processing
  rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0
  pass:loc=3102:cmd="netstat -p tcp"
  Command entered at terminal #5.
;
  rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0
  PASS: Command sent to card
;
  rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0
TCP:
  161 packets sent
    156 data packets (28411 bytes)
    0 data packet (0 byte) retransmitted
    5 ack-only packets (1 delayed)
    0 URG only packet
    0 window probe packet
    0 window update packet
    0 control packet
  161 packets received
    156 acks (for 28255 bytes)
    0 duplicate ack+C2
    0 ack for unsend data
    5 packets (9 bytes) received in-sequence
    0 completely duplicate packet (0 byte)
    0 packet with some dup. data (0 byte duped)
    0 out-of-order packet (0 byte)
    0 packet (0 byte) of data after window
    0 window probe
    0 window update packet
    0 packet received after close
    0 discarded for bad checksum
    0 discarded for bad header offset field
    0 discarded because packet too short
  0 connection request
```

FTP-Based Table Retrieve Application (FTRA) User Guide

```
1 connection accept
1 connection established (including accepts)
0 connection closed (including 0 drop)
0 embryonic connection dropped
156 segments updated rtt (of 157 attempts)
0 retransmit timeout
    0 connection dropped by rexmit timeout
0 persist timeout
0 keepalive timeout
    0 keepalive probe sent
    0 connection dropped by keepalive
0 pcb cache lookup failed

;

rlghncxa03w 05-09-31 19:32:52 GMT EAGLE5 34.0.0

NETSTAT command complete
```

Expected Result:

The network outage causes the TCP/IP problems like:

- Network latency
- Packet drop
- Duplicate packets.

If the TCP Packet Delay, TCP Packet Loss, TCP Packet Error, or TCP Out of Order values are greater than the values shown in Table 11, fix the network problems and retry the connection.

Table 11. TCP Fault Tolerance Table for FTP/SFTP

Protocol	Fault	Threshold Value
SFTP/FTP	TCP Packet Delay	175 milliseconds
SFTP/ FTP	TCP Packet Loss	40% packet loss
SFTP/ FTP	TCP Packet Errors	10%
SFTP/ FTP	TCP Out of Order	30% of packets with offset of 30 packets

SSH/SFTP/SFTPD/SSHD Protocol Troubleshooting

For more information on SSH/SFTP/SFTPD/SSHD protocol troubleshooting, refer to *SSH, the Secure Shell: The Definitive Guide*, First Edition, Barrett and Silverman, O'Reilly, February 2001.

Index

Symbols

- .doc file extension, 37, 74, 98, 102
- .txt file extension, 37, 74, 98, 102

Numerics

- 30 - Read-only file system, 121
- 32 - Broken pipe, 121
- 35 - Unsupported value, 121
- 40 - A destination address is required, 119
- 41 - Protocol wrong type for socket, 119
- 42 - The protocol is not available, 119
- 43 - The protocol is not supported, 119
- 44 - The socket type is not supported, 119
- 45 - The operation is not supported on the socket, 119
- 46 - The protocol family is not supported, 119
- 47 - The address family is not supported, 119
- 48 - The address is already in use, 119
- 49 - The requested address cannot be assigned, 119
- 50 - Socket operation on non-socket, 119
- 51 - The network is unreachable, 119
- 52 - The network dropped the connection on reset, 119
- 53 - Software caused the connection to abort, 119
- 54 - The connection was reset by the peer, 120
- 55 - No buffer space available, 120
- 56 - The socket is already connected, 120
- 569 - The file name is already specified, 106
- 57 - The socket is not connected, 120
- 58 - Can't send after socket shutdown, 120
- 59 - Too many references: can't splice, 120
- 595 - File open failed, 106
- 597 - SFTP client packet send failure, 106
- 598 - The SFTP connection is closed, 106
- 599 - SFTP packet read failure, 106
- 60 - The connection timed out, 120
- 600 - SFTP protocol error, 107
- 601 - Undefined, 107
- 608 - SFTP received a invalid ID in the response received during a read operation on remote directory, 107
- 609 - SFTP: Handle mismatch error, 107
- 61 - The connection was refused, 120
- 610 - Unexpected SSH2_FXP_ATTRS, 107
- 611 - Unexpected SSH_FXP_NAME, 107
- 612 - SSH_FXP_REALPATH request failure, 108
- 613 - SSH_FXP_READLINK request failure, 108
- 614 - unexpected SSH_FXP_NAME, 108
- 615 - The SFTP client received more data than expected, 108
- 616 - The SFTP client failed to read the data from the file descriptor, 108
- 617 - Excessive identity files, 109
- 62 - The network is down, 121
- 624 - The debug levels allowed for SSH protocol in openSSH is 0-9, 109
- 625 - Failure to read the client configuration file, 109
- 626 - Invalid compression level is specified in the client configuration file, 109
- 627 - SSH failure to setup the IO with the server, 109
- 628 - SSH failure to open the channel for the SSH connection with the server, 109
- 629 - SSH failure to setup the channel for the SSH connection with the server, 109
- 630 - SSH failure to verify the SSH client host key, 109
- 631 - SSH user authentication failure, 110
- 632 - The authentication method is NULL in the client software, 110
- 633 - Permission is denied by the server due to authentication failure, 110
- 633 - User login failure, 106
- 640 - A bad message was received during the SSH authentication, 110
- 641 - Missing authentication context, encountered during the SSH user authorization, 111
- 642 - Failure during the public key read/verification operation, 111

- 643 - Undefined SFTP/SSH error, 111
- 644 - Unexpected SSH_FXP_STATUS error, 111
- 645 - A bad option was specified in the SSH client on the EAGLE 5 SAS, 111
- 646 - An unsupported escape character was used in the SSH client on the EAGLE 5 SAS, 111
- 647 - An unsupported cipher type was used in the SSH client on the EAGLE 5 SAS, 111
- 648 - An unsupported MAC type was used in the SSH client on the EAGLE 5 SAS, 112
- 649 - A bad port was used in the SSH client on the EAGLE 5 SAS, 112
- 65 - There is no route to the host, 121
- 656 - Bad forwarding was used in the SSH client on the EAGLE 5 SAS, 112
- 657 - Bad forwarding ports were specified in the SSH client on the EAGLE 5 SAS, 112
- 658 - A bad dynamic port was specified in the SSH client on the EAGLE 5 SAS, 112
- 659 - The host was not specified in the SSH client on the EAGLE 5 SAS, 113
- 660 - An invalid option or argument was specified in the SSH client on the EAGLE 5 SAS, 114
- 661 - The hostname was not specified in the SSH client on the EAGLE 5 SAS, 114
- 663 - The SSH client was unable to load the cipher type on the EAGLE 5 SAS, 114
- 664 - Asynchronous IO is not supported on IPSM, SSH client error, 114
- 665 - Compression is already enabled in the SSH client on the EAGLE 5 SAS, 114
- 666 - Unknown cipher number on the SSH client on the EAGLE 5 SAS, 114
- 667 - The SSH client key length is invalid, 114
- 668 - No key is available on the SSH client on the EAGLE 5 SAS, 114
- 669 - The secure connection was closed by the remote server, 115
- 67 - The host is down, 121
- 670 - Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network, 115
- 671 - An unexpected packet type was received from the SFTP/SSHD server, 115
- 672 - A bad packet length was received from the SSHD/SFTP server, 115
- 673 - A cryptographic attack was detected by the SSH client, 115
- 674 - The SSH/SFTP client on the EAGLE 5 SAS failed to read from the remote side, 116
- 675 - Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 SAS, 116
- 676 - Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 SAS, 116
- 677 - Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 SAS, 116
- 678 - SSH/SFTP tried to close a connection that is already closed, 116
- 679 - The SSH/SFTP client on the EAGLE 5 SAS failed to write to the remote side, 117
- 680 - SSH/SFTP tried to set the packet size twice, 117
- 681 - A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 SAS, 117
- 682 - The connection timed out when SSH tried to connect to SSHD, 118
- 683 - The SSH connection was refused by the remote server, 118
- 684 - The SSHD server is unreachable, 118
- 685 - The network has reset, 118
- 686 - The SSH/SFTP connection has been aborted, 118
- 687 - The SFTP/SSH connection has been reset by the peer, 118
- 688 - Failed to allocate network buffers, 118
- 689 - The SSH/SFTP socket is already connected, 118
- 690 - The SSH/SFTP socket is not connected, 118
- 691 - The network channel is down, 118
- 692 - The SSHD/SFTP server connection host is down, 118
- 693 - SFTP client channel read failure, 118

Index

694 - SFTP client channel write failure, 118
695 - SFTP client channel open failure, 118

A

A bad dynamic port was specified in the SSH client on the EAGLE 5 SAS - Error code 658, 112
A bad message was received during the SSH authentication - Error code 640, 110
A bad option was specified in the SSH client on the EAGLE 5 SAS - Error code 645, 111
A bad packet length was received from the SSHD/SFTP server - Error code 672, 115
A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 SAS - Error code 681, 117
A bad port was used in the SSH client on the EAGLE 5 SAS - Error code 649, 112
A cryptographic attack was detected by the SSH client - Error code 673, 115
A destination address is required - Error code 40, 119
About FTRA window, 13, 104
Activating Controlled Features procedure, 3
Activating the Eagle OA&M IP Security Enhancements Controlled Feature procedure, 3, 19, 24, 40, 105
Add button, 1, 18, 20, 24, 62
Retrieve Tables, 58
Adding
Command to the Selected Commands Box, 62
Multiple Commands to the Selected Commands Box, 63
Range of Commands to the Selected Commands Box, 63
STP Configuration Record, 20, 50
Adding an STP Configuration Record
FTRA 1.0, 20, 21, 22, 23, 24
FTRA 2.0, 20, 21, 22, 23, 24
alw-card command, 45
An invalid option or argument was specified in the SSH client on the EAGLE 5 SAS - Error code 660, 114

An unexpected packet type was received from the SFTP/SSHD server - Error code 671, 115
An unsupported cipher type was used in the SSH client on the EAGLE 5 SAS - Error code 647, 111
An unsupported escape character was used in the SSH client on the EAGLE 5 SAS - Error code 646, 111
An unsupported MAC type was used in the SSH client on the EAGLE 5 SAS - Error code 648, 112
Application, FTRA
exiting, 4, 14
starting, 4
using, 4
Asynchronous IO is not supported on IPSM, SSH client error - Error code 664, 114
AUTOEXEC.BAT, 7

B

Backup IP Address - FTRA 2.0, 22
Backup IP Address - FTRA 2.0 or greater, 18
Backup IP Address Field - FTRA 2.0 or greater, 18, 22
Bad forwarding ports were specified in the SSH client on the EAGLE 5 SAS - Error code 657, 112
Bad forwarding was used in the SSH client on the EAGLE 5 SAS - Error code 656, 112
Box
Command List, 56, 58, 60, 64, 65
Secure Connection - FTRA 2.0 or greater, 19, 24, 40, 45, 50, 51
Selected Commands, 56, 58, 62, 64, 65, 66
Adding a Command, 62
Adding a Range of Commands, 63
Adding Multiple Commands, 63
Command Removed, 65
Command Selected to be Removed, 64
Stop on error
Update Tables, 83

- Stop on error, Update Tables window, 80, 83, 92, 93, 94
 - Use STP and FTP UserNames, Passwords for all STPs, 19, 20, 38, 39, 40
 - Broken pipe - Error code 32, 121
 - Browse button
 - FTP Server Configuration Menu, 52, 53
 - Update Tables, 80, 81
 - Button
 - Add, 1, 18, 20, 24, 58, 62
 - Browse
 - FTP Server Configuration Menu, 52, 53
 - Update Tables window, 80, 81
 - Cancel, 36
 - Print window
 - Retrieve Tables Log, 73
 - System Log, 101
 - Update Tables Log, 97
 - Save window
 - Retrieve Tables Log, 74
 - System Log, 103
 - Update Tables Log, 98
 - Select Starting Directory window, 54
 - Select window, 81, 82
 - Close, 18, 27, 29, 52
 - Retrieve Tables, 58
 - Update Tables, 80
 - Commit, Update Validation Complete window, 85, 86
 - Delete, 18, 27, 29, 42
 - Edit, Update Validation Complete window, 85, 86, 87, 88
 - Load, 58, 66, 75
 - Modify, 18, 38, 39
 - Refresh, 18, 25, 27, 29, 31, 41
 - Remove, 58, 64
 - Reset, 58, 65
 - Retrieve, 56, 58, 66, 67
 - Retrieve from Local Database, 56, 58, 66
 - Retrieve from STP, 56, 58, 67
 - Save
 - Retrieve Tables Log, 74
 - System Log, 103
 - Update Tables Log, 98
 - Select, 18, 27, 29
 - Select Starting Directory window, 54
 - Select window, 81, 82
 - Set, 55
 - FTP Server Configuration Menu, 52
 - Stop, Update Validation Complete window, 85
 - Store, 58, 65, 75
 - Test, 18, 27, 29, 33
 - Validate, 80, 84
 - Update Tables window, 79
- ## C
- Can't send after socket shutdown - Error code 58, 120
 - Cancel button, 36
 - Print window
 - Retrieve Tables Log, 73
 - System Log, 101
 - Update Tables Log window, 97
 - Save window
 - Retrieve Tables Log, 74
 - System Log, 103
 - Update Tables Log, 98
 - Select Starting Directory window, 54
 - Select window, 81, 82
 - Card
 - GPSM-II, 3
 - IPSM, 3
 - MCAP, 3
 - TDM, 3
 - CD-ROM drive, 2, 5, 8
 - chg-ftp-serv EAGLE 5 SAS command, 52
 - chg-trm command, 48
 - chg-trm:trm=:all=no EAGLE 5 SAS command, 67
 - chmod command, 52, 53
 - Clearing the display
 - Connectivity Test Log, 34, 35
 - Retrieve Tables Log, 70, 71
 - System Log, 99, 100
 - Update Tables Log, 94, 95
 - Close button
 - FTP Connection Configuration Menu, 52
 - Retrieve Tables window, 58

Index

- STP Connection Configuration
 - Menu, 18, 27, 29
- Update Tables, 80
- Closing
 - Connectivity Test Log window, 34, 38
 - Retrieve Tables Log window, 70, 74
 - System Log window, 99, 103
 - Update Tables Log window, 94, 98
- Command
 - EAGLE 5 SAS
 - alw-card, 45
 - chg-ftp-serv, 52
 - chg-trm, 48
 - chg-trm:trm=:all=no, 67
 - ent-ftp-serv, 52
 - init-card, 45, 48, 49
 - pass:loc=xxxx
 - cmd="netstat -p tcp", 124
 - cmd="ping yy.yy.yy.yy", 123
 - rst-card, 45
 - rtrv, 58, 75, 77
 - rtrv-card, 3
 - rtrv-ctrl-feat, 3, 19, 24, 40, 105
 - rtrv-feat, 56
 - rtrv-ftp-serv, 119
 - rtrv-gta, 56, 61, 67
 - rtrv-gtt, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
 - rtrv-ip-lnk, 48, 49
 - rtrv-secu-dflt, 23
 - rtrv-trm, 47, 48, 67
 - rtrv-tt, 56, 61, 67
 - FTRA
 - ftra -c, 75, 77
 - Selecting, 60
- Command Complete
 - Connectivity Test window, 34
 - Retrieve Tables window, 56, 67, 68
 - Update Tables window, 85, 86, 89
- Command File
 - Editing, 2, 87
 - Editor window, 85, 87, 88, 89
 - File Menu, 89
 - File Menu, 89
 - Invalid Command, 88
 - Field, Update Tables window, 81, 82, 84
 - Selected, Update Tables window, 81
 - Stop on error box checked, 83
 - Sending to the Selected STP, 86
- Command files, sending to the EAGLE 5 SAS, 4
- Command In progress, Cannot Close
 - Window message, 88
- Command Line Interface, 1, 58, 65, 66, 75
 - Automatic Start, 77
 - Manual Start, 75
 - UNIX, 76
 - Windows, 76
- Command List
 - Box, 56, 58, 60, 64, 65
 - Field
 - Retrieve Tables window, 58
 - Update Tables window, 80
 - Side, 64
- command prompt
 - DOS, 75
 - shell, 75
- Command Removed from the Selected Commands Box, 65
- Command Selected to be Removed in the Selected Commands Box, 64
- Commands
 - EAGLE 5 SAS, 1, 79, 80
 - EGTT
 - rtrv-gta, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
 - GTT
 - rtrv-gtt, 56, 61, 67
 - rtrv-tt, 56, 61, 67
 - Menu, 13
 - Menu window, 58, 65, 80
 - Selecting a Range, 61
 - Selecting Multiple, 62
- Commit button, Update Validation Complete window, 85, 86
- Compression is already enabled in the SSH client on the EAGLE 5 SAS - Error code 665, 114
- Configuration record, STP, 16, 17, 18, 20, 25, 27, 29, 30, 31, 32, 33, 38, 39, 40, 41, 42, 44, 45, 50
- FTRA 1.0, 31
- FTRA 2.0, 31, 32

Configuration record, STP - FTRA 1.0
 Adding, 20, 21, 22, 23, 24

Configuration record, STP - FTRA 2.0
 Adding, 20, 21, 22, 23, 24

Configuring the EAGLE 5 SAS, 3

Connection failure due to network outage or
 the connection was lost due to a faulty
 SSHD/SFTP server or network - Error
 code 670, 115

Connectivity Test - I procedure, 122

Connectivity Test - II procedure, 123

Connectivity Test Log, 33, 34, 35, 36, 37
 Clearing the Display, 34, 35
 closing, 34, 38
 File Menu, 34
 Print window, 36
 Printing, 34, 36
 Save window, 37
 saved file confirmation window, 37, 38
 saving to a file, 34, 37
 window, 33, 34, 35, 36, 37, 38, 46, 49, 50
 errors, 34
 no errors, 33

Connectivity Test Log window
 File Menu, 34, 35

copyright information, 104

Corrupted check bytes were detected on the
 SSH/SFTP client on the EAGLE 5 SAS -
 Error code 675, 116

Corrupted MAC on input was detected by
 the SSH/SFTP client on the EAGLE 5
 SAS - Error code 676, 116

Corrupted pad on input was detected by the
 SSH/SFTP client on the EAGLE 5 SAS -
 Error code 677, 116

cron, 75, 77, 78

CRON FTRA Wrapper Script, 78

crontab, 78

CSV file format, 1, 56, 58, 66, 75, 77

Current STP
 Selected, 43
 FTRA 1.0, 43
 FTRA 2.0, 44
 Selected: field, 41
 Selecting, 4, 42

Customer Care Center, 3, 5, 48, 105, 106,
 107, 108, 109, 110, 111, 112, 113, 114, 115,
 116, 117, 118, 119, 120, 121

D

Database Administration Manual - System
 Management, 3, 19, 24, 40, 105

Database tables, retrieving from the EAGLE
 5 SAS, 4

Database, STP Connection
 Configuration, 16, 18, 19, 20, 24, 42

Delete button, 18, 27, 29, 42

Delete STP Data window, 42

Deleting an STP Configuration Record, 41

Description
 Retrieve Tables window, 58
 Update Tables window, 80

Disk space, 2

Display
 Clearing
 Connectivity Test Log, 34, 35
 Retrieve Tables Log, 70, 71
 System Log, 99, 100
 Update Tables Log, 94, 95

Displaying an Existing STP Configuration
 Record, 25

DOS, 7

DOS command prompt, 75

Drop down list
 STP Name, 18, 25
 FTRA 1.0, 25, 27
 FTRA 2.0, 25, 26, 27, 28

DSA Key Fingerprint, 48, 49

Duplicate packets, 125

E

EAGLE 5 SAS
 Telnet terminals, 18, 48, 67
 UIM - Unsolicited Information
 Message, 48, 49, 67

EAGLE 5 SAS Card
 GPSM-II, 3
 IPSM, 3
 MCAP, 3
 TDM, 3

EAGLE 5 SAS chg-ftp-serv command, 52

EAGLE 5 SAS chg-trm:trm=:all=no
 command, 67

EAGLE 5 SAS command
 alw-card, 45
 chg-ftp-serv, 52

Index

- chg-trm, 48
- chg-trm:trm=:all=no, 67
- ent-ftp-serv, 52
- init-card, 45, 48, 49
- pass:loc=xxxx
 - cmd="netstat -p tcp", 124
 - cmd="ping yy.yy.yy.yy", 123
- rst-card, 45
- rtrv, 58, 75, 77
- rtrv-card, 3
- rtrv-ctrl-feat, 3, 19, 24, 40, 105
- rtrv-feat, 56
- rtrv-ftp-serv, 119
- rtrv-gta, 56, 61, 67
- rtrv-gtt, 56, 61, 67
- rtrv-gttset, 56, 61, 67
- rtrv-gttset, 56, 61, 67
- rtrv-ip-lnk, 48, 49
- rtrv-secu-dflt, 23
- rtrv-trm, 47, 48, 67
- rtrv-tt, 56, 61, 67
- EAGLE 5 SAS command files
 - sending, 4
- EAGLE 5 SAS commands, 1, 79, 80
- EAGLE 5 SAS configuration, 3
- EAGLE 5 SAS database tables
 - retrieving, 4
- EAGLE 5 SAS EGTT commands
 - rtrv-gta, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
- EAGLE 5 SAS ent-ftp-serv command, 52
- EAGLE 5 SAS Feature
 - EGTT, 56
 - FTP Retrieve and Replace, 3
 - GTT, 56
 - IP User Interface, 3
- EAGLE 5 SAS feature
 - Eagle OA&M IP Security Enhancements, 3, 19, 24, 40, 105
- EAGLE 5 SAS GTT commands
 - rtrv-gtt, 56, 61, 67
 - rtrv-tt, 56, 61, 67
- EAGLE 5 SAS Manual, Database Administration Manual - System Management, 3, 19, 24, 40, 105
- EAGLE 5 SAS pass:loc=xxxx
 - cmd="netstat -p tcp" command, 124
 - cmd="ping yy.yy.yy.yy" command, 123
- EAGLE 5 SAS procedure
 - Activating Controlled Features, 3
 - Activating the Eagle OA&M IP Security Enhancements Controlled Feature, 3, 19, 24, 40, 105
- EAGLE 5 SAS Public Host Key
 - Fingerprint, 45, 46, 48, 50
- EAGLE 5 SAS Public Key Fingerprint, 19, 48, 49
- EAGLE 5 SAS release 30.2 or greater, 3, 19, 24
- EAGLE 5 SAS rtrv-card command, 3
- EAGLE 5 SAS rtrv-ctrl-feat command, 3, 19, 24, 40, 105
- EAGLE 5 SAS rtrv-feat command, 56
- EAGLE 5 SAS rtrv-ftp-serv command, 119
- EAGLE 5 SAS rtrv-gta command, 56, 61, 67
- EAGLE 5 SAS rtrv-gtt command, 56, 61, 67
- EAGLE 5 SAS rtrv-gttset command, 56, 61, 67
- EAGLE 5 SAS rtrv-gttset command, 56, 61, 67
- EAGLE 5 SAS rtrv-secu-dflt command, 23
- EAGLE 5 SAS rtrv-trm command, 67
- EAGLE 5 SAS rtrv-tt command, 56, 61, 67
- Eagle OA&M IP Security Enhancements
 - feature, 3, 19, 24, 40, 105
- Edit button, Update Validation Complete window, 85, 86, 87, 88
- Edit menu
 - FTP-Based Table Retrieve Application, 16, 80
- Editing a Command File, 87
- EGTT commands
 - EAGLE 5 SAS
 - rtrv-gta, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
 - rtrv-gttset, 56, 61, 67
- EGTT Feature, 56
- Entering an STP Name, 29
- ent-ftp-serv EAGLE 5 SAS command, 52
- Environment variable
 - FTRA_HOME, 1, 7, 9
 - JRE_HOME, 1, 7, 9
 - system, 7, 9
 - user, 7, 9

Error code

- 30 - Read-only file system, 121
- 32 - Broken pipe, 121
- 35 - Unsupported value, 121
- 40 - A destination address is required, 119
- 41 - Protocol wrong type for socket, 119
- 42 - The protocol is not available, 119
- 43 - The protocol is not supported, 119
- 44 - The socket type is not supported, 119
- 45 - The operation is not supported on the socket, 119
- 46 - The protocol family is not supported, 119
- 47 - The address family is not supported, 119
- 48 - The address is already in use, 119
- 49 - The requested address cannot be assigned, 119
- 50 - Socket operation on non-socket, 119
- 51 - The network is unreachable, 119
- 52 - The network dropped the connection on reset, 119
- 53 - Software caused the connection to abort, 119
- 54 - The connection was reset by the peer, 120
- 55 - No buffer space available, 120
- 56 - The socket is already connected, 120
- 57 - The socket is not connected, 120
- 58 - Can't send after socket shutdown, 120
- 59 - Too many references: can't splice, 120
- 595 - File open failed, 106
- 596 - The file name is already specified, 106
- 597 - SFTP client packet send failure, 106
- 598 - The SFTP connection is closed, 106
- 599 - SFTP packet read failure, 106
- 60 - The connection timed out, 120
- 600 - SFTP protocol error, 107
- 601 - Undefined, 107
- 608 - SFTP received a invalid ID in the response received during a read operation on remote directory, 107
- 609 - SFTP: Handle mismatch error, 107
- 61 - The connection was refused, 120
- 610 - Unexpected SSH2_FXP_ATTRS, 107
- 611 - Unexpected SSH_FXP_NAME, 107
- 612 - SSH_FXP_REALPATH request failure, 108
- 613 - SSH_FXP_READLINK request failure, 108
- 614 - unexpected SSH_FXP_NAME, 108
- 615 - The SFTP client received more data than expected, 108
- 616 - The SFTP client failed to read the data from the file descriptor, 108
- 617 - Excessive identity files, 109
- 62 - The network is down, 121
- 624 - The debug levels allowed for SSH protocol in openSSH is 0-9, 109
- 625 - Failure to read the client configuration file, 109
- 626 - Invalid compression level is specified in the client configuration file, 109
- 627 - SSH failure to setup the IO with the server, 109
- 628 - SSH failure to open the channel for the SSH connection with the server, 109
- 629 - SSH failure to setup the channel for the SSH connection with the server, 109
- 630 - SSH failure to verify the SSH client host key, 109
- 631 - SSH user authentication failure, 110
- 632 - The authentication method is NULL in the client software, 110
- 633 - Permission is denied by the server due to authentication failure, 110
- 633 - User login failure, 106
- 640 - A bad message was received during the SSH authentication, 110

Index

- 641 - Missing authentication context, encountered during the SSH user authorization, 111
- 642 - Failure during the public key read/verification operation, 111
- 643 - Undefined SFTP/SSH error, 111
- 644 - Unexpected SSH_FXP_STATUS error, 111
- 645 - A bad option was specified in the SSH client on the EAGLE 5 SAS, 111
- 646 - An unsupported escape character was used in the SSH client on the EAGLE 5 SAS, 111
- 647 - An unsupported cipher type was used in the SSH client on the EAGLE 5 SAS, 111
- 648 - An unsupported MAC type was used in the SSH client on the EAGLE 5 SAS, 112
- 649 - A bad port was used in the SSH client on the EAGLE 5 SAS, 112
- 65 - There is no route to the host, 121
- 656 - Bad forwarding was used in the SSH client on the EAGLE 5 SAS, 112
- 657 - Bad forwarding ports were specified in the SSH client on the EAGLE 5 SAS, 112
- 658 - A bad dynamic port was specified in the SSH client on the EAGLE 5 SAS, 112
- 659 - The host was not specified in the SSH client on the EAGLE 5 SAS, 113
- 660 - An invalid option or argument was specified in the SSH client on the EAGLE 5 SAS, 114
- 661 - The hostname was not specified in the SSH client on the EAGLE 5 SAS, 114
- 663 - The SSH client was unable to load the cipher type on the EAGLE 5 SAS, 114
- 664 - Asynchronous IO is not supported on IPSM, SSH client error, 114
- 665 - Compression is already enabled in the SSH client on the EAGLE 5 SAS, 114
- 666 - Unknown cipher number on the SSH client on the EAGLE 5 SAS, 114
- 667 - The SSH client key length is invalid, 114
- 668 - No key is available on the SSH client on the EAGLE 5 SAS, 114
- 669 - The secure connection was closed by the remote server, 115
- 67 - The host is down, 121
- 670 - Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network, 115
- 671 - An unexpected packet type was received from the SFTP/SSHD server, 115
- 672 - A bad packet length was received from the SSHD/SFTP server, 115
- 673 - A cryptographic attack was detected by the SSH client, 115
- 674 - The SSH/SFTP client on the EAGLE 5 SAS failed to read from the remote side, 116
- 675 - Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 SAS, 116
- 676 - Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 SAS, 116
- 677 - Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 SAS, 116
- 678 - SSH/SFTP tried to close a connection that is already closed, 116
- 679 - The SSH/SFTP client on the EAGLE 5 SAS failed to write to the remote side, 117
- 680 - SSH/SFTP tried to set the packet size twice, 117
- 681 - A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 SAS, 117

- 682 - The connection timed out when SSH tried to connect to SSHD, 118
 - 683 - The SSH connection was refused by the remote server, 118
 - 684 - The SSHD server is unreachable, 118
 - 685 - The network has reset, 118
 - 686 - The SSH/SFTP connection has been aborted, 118
 - 687 - The SFTP/SSH connection has been reset by the peer, 118
 - 688 - Failed to allocate network buffers, 118
 - 689 - The SSH/SFTP socket is already connected, 118
 - 690 - The SSH/SFTP socket is not connected, 118
 - 691 - The network channel is down, 118
 - 692 - The SSHD/SFTP server connection host is down, 118
 - 693 - SFTP client channel read failure, 118
 - 694 - SFTP client channel write failure, 118
 - 695 - SFTP client channel open failure, 118
 - Error Codes
 - FTP, 105
 - Generic Network, 119
 - SFTP, 105
 - SSH, 105
 - Error message
 - STP Name does not exist, 32
 - Errors
 - SFTP, 106
 - SFTP Client, 106
 - SSH Client, 109
 - SSH/SFTP Connection/Setup, 118
 - Errors - contacting the Customer Care Center, 3, 5, 48, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121
 - Ethernet connection, 2
 - Excessive identity files - Error code 617, 109
 - Exit Confirmation window, 14
 - Exit menu, 13
 - Exit window, 14, 15
 - Exiting the FTRA application, 4, 14
- F**
- Failed to allocate network buffers - Error code 688, 118
 - Failure during the public key read/verification operation - Error code 642, 111
 - Failure to read the client configuration file - Error code 625, 109
 - Feature
 - Eagle OA&M IP Security Enhancements, 3, 19, 24, 40, 105
 - EGTT, 56
 - FTP Retrieve and Replace, 3
 - GTT, 56
 - IP User Interface, 3
 - Field
 - Command File, Update Tables window, 81, 82, 84
 - Command List
 - Retrieve Tables, 58
 - Update Tables, 80
 - Current STP Selected:, 41
 - File Name:, 54
 - Select Starting Directory window, 54
 - Select window, 82
 - Files of type:
 - Select Starting Directory window, 54
 - Select window, 82
 - FTP Password, 18, 24
 - FTP UserName, 18, 23
 - IP Address, 52
 - Backup - FTRA 2.0 or greater, 18, 22
 - Primary - FTRA 2.0 or greater, 17, 22
 - IP Address - FTRA 1.0, 17, 22
 - Look in:
 - Select Starting Directory window, 54
 - Select window, 82
 - Path, 52
 - Selected Commands, Retrieve Tables, 58
 - STP Name, 4, 17, 18, 20, 25, 29
 - STP name typed
 - FTRA 1.0, 29
 - FTRA 2.0, 29, 30

Index

- STP Password, 18, 23
- STP UserName, 18, 22
- Subpath, 52
- file extension
 - .doc, 37, 74, 98, 102
 - .txt, 37, 74, 98, 102
- File format
 - CSV, 1, 56, 58, 66, 75, 77
- File menu
 - Command File Editor window, 89
 - Connectivity Test Log, 34, 35
 - FTP-Based Table Retrieve Application
 - window, 14
 - Retrieve Tables Log, 70, 71
 - System Log, 99, 100
 - Update Tables Log, 94, 95
- File Name: Field
 - Select Starting Directory window, 54
 - Select window, 82
- File open failed - Error code 595, 106
- FileManager, 8
- Files of type: Field
 - Select Starting Directory window, 54
 - Select window, 82
- Fingerprint
 - Key
 - DSA, 48, 49
 - Public Host Key
 - EAGLE 5 SAS, 45, 46, 48, 50
 - Public Key
 - EAGLE 5 SAS, 19, 48, 49
- flag - strict host key, 46
- FTP Error Codes, 105
- FTP Password Field, 18, 24
- FTP Retrieve and Replace Feature, 3
- FTP server, 51, 122
 - secure, 51
- FTP Server Configuration, 1, 4, 51
 - Menu, 13, 51
 - Browse button, 52, 53
 - Close button, 52
 - IP Address, 51, 122
 - IP Address Field, 52
 - Path Field, 52
 - Set button, 52, 55
 - Subpath Field, 52
 - Menu window, 23, 51, 52, 105, 108, 122, 123
- FTP Server Data Set window, 55
- FTP Server Verification procedure, 122
- FTP UserName Field, 18, 23
- FTP-Based Table Retrieve Application
 - Edit Menu, 16, 51, 80
 - File Menu, 14
 - Help Menu, 104
 - View Menu, 72, 95, 100
 - window, 13, 14, 20, 33, 38, 41, 60, 71, 72, 73, 80, 95, 96, 97, 100, 101, 102, 104
 - File menu, 14
- FTRA
 - Command
 - ftra -c, 75, 77
 - Initialization, 13
 - STP IP connection
 - secure, 19, 24
 - version level, 104
- FTRA 1.0
 - Current STP Selected, 43
 - STP Configuration Record, 31
 - Adding, 20, 21, 22, 23, 24
 - STP Connection Configuration Menu
 - IP Address, 18, 22
 - IP Address Field, 17
 - STP Name drop down list, 25, 27
 - STP name typed, 29
- FTRA 2.0
 - Current STP Selected, 44
 - FTP Server, 51
 - Secure FTP Server, 51
 - STP Configuration Record, 31, 32
 - Adding, 20, 21, 22, 23, 24
 - STP Connection Configuration
 - Menu window, 51
 - STP Connection Configuration Menu
 - Backup IP Address, 18
 - Backup IP Address Field, 22
 - IP Address
 - Backup, 18, 22
 - Primary, 17, 22
 - Primary IP Address, 18
 - Primary IP Address Field, 22
 - Secure Connection Box, 19, 24, 40, 45, 50, 51
 - STP Name drop down list, 25, 26, 27, 28
 - STP name typed, 29, 30

FTRA application
 exiting, 4, 14
 starting, 4
 using, 4
 ftra -c command, 75, 77
 ftra file, 46
 FTRA icon, 13
 FTRA Requirements
 Hardware, 2
 Unix Workstation, 2
 Windows Workstation, 2
 Software, 2
 Unix Workstation, 2
 Windows Workstation, 2
 FTRA software
 installing, 4
 Unix, 9
 Windows, 5
 FTRA window
 GTT Warning window, 56
 Retrieve Tables, 4, 56, 57, 60, 75
 description, 58
 GTT Warning window, 56
 Update Tables, 4, 79, 80, 81, 82, 83, 88,
 89, 92, 93, 94
 description, 80
 Select, description, 82
 Update Validation Complete, 84,
 85, 86
 Update Validation Complete with
 errors, 86
 ftra.bat, 7, 46
 FTRA_HOME environment variable, 1, 7, 9

G

Generic Network Error Codes, 119
 GPSM-II, 3
 GTT commands
 EAGLE 5 SAS
 rtrv-gtt, 56, 61, 67
 rtrv-tt, 56, 61, 67
 GTT Feature, 56
 GTT Warning window, 56

H

Hardware Requirements, 2

Unix Workstation, 2
 Windows Workstation, 2
 Help menu
 FTP-Based Table Retrieve
 Application, 104
 hexadecimal, 48
 Host Key - Secure EAGLE 5 SAS
 Provisioning, 45
 host key checking - strict, 46
 Host Key Fingerprint
 Public
 EAGLE 5 SAS, 45, 46, 48, 50
 host key flag - strict, 46
 hosts.xml, 45, 46, 48, 49, 50

I

Icon, FTRA, 13
 init-card command, 45, 48, 49
 Initializing the FTRA, 13
 Initializing window, 13
 Installing
 FTRA software, 4
 Unix, 9
 Windows, 5
 Java 2 Runtime Environment
 software, 5, 8
 InstallShield Wizard, 5
 Invalid compression level is specified in the
 client configuration file - Error code
 626, 109
 Invalid FTP Password warning
 window, 24
 Invalid FTP User Name warning
 window, 23
 Invalid IP Address warning window, 22,
 52, 53
 Invalid STP Name Error Message
 window, 20
 Invalid STP Name warning window, 20
 Invalid STP Password warning
 window, 23
 Invalid STP User Name warning
 window, 22
 IP Address, 17, 18, 51, 122, 123, 124
 Backup - FTRA 2.0, 22
 Backup - FTRA 2.0 or greater, 18
 IPSM, 48, 49

Index

- Primary - FTRA 2.0, 22
- Primary - FTRA 2.0 or greater, 18
- IP address, 18
- IP Address - FTRA 1.0, 22
- IP Address Field, 52
 - Backup - FTRA 2.0 or greater, 18, 22
 - Primary - FTRA 2.0 or greater, 17, 22
- IP Address Field - FTRA 1.0, 17, 22
- IP Address warning message, 45
- IP connection
 - FTRA and STP
 - secure, 19, 24
- IP User Interface Feature, 3
- IPSM, 3, 45, 47, 48, 49, 123, 124
- IPSM IP Address, 48, 49

J

- Java 2 Runtime Environment, 2, 4, 5, 7, 8, 9
 - software, installing, 5, 8
- JRE - Java Runtime Environment, 2, 9
- JRE_HOME environment variable, 1, 7, 9

K

- Key Fingerprint
 - DSA, 48, 49
 - Public
 - EAGLE 5 SAS, 19, 48, 49

L

- Load button, 58, 66, 75
- Log
 - Connectivity Test, 33, 34, 35, 36, 37
 - window, File Menu, 34, 35
 - Retrieve Tables, 13, 56, 67, 68, 69, 70, 72, 73
 - window, File Menu, 70, 71
 - System, 13, 99, 100, 101, 102, 103
 - closing, 99, 103
 - window, 99, 100, 101, 102, 103
 - File menu, 99, 100
 - Update Tables, 13, 79, 80, 83, 84, 85, 86, 89, 90, 91, 92, 93, 94, 95, 96, 97
 - window, 84, 90, 94, 95, 96, 97, 98
 - Commit Command Completed, 90

- File Menu, 94, 95

- Look in: Field

- Select Starting Directory window, 54
- Select window, 82

M

- MCAP, 3

- Menu

- Commands, 13

- Connectivity Test Log

- File, 34

- Edit

- FTP-Based Table Retrieve

- Application, 16, 80

- Exit, 13

- File

- Command File Editor window, 89

- Connectivity Test Log window, 34, 35

- FTP-Based Table Retrieve

- Application window, 14

- Retrieve Tables Log window, 70, 71

- System Log window, 99, 100

- Update Tables Log window, 94, 95

- FTP Server Configuration, 13, 51

- Browse button, 52, 53

- Set button, 52

- FTP-Based Table Retrieve

- Application, 51

- Help

- FTP-Based Table Retrieve

- Application, 104

- Retrieve Tables Log

- File, 70

- STP Connection Configuration, 13, 16

- View

- FTP-Based Table Retrieve

- Application, 72, 95, 100

- Message

- Command In Progress, Cannot Close

- Window, 88

- IP Address warning, 45

- Must Enter Command Script File

- Name, 84

- Processing Validate Request, Please

- Wait, 84, 90

Update Tables processing completed without errors, 89

Missing authentication context, encountered during the SSH user authorization - Error code 641, 111

Modify button, 18, 38, 39

Modify Warning window, 41

Modifying an Existing STP Configuration Record, 38, 45, 50

Must Enter Command Script File Name message, 84

N

netstat -a | grep 21, 122

Network latency, 125

No buffer space available - Error code 55, 120

No key is available on the SSH client on the EAGLE 5 SAS - Error code 668, 114

O

openSSH 3.0.2p1, 107, 108, 109, 110, 111, 112, 113, 115, 116, 117, 118, 122

Operating system, 2

Windows 2000, 7

Windows 98, 7

Windows NT, 7

P

Packet drop, 125

pass:loc=xxxx

cmd="netstat -p tcp" EAGLE 5 SAS command, 124

cmd="ping yy.yy.yy.yy" EAGLE 5 SAS command, 123

Path Field, 52

path parameter, 52

Permission is denied by the server due to authentication failure - Error code 633, 110

ping -s zz.zz.zz.zz command, 123

Primary IP Address - FTRA 2.0, 22

Primary IP Address - FTRA 2.0 or greater, 18

Primary IP Address Field - FTRA 2.0 or greater, 17, 22

Print window

Cancel button

Update Tables Log, 97

Connectivity Test Log, 36

Retrieve Tables Log, 72, 73

System Log, 101

Update Tables Log, 96

Printing

Connectivity Test Log, 34, 36

Retrieve Tables Log, 70, 72

System Log, 99, 101

Update Tables Log, 94, 96

Problems - contacting the Customer Care Center, 3, 5, 48, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121

Procedure

Activating Controlled Features, 3

Activating the Eagle OA&M IP Security Enhancements Controlled Feature, 3, 19, 24, 40, 105

Connectivity Test - I, 122

Connectivity Test - II, 123

FTP Server Verification, 122

SFTP Server Verification, 122

SSHD Server Verification, 122

Processing Retrieve Request

Update Tables Log window, 84

Processing Validate Request, Please Wait message, 84, 90

Processor speed, 2

Protocol Troubleshooting, 125

Protocol wrong type for socket - Error code 41, 119

Provisioning the Secure EAGLE 5 SAS Host Key, 45

ps, 122

ps -ef | grep sshd, 105

ps -f | grep sshd, 122

Public Host Key Fingerprint

EAGLE 5 SAS, 45, 46, 48, 50

Public Key Fingerprint

EAGLE 5 SAS, 19, 48, 49

Index

R

- RAM, 2
- Read-only file system - Error code 30, 121
- Record, STP configuration, 16
- Refresh button, 18, 25, 27, 29, 31, 41
- release 30.2 or greater - EAGLE 5 SAS, 3, 19, 24
- Release Not Compatible Error - Retrieve Tables Log window, 59
- Remove button, 58, 64
- Requirements
 - Hardware, 2
 - Unix Workstation, 2
 - Windows Workstation, 2
 - Software, 2
 - Unix Workstation, 2
 - Windows Workstation, 2
- Reset button, 58, 65
- Retrieve button, 56, 58, 66, 67
- Retrieve Database Tables from an STP, 56
- Retrieve from Local Database button, 56, 58, 66
- Retrieve from STP button, 56, 58, 67
- Retrieve Tables
 - Command List Box, 56, 58, 60, 64, 65
 - Selected Commands Box, 56, 58, 62, 64, 65, 66
- Retrieve Tables Log, 13, 56, 67, 68, 69, 70, 72, 73
 - Clearing the Display, 70, 71
 - closing, 70, 74
 - File Menu, 70
 - Print window, 72, 73
 - Printing, 70, 72
 - Save window, 73, 74
 - saved file confirmation window, 74
 - saving to a file, 70, 73
- Retrieve Tables Log window, 67, 68, 69, 70, 71, 72, 73, 74
 - File Menu, 70, 71
 - Processing Retrieve Request, 67
 - Release Not Compatible Error, 59
 - with Errors, 70
 - without Errors, 69
- Retrieve Tables window, 4, 56, 57, 60, 75
 - Add button, 58, 62
 - Close button, 58
 - description, 58
 - GTT Warning window, 56
 - Load button, 58, 66, 75
 - Remove button, 58, 64
 - Reset button, 58, 65
 - Retrieve button, 56, 58, 66, 67
 - Retrieve from Local Database button, 56, 58, 66
 - Retrieve from STP button, 56, 58, 67
 - Store button, 58, 65, 75
- Retrieving EAGLE 5 SAS database tables, 1, 4
- rst-card command, 45
- rtrv commands, 58, 75, 77
- rtrv-card EAGLE 5 SAS command, 3
- rtrv-ctrl-feat EAGLE 5 SAS command, 3, 19, 24, 40, 105
- rtrv-feat EAGLE 5 SAS command, 56
- rtrv-ftp-serv EAGLE 5 SAS command, 119
- rtrv-gta EAGLE 5 SAS command, 56, 61, 67
- rtrv-gtt EAGLE 5 SAS command, 56, 61, 67
- rtrv-gttset EAGLE 5 SAS command, 56, 61, 67
- rtrv-gttset EAGLE 5 SAS command, 56, 61, 67
- rtrv-ip-lnk command, 48, 49
- rtrv-secu-dflt EAGLE 5 SAS command, 23
- rtrv-trm command, 47, 48
- rtrv-trm EAGLE 5 SAS command, 67
- rtrv-tt EAGLE 5 SAS command, 56, 61, 67

S

- Save button
 - Retrieve Tables Log
 - Save window, 74
 - System Log Save window, 103
 - Update Tables Log Save window, 98
- Save window
 - Cancel button
 - System Log, 103
 - Update Tables Log, 98
 - Connectivity Test Log, 37
 - Retrieve Tables Log, 73, 74
 - System Log, 102, 103
 - Update Tables Log, 97, 98
- Saved File Confirmation window
 - Connectivity Test Log, 37, 38
 - Retrieve Tables Log, 74

- System Log, 103
- Update Tables Log, 98
- Saving to a file
 - Connectivity Test Log, 34, 37
 - Retrieve Tables Log, 70, 73
 - System Log, 99, 102
 - Update Tables Log, 94, 97
- secure connection, 3, 19, 45
- Secure Connection Box - FTRA 2.0 or greater, 19, 24, 40, 45, 50, 51
- Secure EAGLE 5 SAS Host Key
 - Provisioning, 45
- Secure FTP server, 51
- Secure Host Key - EAGLE 5 SAS
 - Provisioning, 45
- secure IP connection between FTRA and STP, 19, 24
- Security Administration, 48
- Select button, 18, 27, 29
 - Select Starting Directory window, 54
 - Select window, 81, 82
- Select Starting Directory window, 52, 53, 54
 - Cancel button, 54
 - Select button, 54
- Select window
 - Cancel button, 81, 82
 - description, 82
 - Select button, 81, 82
 - Update Tables, 79, 80, 81, 82
- Selected Commands
 - Box, 56, 58, 62, 64, 65, 66
 - Adding a Command, 62
 - Adding a Range of Commands, 63
 - Adding Multiple Commands, 63
 - Command Selected Removed, 65
 - Command Selected to be Removed, 64
 - Field, Retrieve Tables window, 58
- Selected STP, 1, 4, 43, 56, 58, 65, 66, 67, 79, 80, 85, 86, 87, 89
 - Sending a Command File, 86
- Selecting
 - Command, 60
 - Current STP, 4, 42
 - Multiple Commands, 62
 - Range of Commands, 61
- Sending a Command File to the Selected STP, 86
- Sending EAGLE 5 SAS command files, 4
- Server
 - FTP - FTRA 2.0, 51
 - FTP, Configuration, 4
 - Secure FTP - FTRA 2.0, 51
- Set button, 55
 - FTP Server Configuration Menu, 52
- SFTP client channel open failure - Error code 695, 118
- SFTP client channel read failure - Error code 693, 118
- SFTP client channel write failure - Error code 694, 118
- SFTP Client Errors, 106
- SFTP client packet send failure - Error code 597, 106
- SFTP Connection Errors, 118
- SFTP Error Codes, 105
- SFTP Errors, 106
- SFTP packet read failure - Error code 599, 106
- SFTP protocol error - Error code 600, 107
- SFTP received a invalid ID in the response received during a read operation on remote directory - Error code 608, 107
- SFTP Server, 115, 118, 122
- SFTP Server Verification procedure, 122
- SFTP Setup Errors, 118
- SFTP/SSH Error Codes, 105
- SFTP: Handle mismatch error - Error code 609, 107
- Shell command prompt, 75
- Socket operation on non-socket - Error code 50, 119
- Software
 - FTRA
 - Installing, 4
 - Unix, 9
 - Windows, 5
 - Java 2 Runtime Environment
 - installing, 5, 8
- Software caused the connection to abort - Error code 53, 119
- Software Requirements, 2
 - Unix Workstation, 2
 - Windows Workstation, 2
- SSH Client Errors, 109
- SSH Connection Errors, 118

Index

- SSH Error Codes, 105
- SSH failure to open the channel for the SSH connection with the server - Error code 628, 109
- SSH failure to setup the channel for the SSH connection with the server - Error code 629, 109
- SSH failure to setup the IO with the server - Error code 627, 109
- SSH failure to verify the SSH client host key - Error code 630, 109
- SSH Setup Errors, 118
- SSH user authentication failure - Error code 631, 110
- SSH, the Secure Shell: The Definitive Guide, 125
- SSH/SFTP Error Codes, 105
- SSH/SFTP tried to close a connection that is already closed - Error code 678, 116
- SSH/SFTP tried to set the packet size twice - Error code 680, 117
- SSH_FXP_READLINK request failure - Error code 613, 108
- SSH_FXP_REALPATH request failure - Error code 612, 108
- SSHD Server, 115, 118, 122
- SSHD Server Verification procedure, 122
- sshtools.xml, 116
- Starting the FTRA application, 4
- Stop button, Update Validation Complete window, 85
- Stop on error box
 - Update Tables window, 80, 83, 92, 93, 94
- Stop on error box Checked
 - Command File Selected
 - Update Tables window, 83
- Stop Without Sending or Editing a Command File, 87
- Store button, 58, 65, 75
- STP
 - FTRA IP connection
 - secure, 19, 24
 - Retrieve Database Tables, 56
 - selecting current, 4
 - STP Added window, 24
 - STP Configuration Record, 16, 17, 18, 20, 25, 27, 29, 30, 31, 32, 33, 38, 39, 40, 41, 42, 44, 45, 50
 - Adding, 20, 50
 - Deleting, 41
 - Displaying, 25
 - FTRA 1.0, 31
 - FTRA 2.0, 31, 32
 - Modifying, 38, 45, 50
 - testing, 33
 - STP Configuration Record - FTRA 1.0
 - Adding, 20, 21, 22, 23, 24
 - STP Configuration Record - FTRA 2.0
 - Adding, 20, 21, 22, 23, 24
 - STP Connection Configuration, 1
 - Database, 16, 18, 19, 20, 24, 42
 - Menu, 13, 16
 - Menu window, 16, 17, 18, 20, 25, 29, 33, 38, 41, 42, 43, 106, 123, 124
 - FTRA 1.0, 16
 - FTRA 2.0, 51
 - FTRA 2.0 or greater, 16, 17
 - STP Connection Configuration Menu
 - Add button, 1, 18, 20, 24
 - Close button, 18, 27, 29
 - Delete button, 18, 27, 29, 42
 - FTP Password Field, 18, 24
 - FTP UserName Field, 18, 23
 - IP Address, 18, 123, 124
 - Backup - FTRA 2.0, 22
 - Backup - FTRA 2.0 or greater, 18
 - Primary - FTRA 2.0, 22
 - Primary - FTRA 2.0 or greater, 18
 - IP Address - FTRA 1.0, 22
 - IP Address Field
 - Backup - FTRA 2.0 or greater, 18, 22
 - Primary - FTRA 2.0 or greater, 17, 22
 - IP Address Field - FTRA 1.0, 17, 22
 - Modify button, 18, 38, 39
 - Refresh button, 18, 25, 27, 29, 31, 41
 - Secure Connection Box - FTRA 2.0 or greater, 19, 24, 40, 45, 50, 51
 - Select button, 18, 29
 - STP Name drop down list, 18, 25
 - FTRA 1.0, 25, 27
 - FTRA 2.0, 25, 26, 27, 28
 - STP Name Field, 4, 17, 18, 20, 25, 29

- STP name typed
 - FTRA 1.0, 29
 - FTRA 2.0, 29, 30
- STP Password Field, 18, 23
- STP UserName Field, 18, 22
- Test button, 18, 27, 29, 33
- Use STP and FTP UserNames,
 - Passwords for all STPs Box, 19, 20, 38, 39, 40
- STP Connectivity Test, 1
- STP Data Modified window, 39, 41
- STP Name, 17, 18, 19, 20, 24, 25, 26, 27, 29, 32, 38, 42, 43, 44
 - entering, 29
- STP Name does not exist error message, 32
- STP Name drop down list, 18, 25
 - FTRA 1.0, 25, 27
 - FTRA 2.0, 25, 26, 27, 28
- STP Name Field, 4, 17, 18, 20, 25, 29
 - STP name typed
 - FTRA 1.0, 29
 - FTRA 2.0, 29, 30
- STP Password Field, 18, 23
- STP Selection Change window, 18, 43, 44
- STP UserName Field, 18, 22
- strict host key checking, 46
- strict host key flag, 46
- Subpath Field, 52
- Sun Microsystems, 5, 9
- Support - contacting the Customer Care
 - Center, 3, 5, 48, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121
- system environment variable, 7
- System Log, 13, 99, 100, 101, 102, 103
 - Clearing the Display, 99, 100
 - closing, 99, 103
 - Print window, 101
 - Printing, 99, 101
 - Save window, 102, 103
 - saved file confirmation window, 103
 - saving to a file, 99, 102
- System Log window, 99, 100, 101, 102, 103
 - Cancel button, 101
 - File menu, 99, 100

T

- Task Scheduler
 - Windows, 75, 77
- TCP Out of Order, 125
- TCP Packet Delay, 125
- TCP Packet Error, 125
- TCP Packet Errors, 125
- TCP Packet Loss, 125
- TDM, 3
- Technical Assistance - contacting the
 - Customer Care Center, 3, 5, 48, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121
- telnet server, 45
- Telnet terminals, 18, 48, 67
- Terminals
 - EAGLE 5 SAS
 - Telnet, 18, 48, 67
- Test button, 18, 27, 29, 33
- Testing an STP Configuration Record, 33
- The address family is not supported - Error code 47, 119
- The address is already in use - Error code 48, 119
- The authentication method is NULL in the client software - Error code 632, 110
- The connection timed out - Error code 60, 120
- The connection timed out when SSH tried to connect to SSHD - Error code 682, 118
- The connection was refused - Error code 61, 120
- The connection was reset by the peer - Error code 54, 120
- The debug levels allowed for SSH protocol in openSSH is 0-9 - Error code 624, 109
- The file name is already specified - Error code 596, 106
- The host is down - Error code 67, 121
- The host was not specified in the SSH client on the EAGLE 5 SAS - Error code 659, 113
- The hostname was not specified in the SSH client on the EAGLE 5 SAS - Error code 661, 114
- The network channel is down - Error code 691, 118

Index

- The network dropped the connection on reset - Error code 52, 119
 - The network has reset - Error code 685, 118
 - The network is down - Error code 62, 121
 - The network is unreachable - Error code 51, 119
 - The operation is not supported on the socket - Error code 45, 119
 - The protocol family is not supported - Error code 46, 119
 - The protocol is not available - Error code 42, 119
 - The protocol is not supported - Error code 43l, 119
 - The requested address cannot be assigned - Error code 49, 119
 - The secure connection was closed by the remote server - Error code 669, 115
 - The SFTP client failed to read the data from the file descriptor - Error code 616, 108
 - The SFTP client received more data than expected - Error code 615, 108
 - The SFTP connection is closed - Error code 598, 106
 - The SFTP/SSH connection has been reset by the peer - Error code 687, 118
 - The socket is already connected - Error code 56, 120
 - The socket is not connected - Error code 57, 120
 - The socket type is not supported - Error code 44, 119
 - The SSH client key length is invalid - Error code 667, 114
 - The SSH client was unable to load the cipher type on the EAGLE 5 SAS - Error code 663, 114
 - The SSH connection was refused by the remote server - Error code 683, 118
 - The SSH/SFTP client on the EAGLE 5 SAS failed to read from the remote side - Error code 674, 116
 - The SSH/SFTP client on the EAGLE 5 SAS failed to write to the remote side - Error code 679, 117
 - The SSH/SFTP connection has been aborted - Error code 686, 118
 - The SSH/SFTP socket is already connected - Error code 689, 118
 - The SSH/SFTP socket is not connected - Error code 690, 118
 - The SSHD server is unreachable - Error code 684, 118
 - The SSHD/SFTP server connection host is down - Error code 692, 118
 - There is no route to the host - Error code 65, 121
 - Too many references: can't splice - Error code 59, 120
 - Troubleshooting Procedures, 122
- ## U
- UIM - Unsolicited Information Message
 - EAGLE 5 SAS, 48, 49, 67
 - UIM 1493, 48, 49
 - UIM 1494, 48, 49
 - Undefined - Error code 601, 107
 - Undefined SFTP/SSH error - Error code 643, 111
 - Unexpected SSH_FXP_NAME - Error code 611, 107
 - unexpected SSH_FXP_NAME - Error code 614, 108
 - Unexpected SSH_FXP_STATUS error - Error code 644, 111
 - Unexpected SSH2_FXP_ATTRS - Error code 610, 107
 - Unix Workstation Requirements, 2
 - Unknown cipher number on the SSH client on the EAGLE 5 SAS - Error code 666, 114
 - Unsupported value - Error code 35, 121
 - Update Tables Log, 13, 79, 80, 83, 84, 85, 86, 89, 90, 91, 92, 93, 94, 95, 96, 97
 - Clearing the Display, 94, 95
 - closing, 94, 98
 - Print window, 96
 - Printing, 94, 96
 - Save window, 97, 98
 - saved file confirmation window, 98
 - saving to a file, 94, 97
 - Update Tables Log window, 84, 90, 94, 95, 96, 97, 98
 - Commit Command Completed, 90

- File Menu, 94
- File menu, 94, 95
- Processing Retrieve Request, 84
- Update Tables processing completed without errors message, 89
- Update Tables window, 4, 79, 80, 81, 82, 83, 88, 89, 92, 93, 94
 - Browse button, 80, 81
 - Close button, 80
 - Command File field, 81, 82, 84
 - Command File Selected, 81
 - Stop on error box Checked, 83
 - description, 80
 - Select window, description, 82
 - Update Validation Complete Window
 - Update Tables
 - Update Validation
 - Complete, 84, 85, 86
 - Update Validation Complete window, 79, 85, 87, 88
 - with errors Window
 - Update Tables
 - Update Validation Complete with errors, 86
 - Validate button, 79, 80, 84
- Update Validation Complete window, 79, 84, 85, 86, 87, 88
 - description, 85
 - with errors, 86
 - without errors, 86
- Updating Database Tables in the Selected STP, 79
- Use STP and FTP UserNames, Passwords for all STPs Box, 19, 20, 38, 39, 40
- user environment variables, 7
- User Guide Conventions, 1
- User login failure - Error code 633, 106
- Using the FTRA application, 4

V

- Validate button
 - Update Tables, 80, 84
 - Update Tables window, 79
- Validating command files, 2
- Variable
 - environment
 - FTRA_HOME, 1, 7, 9

- JRE_HOME, 1, 7, 9
 - system environment, 7, 9
 - user environment, 7, 9
- Version level, 104
- View menu
 - FTP-Based Table Retrieve
 - Application, 72, 95, 100
- Viewing log files, 2

W

- Window
 - About FTRA, 13, 104
 - Command Complete Connectivity Test, 34
 - Command File Editor, 85, 87, 88, 89
 - File Menu, 89
 - Invalid Command, 88
 - Command File Editor window
 - File Menu, 89
 - Commands Menu, 58, 65, 80
 - Connectivity Test Log, 33, 34, 35, 36, 37, 38, 46, 49, 50
 - closing, 34, 38
 - File Menu, 34, 35
 - Print, 36
 - Save, 37
 - Saved file confirmation, 37, 38
 - with errors, 34
 - with no errors, 33
 - Exit, 14, 15
 - Exit Confirmation, 14
 - FTP Server Configuration Menu, 23, 51, 52, 105, 108, 122, 123
 - FTP Server Data Set, 55
 - FTP-Based Table Retrieve
 - Application, 13, 14, 20, 33, 38, 41, 60, 71, 72, 73, 80, 95, 96, 97, 100, 101, 102, 104
 - GTT Warning, 56
 - Initializing, 13
 - Invalid FTP Password warning, 24
 - Invalid FTP User Name warning, 23
 - Invalid IP Address warning, 22, 52, 53
 - Invalid STP Name Error Message, 20
 - Invalid STP Name warning, 20
 - Invalid STP Password warning, 23
 - Invalid STP User Name warning, 22

Index

- Modify Warning, 41
- Print
 - Retrieve Tables Log, 73
 - Update Tables Log, 97
- Retrieve Tables, 4, 56, 57, 60, 75
 - Add button, 58, 62
 - Close button, 58
 - Command Complete, 56, 67, 68
 - Command List Field, 58
 - description, 58
 - GTT Warning, 56
 - Load button, 58, 66, 75
 - Remove button, 58, 64
 - Reset button, 58, 65
 - Retrieve button, 56, 58, 66, 67
 - Retrieve from Local Database button, 56, 58, 66
 - Retrieve from STP button, 56, 58, 67
 - Selected Commands Field, 58
 - Store button, 58, 65, 75
- Retrieve Tables Log, 67, 68, 69, 70, 71, 72, 73, 74
 - closing, 70, 74
 - File Menu, 70, 71
 - Print, 72, 73
 - Processing Retrieve Request, 67
 - Release Not Compatible Error, 59
 - Save, 73, 74
 - Saved file confirmation, 74
 - with Errors, 70
 - without Errors, 69
- Save
 - Retrieve Tables window, 74
- Select
 - File Name: Field, 82
 - Files of type: Field, 82
 - Look in: Field, 82
 - Update Tables, 79, 80, 81, 82
- Select Starting Directory, 52, 53, 54
 - File Name: Field, 54
 - Files of type: Field, 54
 - Look in: Field, 54
- Select, description, 82
- STP Added, 24
- STP Connection Configuration
 - Menu, 16, 17, 18, 20, 25, 29, 33, 38, 41, 42, 43, 106, 123, 124
 - FTRA 1.0, 16
 - FTRA 2.0, 51
 - FTRA 2.0 or greater, 16, 17
- STP Data Deleted, 42
- STP Data Modified, 39, 41
- STP Selection Change, 18, 43, 44
- System Log, 99, 100, 101, 102, 103
 - closing, 99, 103
 - File Menu, 99, 100
 - Print, 101
 - Print window
 - Cancel button, 101
 - Save, 102, 103
 - Saved file confirmation, 103
- Update Tables, 4, 79, 80, 81, 82, 83, 88, 89, 92, 93, 94
 - Browse button, 80, 81
 - Close button, 80
 - Command Complete, 85, 86, 89
 - Command File field, 81, 82, 84
 - Command File Selected, 81
 - Command List Field, 80
 - description, 80
 - Select, description, 82
 - Stop on error box, 80, 83, 92, 93, 94
 - Update Validation Complete, 85
 - Validate button, 79, 80, 84
- Update Tables Log, 84, 90, 94, 95, 96, 97, 98
 - closing, 94, 98
 - Commit Command Completed, 90
 - File Menu, 94, 95
 - Print, 96
 - Processing Retrieve Request, 84
 - Save, 97, 98
 - Saved file confirmation, 98
- Update Validation Complete, 79, 84, 85, 86, 87, 88
 - Commit button, 85, 86
 - description, 85
 - Edit button, 85, 86, 87, 88
 - Stop button, 85
 - with errors, 86
 - without errors, 86

Windows 2000 operating system, 7
Windows 98 operating system, 7
Windows Explorer, 5, 6
Windows NT operating system, 7
Windows Task Scheduler, 75, 77
Windows Workstation Requirements, 2