Tekelec EAGLE® 5 Integrated Signaling System

FTP-Based Table Retrieve Application (FTRA) User Guide

910-5280-001 Revision A

June 2009

Notice

Information in this documentation is subject to change without notice. Unauthorized use, copying, or translation 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, translated, 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.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks

The Tekelec logo, EAGLE, G-Flex, G-Port, IP7, IP7 Edge, and IP7 Secure Gateway are registered trademarks of Tekelec. TekServer, A-Port, EAGLE 5 ISS, and V-Flex are trademarks of Tekelec. 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:
5,732,213; 5,953,404; 6,115,746; 6,167,129; 6,324,183; 6,327,350; 6,456,845; 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; 6,987,781; 6,987,849; 6,990,089; 6,990,347; 6,993,038; 7,002,988; 7,020,707; 7,031,340; 7,035,239; 7,035,387; 7,043,000; 7,043,001; 7,043,002; 7,046,667; 7,050,456; 7,050,562; 7,054,422; 7,068,773; 7,072,678; 7,075,331; 7,079,524; 7,088,728; 7,092,505; 7,108,468; 7,110,780; 7,113,581; 7,113,781; 7,117,411; 7,123,710; 7,127,057; 7,133,420; 7,136,477; 7,139,388; 7,145,875; 7,146,181; 7,155,206; 7,155,243; 7,155,505; 7,155,512; 7,181,194; 7,190,702; 7,190,772; 7,190,959; 7,197,036; 7,206,394; 7,215,748; 7,219,264; 7,222,192; 7,227,927; 7,231,024; 7,242,695; 7,254,391; 7,260,086; 7,260,207; 7,283,969; 7,286,516; 7,286,647; 7,286,839; 7,295,579; 7,299,050; 7,301,910; 7,304,957; 7,318,091; 7,319,857; 7,327,670
Foreign Patent Numbers:
EP1062792; EP1308054; EP1247378; EP1303994; EP1252788; EP1161819; EP1177660; EP1169829; EP1135905; EP1364520; EP1192758; EP1240772; EP1173969; CA2352246

Ordering Information

Your Tekelec Sales Representative can provide you with information about how to order additional discs.

Table of Contents

Chapter 1: Introduction.....1

Overview.....2
Related Publications.....2
User Guide Conventions.....2
Documentation Availability, Packaging, and Updates.....3
Documentation Admonishments.....3
Customer Care Center.....4
Emergency Response.....6

Chapter 2: Using the FTRA.....9

FTRA Initialization.....10
Exit the FTRA.....11
STP Connection Configuration Menu.....12
Adding an STP Configuration Record.....16
Displaying an Existing STP Configuration Record.....20
To Enter the STP Name.....22
Testing an STP Configuration Record.....23
Connectivity Test Log File Menu.....25
Modifying an Existing STP Configuration Record.....28
Deleting an STP Configuration Record.....30
Selecting the Current STP.....31
Secure EAGLE 5 ISS Host Key Provisioning.....32
FTP Server Configuration.....37
Retrieve Database Tables from an STP.....42
Retrieve Tables Window.....42
Retrieve Tables Log.....53
Command Line Interface.....59
Updating Database Tables in the Selected STP.....65
Validating a Command File.....66
Update Validation Complete Window.....69
Sending a Command File to the Selected STP.....71
Stop Without Sending or Editing a Command File.....71
Editing a Command File.....71
Update Tables Log Window.....74
File Menu in the Update Tables Log Window.....78

Clearing the Update Tables Log Display....78
Printing the Update Tables Log....79
Saving the Update Tables Log to a File....80
Closing the Update Tables Log Window....81
The System Log....81
File Menu in the System Log Window....82
Clearing the System Log Display....82
Printing the System Log....83
Saving the System Log to a File....83
Closing the System Log Window....84
About FTRA Window....85
FTRA release 4.2....85
RTRV-STP Command....86
RTRV-STP Command Retrieval Session....87
Version Information....88
SSH/SFTP Error Codes....89
Troubleshooting Procedures....104
FTP Server Verification....104
SFTP /SSHD Server Verification....105
Connectivity Test – I....105
Connectivity Test - II....106
Network Outage Trouble Shooting....106
SSH/SFTP/SFTPD/SSHD Protocol Troubleshooting....108
Glossary....109

List of Figures

Figure 1: FTP-Based Table Retrieve Application Window....10
Figure 2: File Menu in the FTP-Based Table Retrieve Application Window....11
Figure 3: Exit Confirmation Window....11
Figure 4: Exit Window....12
Figure 5: Edit Menu....12
Figure 6: STP Connection Configuration Menu Window (FTRA 4.2)....13
Figure 7: Invalid STP Name Error Message....17
Figure 8: Adding an STP Configuration Record (FTRA 4.2)....17
Figure 9: Invalid IP Address Error Message....18
Figure 10: Invalid STP User Name Error Message....18
Figure 11: Invalid STP Password Error Message....19
Figure 12: Invalid FTP User Name Error Message....19
Figure 13: Invalid FTP Password Error Message....19
Figure 14: STP Added Window....20
Figure 15: Selecting an STP Name from the STP Name Drop Down List (FTRA 4.2)....21
Figure 16: STP Name Selected from the STP Name Drop Down List (FTRA 4.2)....21
Figure 17: Selecting an STP Configuration Record by Typing in the STP Name Field (FTRA 4.2)....22
Figure 18: STP Configuration Record (FTRA 4.2)....22
Figure 19: STP Name Does Not Exist Error Message....23
Figure 20: Connectivity Test Log Window with No Errors....23
Figure 21: Connectivity Test Log Window with Errors....24
Figure 22: Command Complete Connectivity Test Window....24
Figure 23: File Menu in the Connectivity Test Log Window....25
Figure 24: Print Window....26
Figure 25: Save Window....26
Figure 26: Saved File Confirmation Window....27
Figure 27: Modifying STP Configuration Record Parameters (FTRA 4.2)....28
Figure 28: STP Data Modified Window....29
Figure 29: Modify Warning Window....30
Figure 30: Delete STP Window....30
Figure 32: Current STP Selected (FTRA 4.2)....31
Figure 33: IP Address Warning Message....32
Figure 34: FTP-Based Table Retrieve Application Edit Commands Menu....37
Figure 35: FTP Server Configuration Menu Window....37
Figure 36: Invalid IP Address Error Message....39
Figure 37: Select Starting Directory Window....39

Figure 38: Invalid Subpath Window....41
Figure 39: FTP Server Configuration Example....41
Figure 40: FTP Server Data Set Window....41
Figure 41: GTT Warning Window....42
Figure 42: Retrieve Tables Window....42
Figure 43: Retrieve Table Log - Release Not Supported Error....44
Figure 44: Commands Menu in the FTP-Based Table Retrieve Application Window....45
Figure 45: Selecting a Command....45
Figure 46: Selecting a Range of Commands....46
Figure 47: Selecting Multiple Commands....47
Figure 48: Adding a Command to the Selected Commands Box....47
Figure 49: Adding a Range of Commands to the Selected Commands Box....48
Figure 50: Adding Multiple Commands to the Selected Commands Box....48
Figure 51: Command Selected to be Removed in the Selected Commands Box....49
Figure 52: Command Removed from the Selected Commands Box....50
Figure 53: Command Data Stored Window....50
Figure 54: Retrieving Database Tables from the Local Database....51
Figure 55: Retrieve Tables Log Window - Processing Retrieve Request....52
Figure 56: Command Complete Window Without Errors....52
Figure 57: Command Complete Window With Errors....52
Figure 58: Retrieve Tables Log Window without Errors....53
Figure 59: Retrieve Table Log with Errors....54
Figure 60: Retrieve Table Log with the RTRV-STP Command CSV Example....54
Figure 61: File Menu in the Retrieve Tables Log Window....55
Figure 62: View Menu....56
Figure 63: Print Window....57
Figure 64: Save Window....58
Figure 65: Saved File Confirmation Window....58
Figure 66: FTRA Windows Command Line Interface....59
Figure 67: FTRA Windows Command Line Interface to modify STP data....60
Figure 68: FTRA UNIX Command Line Interface....60
Figure 69: FTRA UNIX Command Line Interface to modify STP data....60
Figure 70: FTRA Windows Scheduled Task 61
Figure 71: FTRA Windows Scheduled Task to modify STP data....61
Figure 72: UNIX cron job scheduled via crontab 62
Figure 73: FTRA wrapper script example for UNIX....62
Figure 74: FTRA wrapper script example on UNIX for modifying STP configuration....63
Figure 75: Update Tables Window....65
Figure 76: Edit Menu....66

Figure 77: Select Window....67
Figure 78: Update Tables Window with a Command File Selected and Stop on Error Box Checked....68
Figure 79: Update Tables Log Window - Processing Retrieve Request....68
Figure 80: Must Enter Command Script File Name Message....69
Figure 81: Update Validation Complete Window without Errors....69
Figure 82: Update Validation Complete Window with Errors....70
Figure 83: Command Complete Window....71
Figure 84: Command File Editor Window....71
Figure 85: Command In progress, Cannot Close Window....72
Figure 86: Command File Editor with Invalid Command....72
Figure 87: File Menu in the Command File Editor Window....73
Figure 88: Command Complete Window....74
Figure 89: Update Tables Log Window after the Commit Command Completed....74
Figure 90: Update Tables Log....75
Figure 91: Update Tables Log with Stop on Error Box Checked in the Update Tables Window....75
Figure 92: Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window....76
Figure 93: File Menu in the Update Tables Log Window....78
Figure 94: View Menu....78
Figure 95: Print Window....79
Figure 96: Save Window....80
Figure 97: Saved Confirmation Window....81
Figure 98: System Log Window....81
Figure 99: File Menu in the System Log Window....82
Figure 100: View Menu....82
Figure 101: Print Window....83
Figure 102: Save Window....83
Figure 103: Saved Confirmation Window....84
Figure 104: Help Menu....85
Figure 105: Typical About FTRA Window....85
Figure 106: Retrieve Tables window with rtrv-stp command selected for retrieval....86
Figure 107: Successful Retrieval Session for rtrv-stp command....87
Figure 108: Rtrv-stp Command unsupported on EAGLE release....88
Figure 109: About FTRA Display Window....88

List of Tables

Table 1: Admonishments....4
Table 2: FTP-Based Table Retrieve Application Menu Description....10
Table 3: STP Connection Configuration Menu Description....14
Table 4: FTP Server Configuration Menu Window Descriptions....38
Table 5: Select Starting Directory Window Descriptions....40
Table 6: Retrieve Tables Window Description....43
Table 7: FTRA - Eagle Compatibility Matrix....64
Table 8: Update Tables Window Description....65
Table 9: Select Window Descriptions....67
Table 10: Update Validation Complete Window Description....70
Table 11: FTP/SFTP/SSH Error Codes....89
Table 12: Generic Network Error Codes....101
Table 13: TCP Fault Tolerance Table for FTP/SFTP....108

Chapter 1

Introduction

Topics:

- *Overview.....2*
- *Related Publications.....2*
- *User Guide Conventions.....2*
- *Documentation Availability, Packaging, and Updates.....3*
- *Documentation Admonishments.....3*
- *Customer Care Center.....4*
- *Emergency Response.....6*

This chapter contains general information about manual organization, scope and audience, related documentation, gow to locate customer documentation on the Customer Support site, how to get technical assistance, and RMA requirements.

Overview

The FTP-Based Table Retrieve Application (FTRA) is designed in conjunction with the FTP Retrieve and Replace feature to transfer EAGLE 5 ISS 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 STPs. Database tables can be retrieved from the EAGLE 5 ISS, using the EAGLE 5 ISS's retrieve commands. The output of these retrieve commands is converted to CSV (comma separated value) files. EAGLE 5 ISS 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 ISS 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.

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications* document. The *Related Publications* document is published as a part of the *Release Documentation* and is also published as a separate document on the Tekelec Customer Support Site.

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:

```
SETFTRA_HOME="C:\ <download_directory> "
SETJRE_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*>.

Documentation Availability, Packaging, and Updates

Tekelec provides documentation with each system and in accordance with contractual agreements. For General Availability (GA) releases, Tekelec publishes a complete EAGLE 5 ISS documentation set. For Limited Availability (LA) releases, Tekelec may publish a documentation subset tailored to specific feature content or hardware requirements. Documentation Bulletins announce a new or updated release.

The Tekelec EAGLE 5 ISS documentation set is released on an optical disc. This format allows for easy searches through all parts of the documentation set.

The electronic file of each manual is also available from the Tekelec Customer Support site (*support.tekelec.com*). This site allows for 24-hour access to the most up-to-date documentation, including the latest versions of Feature Notices.

Printed documentation is available for GA releases on request only and with a lead time of six weeks. The printed documentation set includes pocket guides for commands and alarms. Pocket guides may also be ordered separately. Exceptions to printed documentation are:

- Hardware or Installation manuals are printed without the linked attachments found in the electronic version of the manuals.
- The Release Notice is available only on the Customer Support site.

Note: Customers may print a reasonable number of each manual for their own use.

Documentation is updated when significant changes are made that affect system operation. Updates resulting from Severity 1 and 2 PRs are made to existing manuals. Other changes are included in the documentation for the next scheduled release. Updates are made by re-issuing an electronic file to the customer support site. Customers with printed documentation should contact their Sales Representative for an addendum. Occasionally, changes are communicated first with a Documentation Bulletin to provide customers with an advanced notice of the issue until officially released in the documentation. Documentation Bulletins are posted on the Customer Support site and can be viewed per product and release.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)
	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Central and Latin America (CALA)**

  Phone:

USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

  Phone:

  0-800-555-5246 (toll-free)

- **Brazil**

  Phone:

  0-800-891-4341 (toll-free)

  TAC Regional Support Office Hours:

  8:30 a.m. through 6:30 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

  Phone:

  1230-020-555-5468

- **Columbia**

  Phone:

  01-800-912-0537

- **Dominican Republic**

  Phone:

  1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552 (1-888-FOR-TKLC)

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**
  - **Signaling**

Phone:

+44 1784 467 804 (within UK)

TAC Regional Support Office Hours:

8:00 a.m. through 7:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Software Solutions**

  Phone:

  +33 3 89 33 54 00

  TAC Regional Support Office Hours:

  8:00 a.m. through 7:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Asia**
  - **India**

    Phone:

    +91 124 436 8552 or +91 124 436 8553

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays
  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with an EAGLE 5 ISS that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical problems affect service and/or system operation resulting in:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with the Tekelec Customer Care Center.

Chapter 2

Using the FTRA

Topics:

- *FTRA Initialization.....10*
- *Exit the FTRA.....11*
- *STP Connection Configuration Menu.....12*
- *Adding an STP Configuration Record.....16*
- *Displaying an Existing STP Configuration Record.....20*
- *Testing an STP Configuration Record.....23*
- *Modifying an Existing STP Configuration Record.....28*
- *Deleting an STP Configuration Record.....30*
- *Selecting the Current STP.....31*
- *Secure EAGLE 5 ISS Host Key Provisioning.....32*
- *FTP Server Configuration.....37*
- *Retrieve Database Tables from an STP.....42*
- *Command Line Interface.....59*
- *Updating Database Tables in the Selected STP.....65*
- *Update Tables Log Window.....74*
- *The System Log.....81*
- *About FTRA Window.....85*
- *SSH/SFTP Error Codes.....89*
- *Troubleshooting Procedures.....104*

This chapter contains information regarding the various ways to use the FTP-Based Table Retrieve Application (FTRA).

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: FTP-Based Table Retrieve Application Window* on page 10. 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

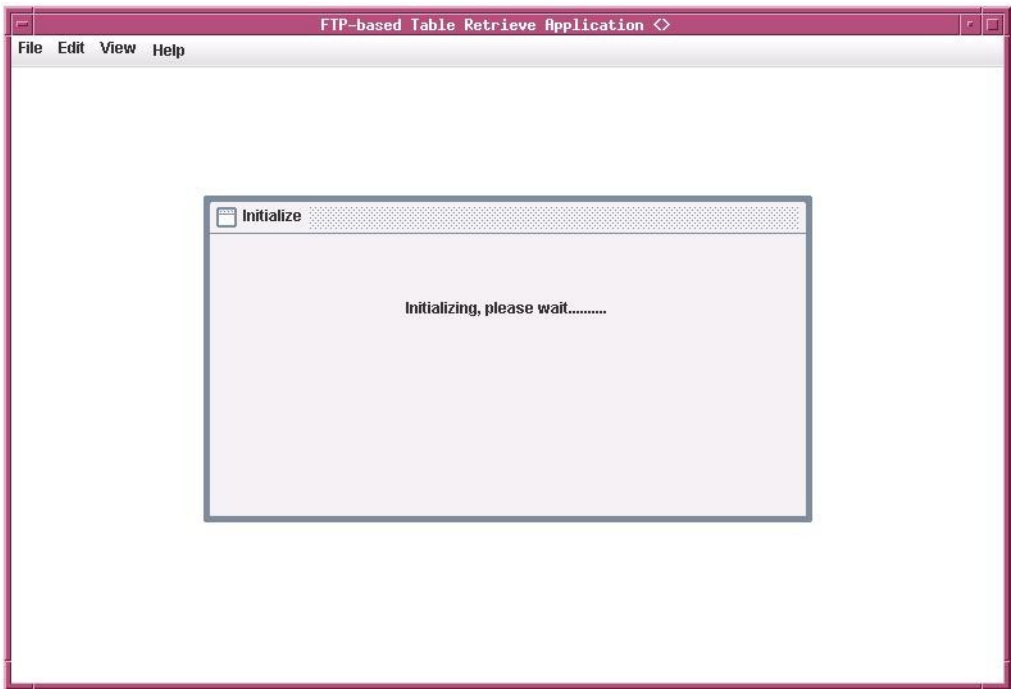


Table 2: FTP-Based Table Retrieve Application Menu Description on page 10 shows the description of the menus in the **FTP-Based Table Retrieve Application** window.

Table 2: 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: • The Retrieve Tables Log • The Update Tables Log

Item	Description
	• The System Log.
Help	Selects the **About FTRA** window.

Exit the FTRA

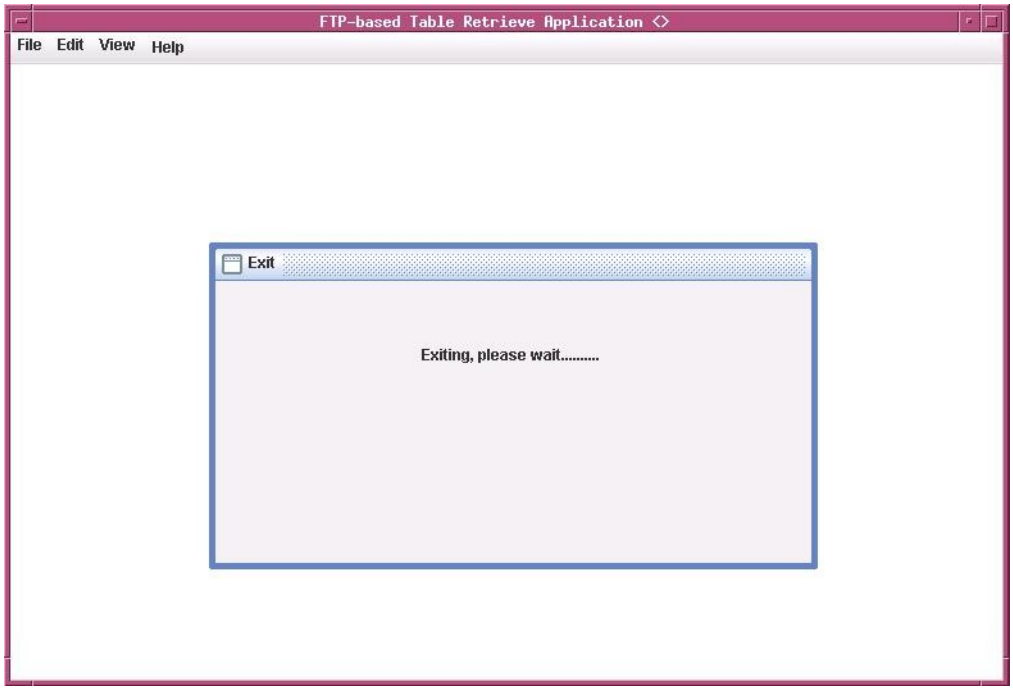
To close the **FTP-Based Table Retrieve Application** window and exit the FTRA, either select **File > Exit** from the **File** menu, see *Figure 2: File Menu in the FTP-Based Table Retrieve Application Window* on page 11, or click the close window button in the upper right hand corner of the window.

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

The **Exit?** confirmation window (see *Figure 3: Exit Confirmation Window* on page 11) opens with "You are about to exit. Continue?" Click **OK** to exit and close the application. The **Exit** window (see *Figure 4: Exit Window* on page 12) 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: Edit Menu* on page 12.

Figure 5: Edit Menu

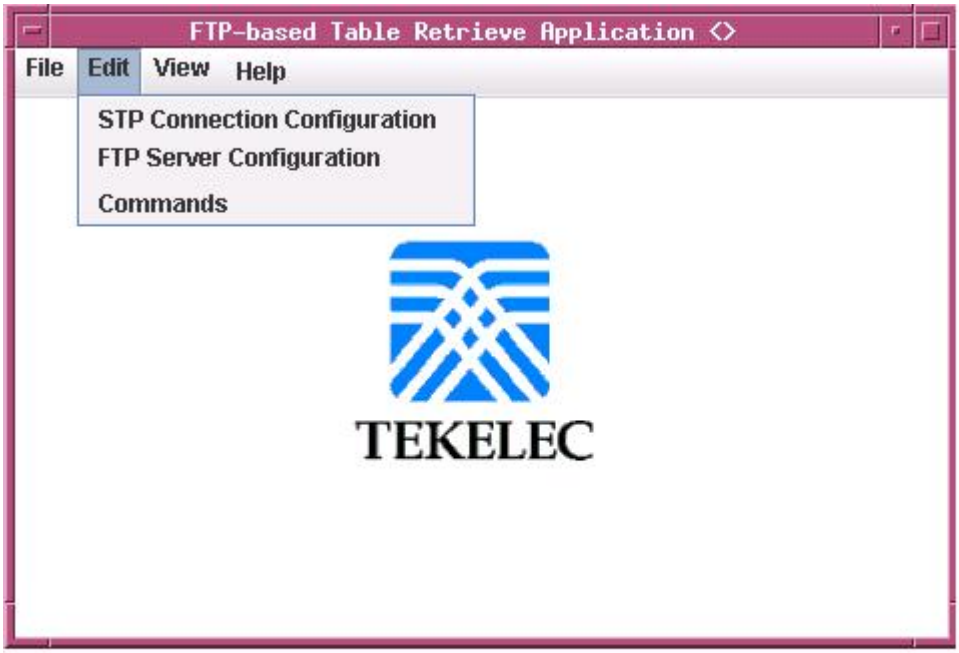


Figure 6: STP Connection Configuration Menu Window (FTRA 4.2)

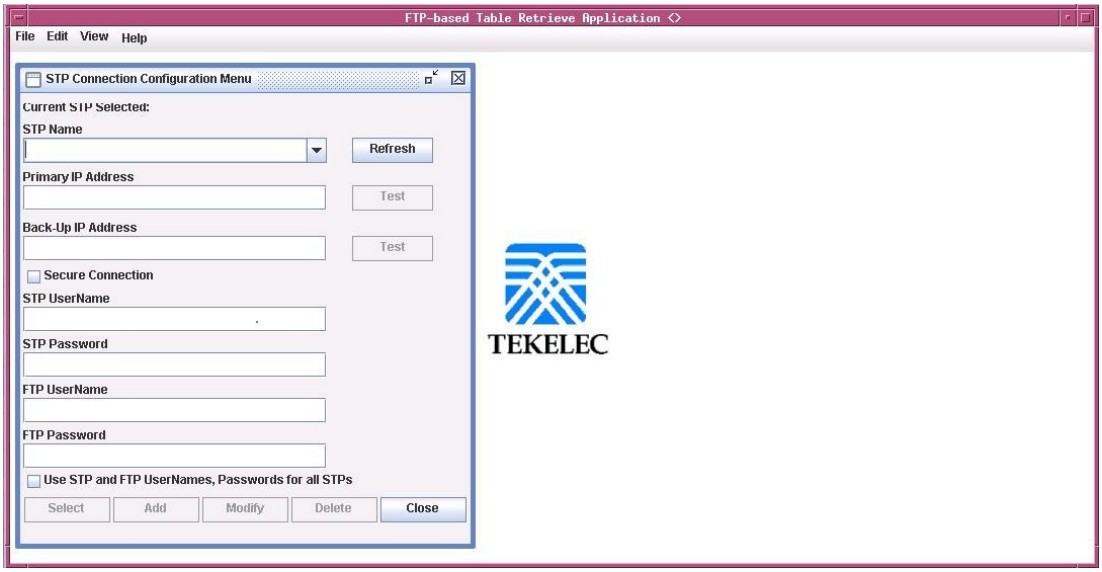


Table 3: STP Connection Configuration Menu Description on page 14 shows the description of the fields, buttons, and boxes in the **STP Connection Configuration Menu** window.

Table 3: 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.
Primary IP Address (FTRA 4.2)	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 ISS.
Backup IP Address (FTRA 4.2)	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 ISS.
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 `mylogin#1`, you would enter `“mylogin#1”`).
FTP Password	The FTP password assigned to the user by the administrator (used for FTP).
Buttons	

Item	Description
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 ISS through an available telnet terminal at the specified IP address. For FTRA 4.0, the STP Connection Configuration Menu window has only one **Test** button. For FTRA 4.0 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.
Boxes	
Secure Connection (FTRA 4.2)	Enables the FTRA to use a secure IP connection to the STP. To use a secure connection for the FTRA to EAGLE 5 ISS communication, make sure the EAGLE 5 ISS is running release 30.2 or greater and that the Eagle OA&M IP Security Enhancements feature is enabled and activated.

Item	Description
	This can be verified by entering the `rtrv-ctrl-feat` command at the EAGLE 5 ISS. 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. **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. If this box is checked, the public key fingerprint for the EAGLE 5 ISS specified in this window must be installed onto the FTRA for the FTRA and the specified EAGLE 5 ISS 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 ISS Host Key Provisioning* on page 32 procedure.
Use STP and FTP UserNames, Passwords for all STPs Box	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.

Adding an STP Configuration Record

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window.

   See *Figure 5: Edit Menu* on page 12. The **STP Connection Configuration Menu** window opens. 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 8: Adding*

an STP Configuration Record (FTRA 4.2) on page 17 (FTRA 4.2). The STP Name will always be entered in uppercase regardless of the Caps Lock key setting on your keyboard.

If characters other then alphanumeric characters or spaces are included in the STP name, the **Invalid STP Name** warning window is displayed. 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* on page 20.

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* on page 28 to change an existing STP configuration record.

Figure 7: Invalid STP Name Error Message

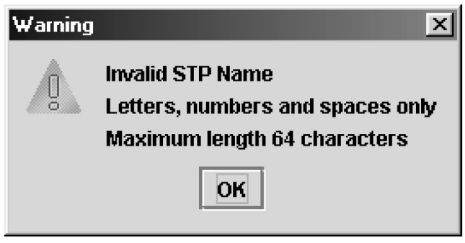
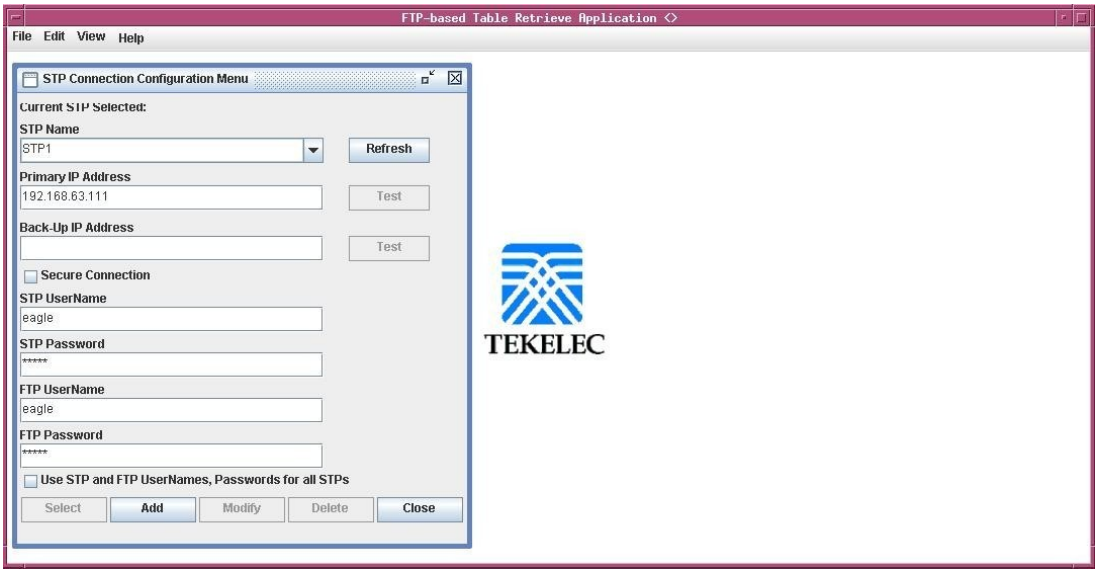


Figure 8: Adding an STP Configuration Record (FTRA 4.2)



3. Enter the IP address of the STP in the **Primary IP Address** field, and a backup IP address in the **Backup IP Address** field. See *Figure 8: Adding an STP Configuration Record (FTRA 4.2)* on page 17 (FTRA 4.2).

CAUTION:

If the backup IP address is not entered for FTRAs running 4.0 and later, the FTRA will not be able to connect to the STP when the connection to the STP using the IP address fails. It is recommended that you specify a backup IP address for the STP.

If the primary and backup IP addresses (FTRA 4.2) is not entered correctly, the **Invalid IP Address** warning window is displayed. See *Figure 9: Invalid IP Address Error Message* on page 18. If the **Invalid IP Address** window appears, click **OK** , and re-enter the IP address in the primary or backup IP addresses (FTRA 4.2) in the **Primary IP Address** or **Backup IP Address** fields in the correct format.

Figure 9: 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 8: Adding an STP Configuration Record (FTRA 4.2)* on page 17 (FTRA 4.2). If the format of the STP user name is not correct, the **Invalid STP User Name** warning window is displayed. See *Figure 7: Invalid STP Name Error Message* on page 17. If the **Invalid STP User Name** window appears, click **OK**, and re-enter the STP user name in the **STP UserName** field.

Figure 10: 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 ISS system administrator for telnet sessions. See *Figure 8: Adding an STP Configuration Record (FTRA 4.2)* on page 17 (FTRA 4.2). If the format of the STP password is not correct, the **Invalid STP Password** warning window is displayed. See *Figure 11: Invalid STP Password Error Message* on page 19. 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 ISS passwords. The passwords are validated by the EAGLE 5 ISS when the FTRA attempts a connection to the EAGLE 5 ISS. The requirements for the format of EAGLE 5 ISS passwords is shown in the output of the EAGLE 5 ISS's `rtrv-secu-dflt` command.

Figure 11: Invalid STP Password Error Message

6. Enter the FTP user name assigned by the FTP server administrator in the **FTP UserName** field.

   See *Figure 8: Adding an STP Configuration Record (FTRA 4.2)* on page 17 (FTRA 4.2). 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 12: Invalid FTP User Name Error Message* on page 19. 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 34: FTP Server Configuration Menu Window* on page 37), must allow FTPs to the IP address specified in the FTP Server Configuration Menu window.

Figure 12: Invalid FTP User Name Error Message

7. Enter the FTP password assigned by the FTP server administrator in the **FTP Password** field.

   See *Figure 8: Adding an STP Configuration Record (FTRA 4.2)* on page 17 (FTRA 4.2). If the format of the STP user name is not correct, the **Invalid FTP Password** warning window is displayed. See *Figure 13: Invalid FTP Password Error Message* on page 19. If the **Invalid FTP Password** window appears, click **OK** , and re-enter the FTP password in the **FTP Password** field.

Figure 13: Invalid FTP Password Error Message

Note:

If you are running FTRA 4.0 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 ISS 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 ISS. 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 8: Adding an STP Configuration Record (FTRA 4.2)* on page 17 (FTRA 4.2). The newly entered STP Name and associated data is added to the STP Connection Configuration database, and the **STP Added** window (*Figure 14: STP Added Window* on page 20) is displayed. Click **OK** to continue.

   Figure 14: STP Added Window

10. Verify the addition of the new STP name.

    See the *Displaying an Existing STP Configuration Record* on page 20.

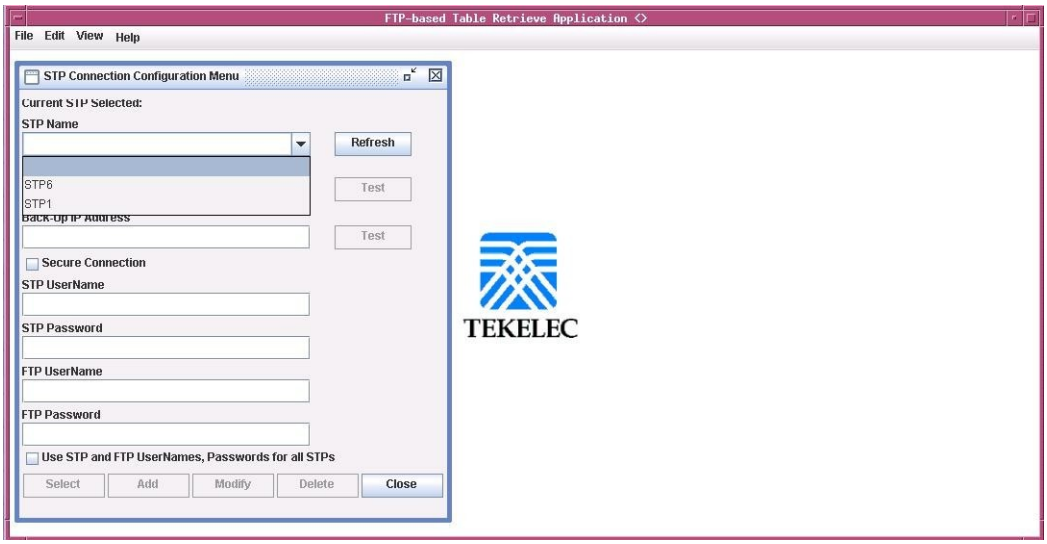
Displaying an Existing STP Configuration Record

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 theSTP 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

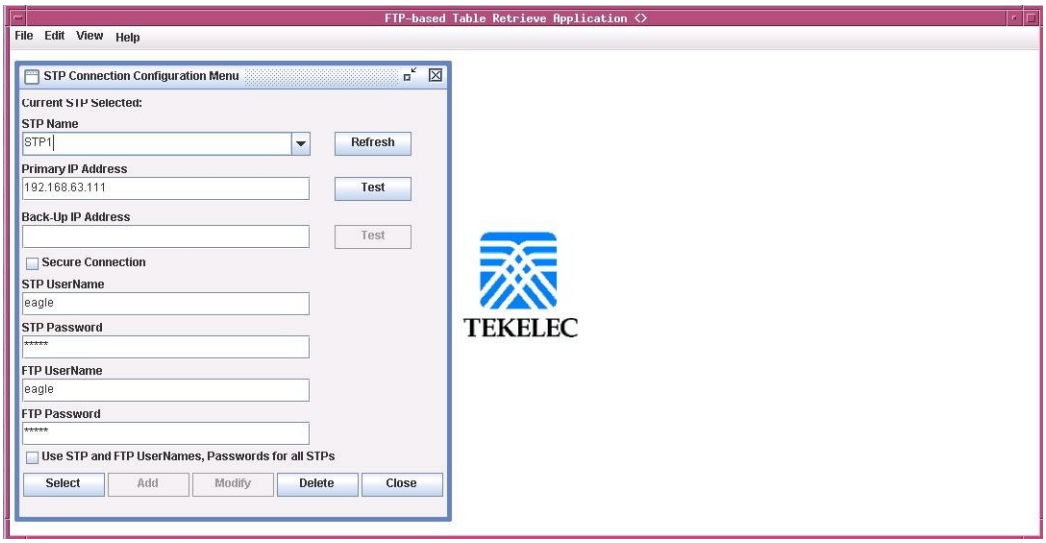
1. In the STP Connection Configuration Menu window, click on the STP Name drop down list. The STP Name drop down list opens. Move the cursor to the STP name to be selected. Click on the desired STP name in the drop down list.

Figure 15: Selecting an STP Name from the STP Name Drop Down List (FTRA 4.2)



2. When the STP name is selected in step 1, the STP configuration record for the specified STP is displayed. The Refresh, Test, Select, Delete, and Close buttons are enabled.

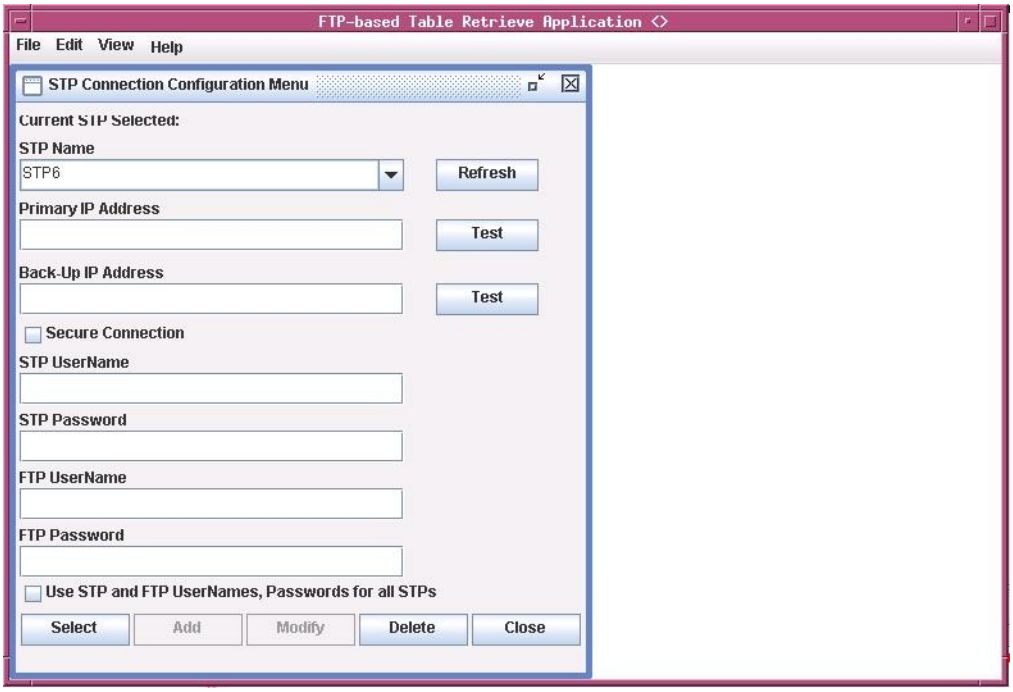
Figure 16: STP Name Selected from the STP Name Drop Down List (FTRA 4.2)



To Enter the STP Name

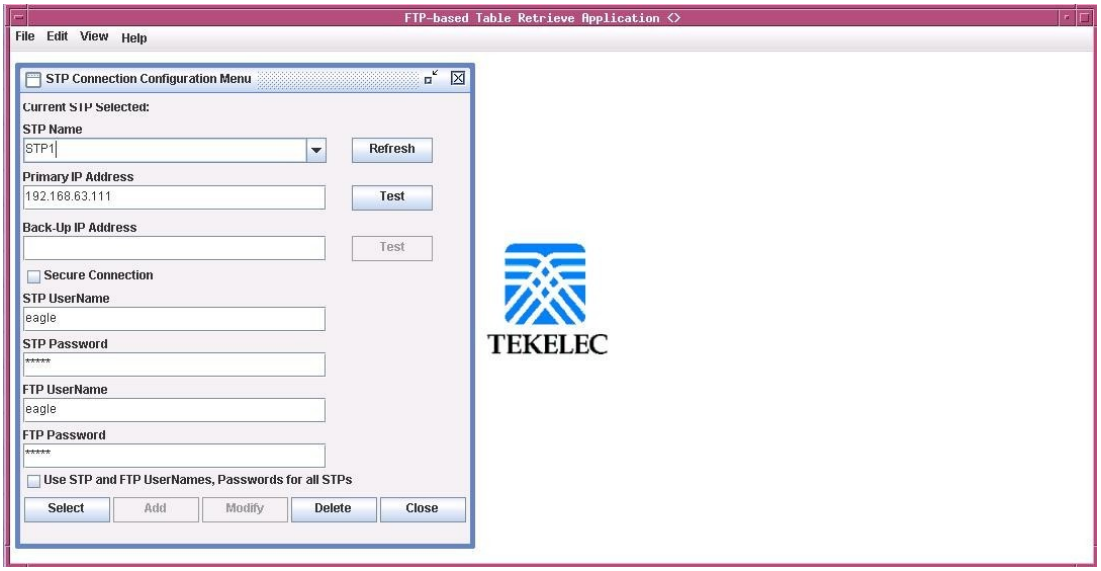
1. Type the STP name in the STP Name field in the STP Connection Configuration Menu window. The Refresh, Test, Select, Delete, and Close buttons are enabled.

   Figure 17: Selecting an STP Configuration Record by Typing in the STP Name Field (FTRA 4.2)



2. Click the Refresh button. The STP configuration record for the specified STP is displayed.

   Figure 18: STP Configuration Record (FTRA 4.2)



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.

Figure 19: STP Name Does Not Exist Error Message

Testing an STP Configuration Record

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window.

   See *Figure 6: STP Connection Configuration Menu Window (FTRA 4.2)* on page 13. The **STP Connection Configuration Menu** window opens.

2. Display the STP configuration record being modified.

   Go to the *Displaying an Existing STP Configuration Record* on page 20 procedure.

3. Click the **Test** button.

   The **Connectivity Test Log** window opens. See *Figure 20: Connectivity Test Log Window with No Errors* on page 23 and *Figure 21: Connectivity Test Log Window with Errors* on page 24.

   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 20: Connectivity Test Log Window with No Errors

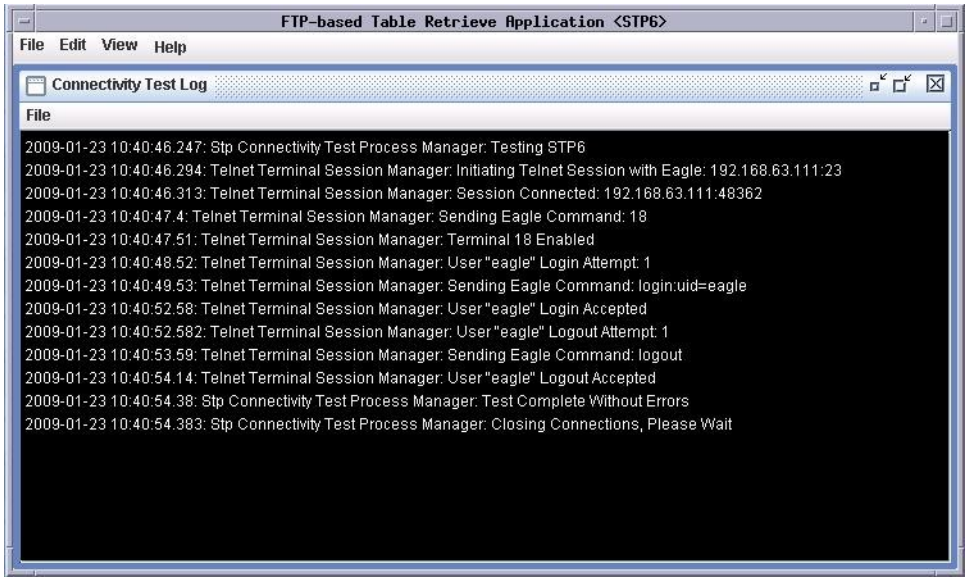
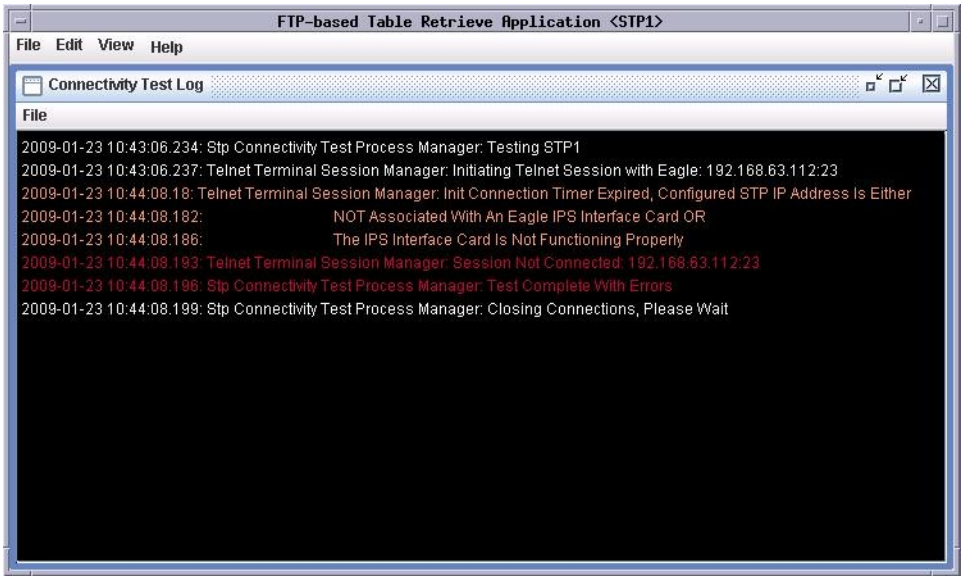


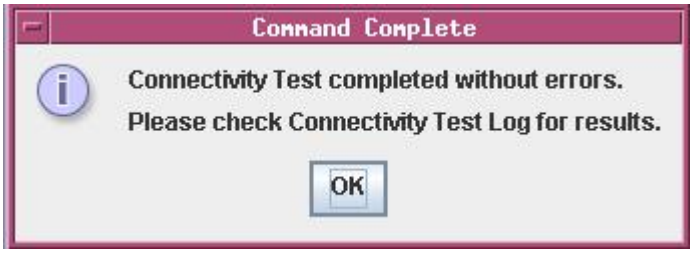
Figure 21: Connectivity Test Log Window with Errors



4. When the test is complete, the **Command Complete** window opens.

   See *Figure 22: Command Complete Connectivity Test Window* on page 24. Click **OK** to continue.

Figure 22: Command Complete Connectivity Test Window

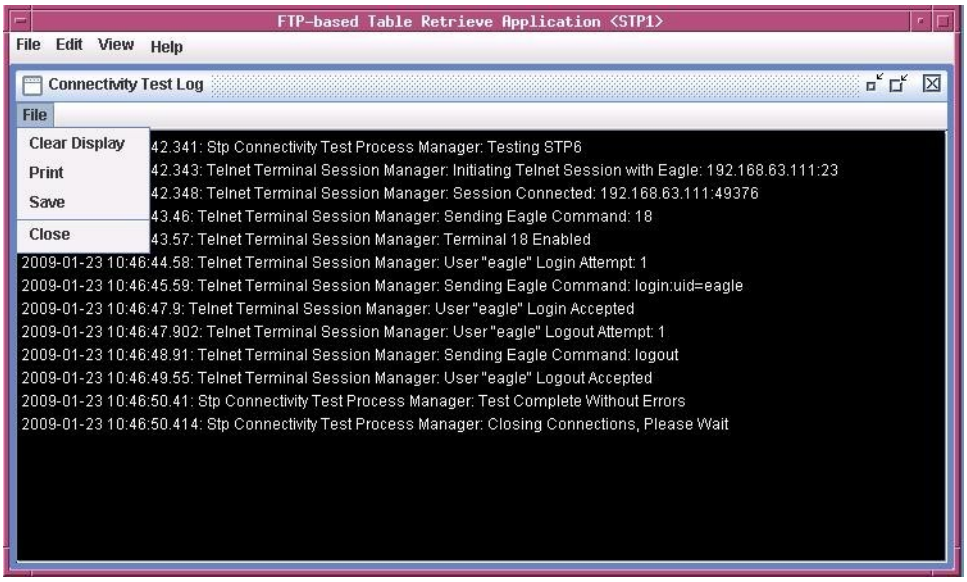


Connectivity Test Log File Menu

The **File** menu in the **Connectivity Test Log** window, shown in *Figure 23: File Menu in the Connectivity Test Log Window* on page 25, 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 23: 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.

Select **File > Clear Display** in the **Connectivity Test Log** window.

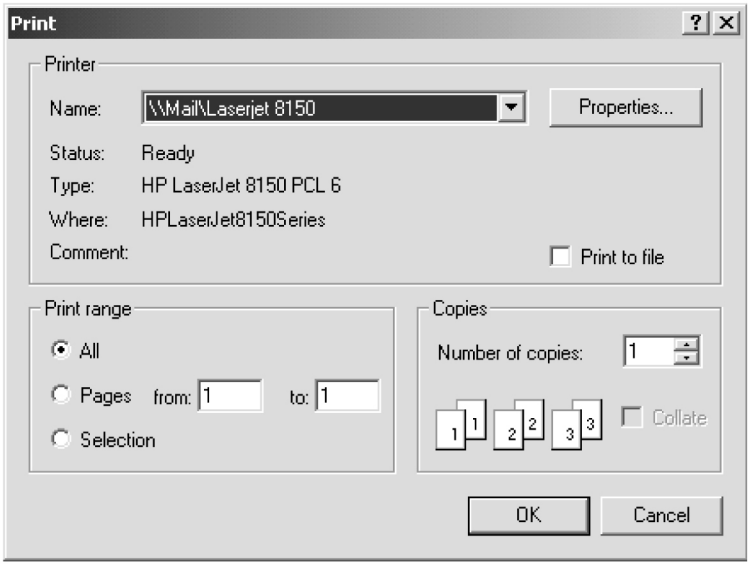
The Connectivity Test Log display clears.

Printing the Connectivity Test Log

1. Select **File > Print** in the **Connectivity Test Log** window.

   The **Print** window opens. See *Figure 24: Print Window* on page 26.

   Figure 24: 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.

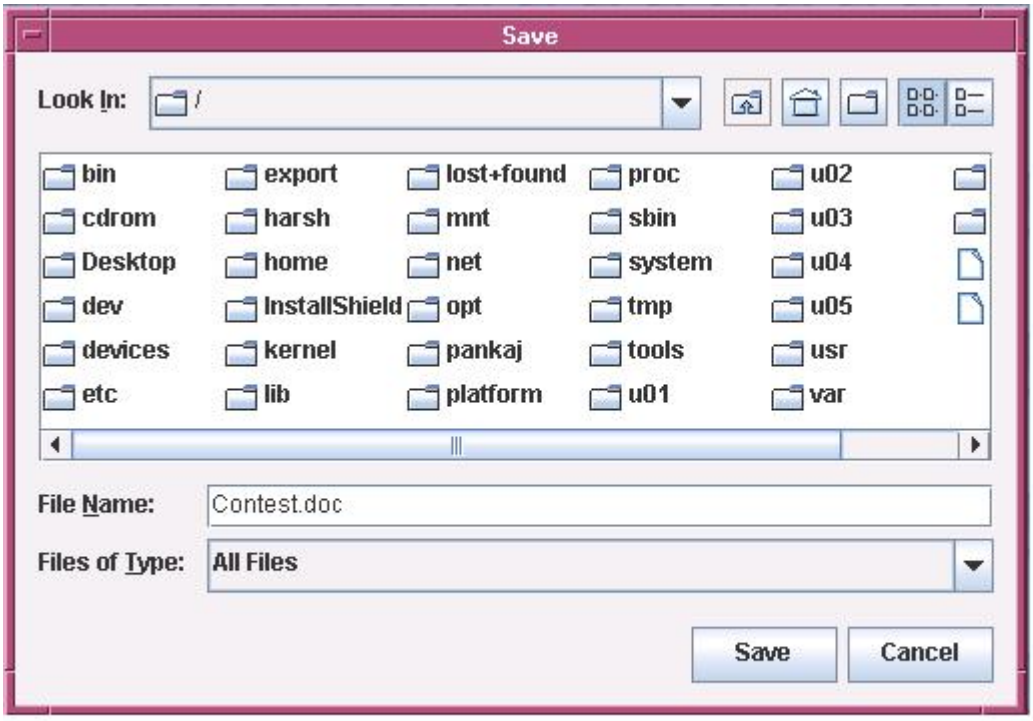
4. If you decide not to print the Connectivity Test Log, click the **Cancel** button in the **Print** window.

Saving the Connectivity Test Log to a File

1. Select **File > Save** in the **Connectivity Test Log** window.

   The **Save** window opens. See *Figure 25: Save Window* on page 26.

   Figure 25: 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:

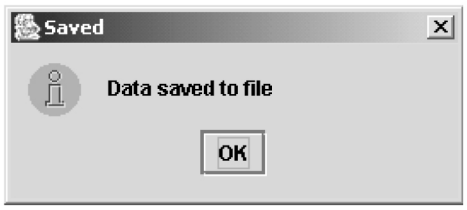
   The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.

   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."

   Figure 26: 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

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.

The **Connectivity Test Log** window closes.

Modifying an Existing STP Configuration Record

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window.

   See *Figure 6: STP Connection Configuration Menu Window (FTRA 4.2)* on page 13. The **STP Connection Configuration Menu** window opens.

2. Display the STP configuration record being modified.

   Go to the *Displaying an Existing STP Configuration Record* on page 20 procedure.

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:

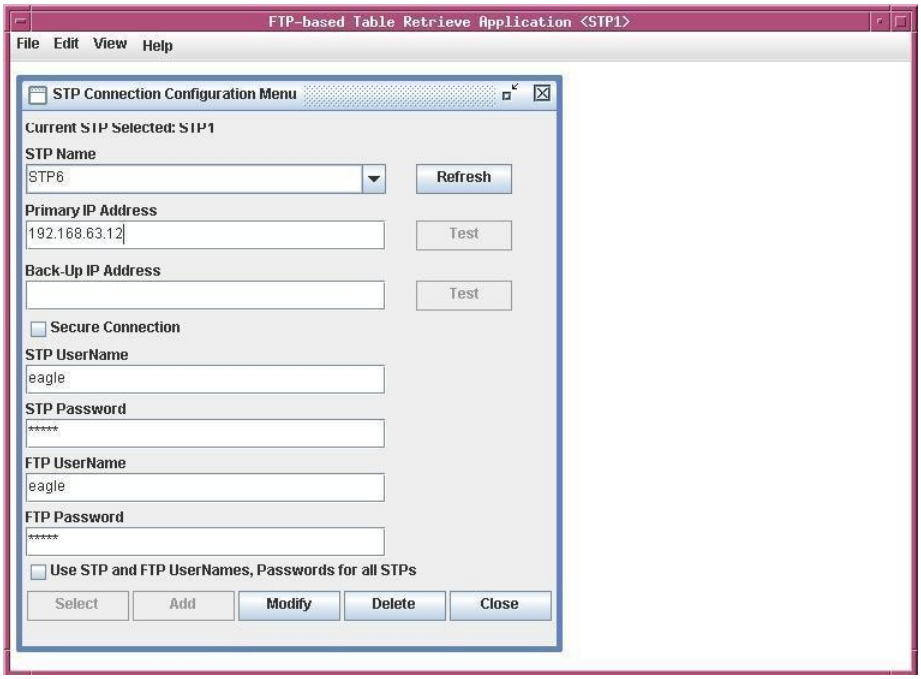
   The STP name cannot be changed.

   If the IP address, STP user name, or STP password is not entered correctly, an error message is displayed. See *Figure 9: Invalid IP Address Error Message* on page 18, *Figure 10: Invalid STP User Name Error Message* on page 18, or *Figure 11: Invalid STP Password Error Message* on page 19. If the FTP user name and FTP password are not entered, an error message is displayed. See *Figure 12: Invalid FTP User Name Error Message* on page 19 or *Figure 13: Invalid FTP Password Error Message* on page 19.

4. To apply the changes, click the **Modify** button.

   See *Figure 27: Modifying STP Configuration Record Parameters (FTRA 4.2)* on page 28 (FTRA 4.2 and later). 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 28: STP Data Modified Window* on page 29). Click **OK** in the **STP Data Modified** window to continue.

   Figure 27: Modifying STP Configuration Record Parameters (FTRA 4.2)



CAUTION

CAUTION:

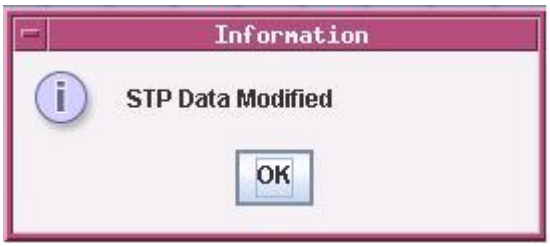
If the Use STP and FTP UserNames and Passwords for all STPs box is checked, then all user names and passwords for all STPs in the STP Configuration database are changed to the user name and password for the displayed STP.

CAUTION

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 ISS. 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 28: 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 29: Modify Warning Window* on page 30.

Figure 29: 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* on page 20 procedure.

Deleting an STP Configuration Record

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window.

   See *Figure 6: STP Connection Configuration Menu Window (FTRA 4.2)* on page 13. The **STP Connection Configuration Prabhat Menu** window opens.

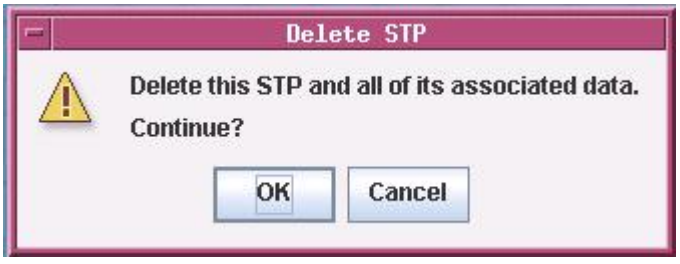
2. Display the STP configuration record being deleted.

   Go to the *Displaying an Existing STP Configuration Record* on page 20 procedure. 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 30: Delete STP Window* on page 30.

   Figure 30: 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 nameis no longer in the STP Connection Configuration database.

   Go to the *Displaying an Existing STP Configuration Record* on page 20 procedure.

Selecting the Current STP

Before retrieving database tables from an EAGLE 5 ISS, or sending commands to an EAGLE 5 ISS, 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.

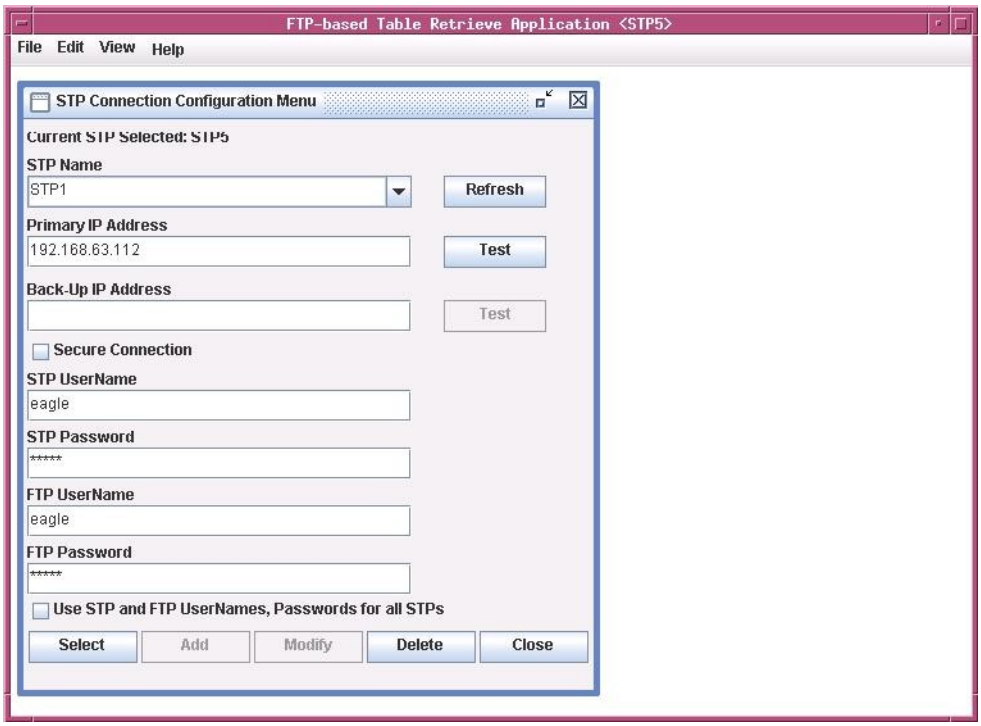
1. Display an existing STP configuration record.

   Go to the *Displaying an Existing STP Configuration Record* on page 20 procedure.

2. Click the **Select** button.

3. 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 31: Current STP Selected (FTRA 4.2)* on page 31 (FTRA 4.2) .

   Figure 31: Current STP Selected (FTRA 4.2)



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 ISS Host Key Provisioning

An EAGLE 5 ISS using secure connections has a unique host key for each IPSM in the EAGLE 5 ISS. This key is used by the FTRA (FTRA 4.0 and later) to positively identify or authenticate each IPSM's telnet server on the EAGLE 5 ISS. The FTRA will not connect to an unauthenticated server. The FTRA authenticates the server by matching its preinstalled host key with the key received from the EAGLE 5 ISS when the connection between the EAGLE 5 ISS and the FTRA is made.

This procedure installs the public host key fingerprint, generated when the IPSM is installed into the EAGLE 5 ISS, re initialized 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 ISS that the FTRA will connect to, but only for EAGLE 5 ISSs using secure connections to connect to the FTRA. This procedure must be performed before any secure connection between the EAGLE 5 ISS and the FTRA can be initiated.

Note:

Once the IPSM is installed into the EAGLE 5 ISS, 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. Re initializing 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 ISS 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 ISS, you will receive the following warning message (*Figure 32: IP Address Warning Message* on page 32).

Figure 32: IP Address Warning Message

If the warning message shown in *Figure 32: IP Address Warning Message* on page 32 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* on page 28), or add the public host key fingerprint to the FTRA's **hosts.xml** file.

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 ISS) strong authentication, designed to provide security between the FTRA and the EAGLE 5 ISS. This also prevents a hostile server from tricking the FTRA into exposing any EAGLE 5 ISS 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 ISS 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.

1. On the EAGLE 5 ISS, 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 ISS, 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* on page 4 before removing and reinserting the IPSM.

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 ISS, 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 *Adding an STP Configuration Record* on page 16 procedure), 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 *Modifying an Existing STP Configuration Record* on page 28 procedure). 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* on page 23 procedure.

   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 ISS and the FTRA shown in the Connectivity Test Log match. The Connectivity Test Log shows both the key received from the EAGLE 5 ISS host and the key contained in the **hosts.xml** file for the EAGLE 5 ISS host. The following is an example from the Connectivity Test Log containing a host key mismatch. The key received from the EAGLE 5 ISS 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 ISS using the **FTP Server Configuration** menu before database tables can be retrieved from the EAGLE 5 ISS, or command files can be sent to the EAGLE 5 ISS.

Note:

If the Secure Connection box in the STP Connection Configuration Menu window 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.

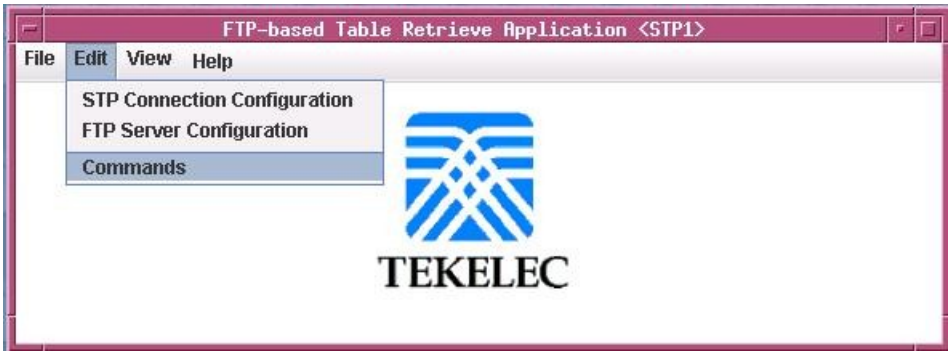
Note:

Any firewall between the FTRA and the FTP server configured in the FTP Server Configuration Menu window (*Figure 34: FTP Server Configuration Menu Window* on page 37), must allow FTPs to the IP address specified in the FTP Server Configuration Menu window.

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

   See *Figure 33: FTP-Based Table Retrieve Application Edit Commands Menu* on page 37.

   Figure 33: FTP-Based Table Retrieve Application Edit Commands Menu



   The **FTP Server Configuration Menu** window opens. See *Figure 34: FTP Server Configuration Menu Window* on page 37 and *Table 4: FTP Server Configuration Menu Window Descriptions* on page 38.

   Figure 34: FTP Server Configuration Menu Window

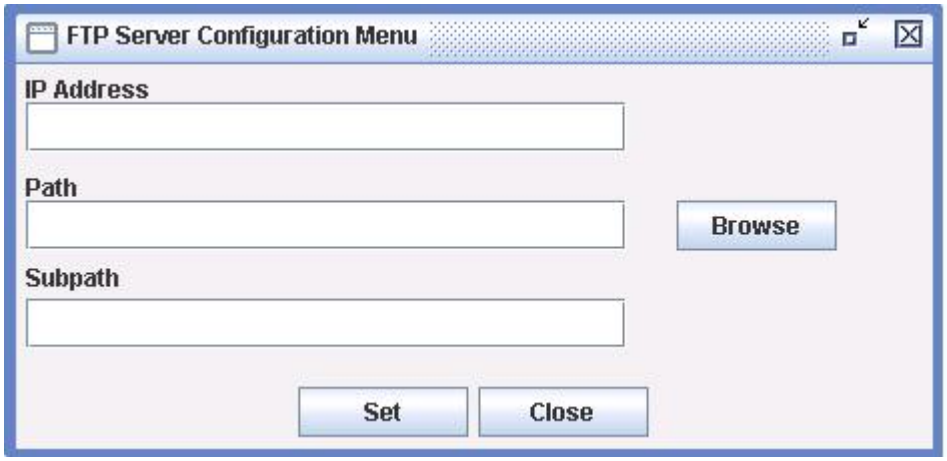


Table 4: FTP Server Configuration Menu Window Descriptions

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 ISS `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.

Item	Description
Set	Stores the FTP server configuration data.
Close	Closes the **FTP Server Configuration Menu** window.

2. Enter the IP address of the STP in the **IP Address** field.

   Note:

   If the format is not entered correctly, the Invalid IP Address warning window is displayed. See *Figure 35: Invalid IP Address Error Message* on page 39.

   Figure 35: 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 36: Select Starting Directory Window* on page 39 and *Table 5: Select Starting Directory Window Descriptions* on page 40.

   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 36: Select Starting Directory Window

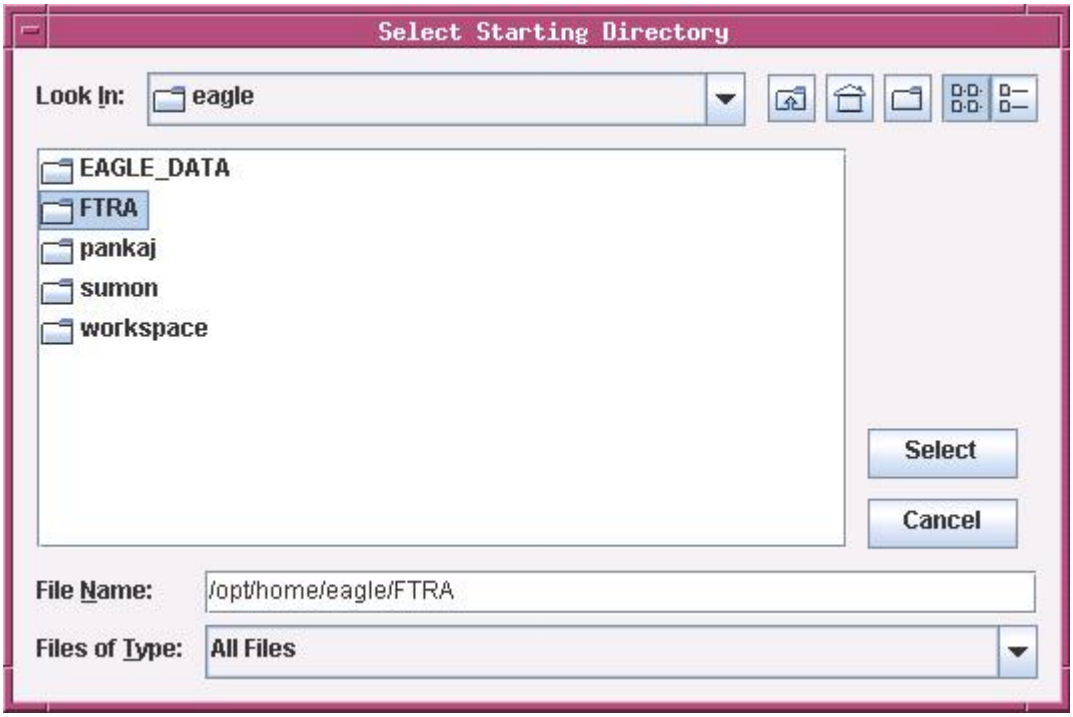


Table 5: Select Starting Directory Window Descriptions

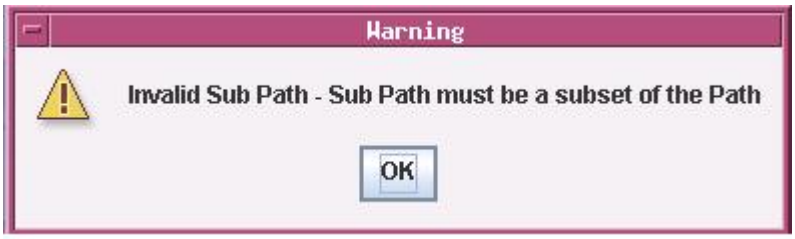
Item	Description
Fields	
Look in:	A drop down menu that allows the user to browse through the directory structures.
File Name:	The name of the file to be selected.
Files of type:	A drop down menu that allows the user to select all files of a particular type.
Buttons	
Select	Takes the contents of the **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 37: Invalid Subpath Window* on page 41.

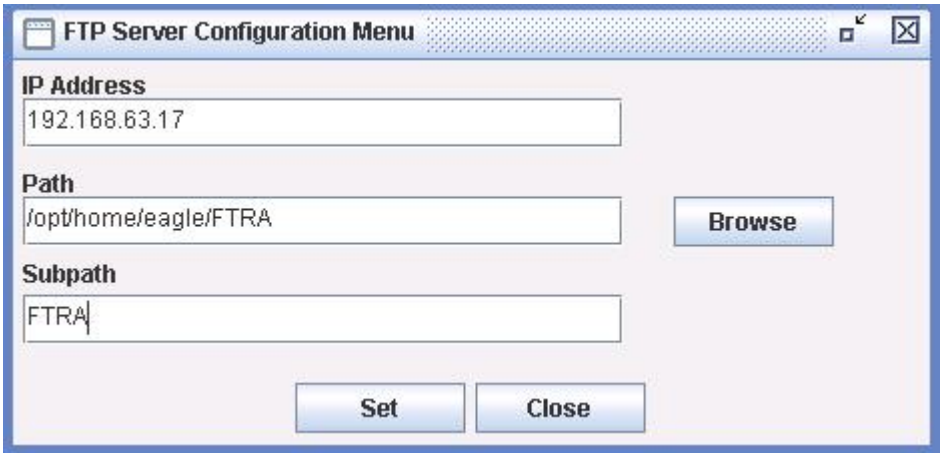
Figure 37: Invalid Subpath Window



5. Click the **Set** button.

See *Figure 38: FTP Server Configuration Example* on page 41.

Figure 38: FTP Server Configuration Example



The **FTP Server Data Set** window opens. See *Figure 39: FTP Server Data Set Window* on page 41.

Figure 39: FTP Server Data Set Window

Click **OK** to continue.

Retrieve Database Tables from an STP

Retrieve Tables Window

The **Retrieve Tables** window (see *Figure 41: Retrieve Tables Window* on page 42) 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

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 E GTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`) in the same retrieve tables request, you will receive a warning (*Figure 40: GTT Warning Window* on page 42) that errors can be caused by attempting to retrieve and convert the GTT and EGTT database tables from the same EAGLE 5 ISS.

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-gttsel`, `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 40: GTT Warning Window

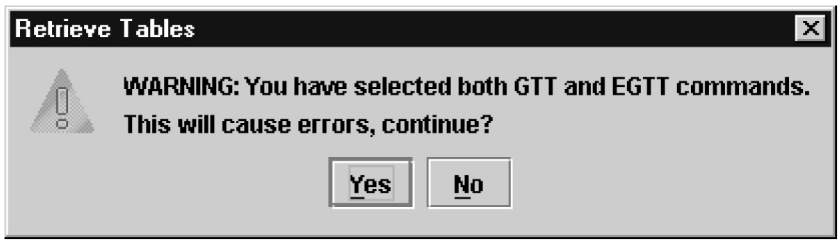


Figure 41: Retrieve Tables Window

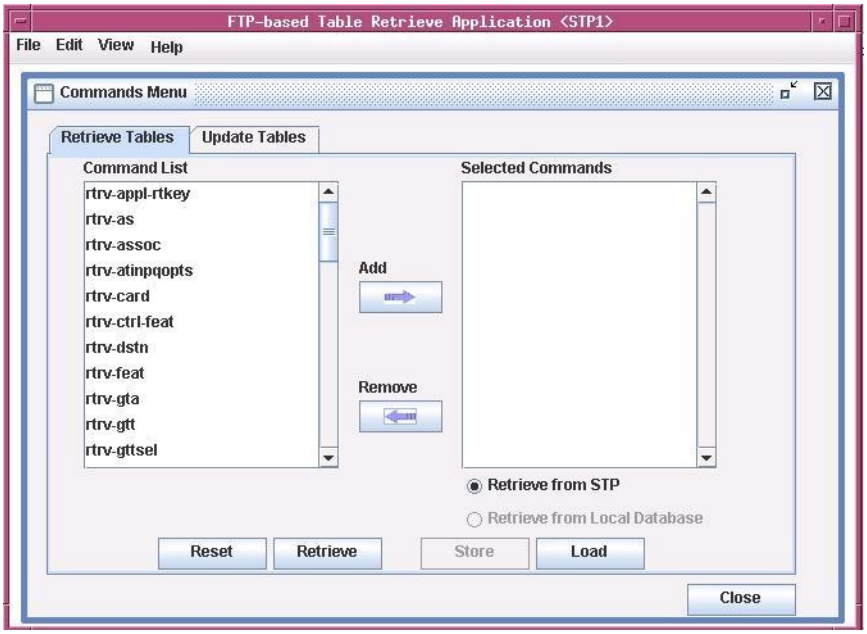


Table 6: Retrieve Tables Window Description on page 43 shows the description of the fields and buttons in the **Retrieve Tables** window.

Table 6: Retrieve Tables Window Description

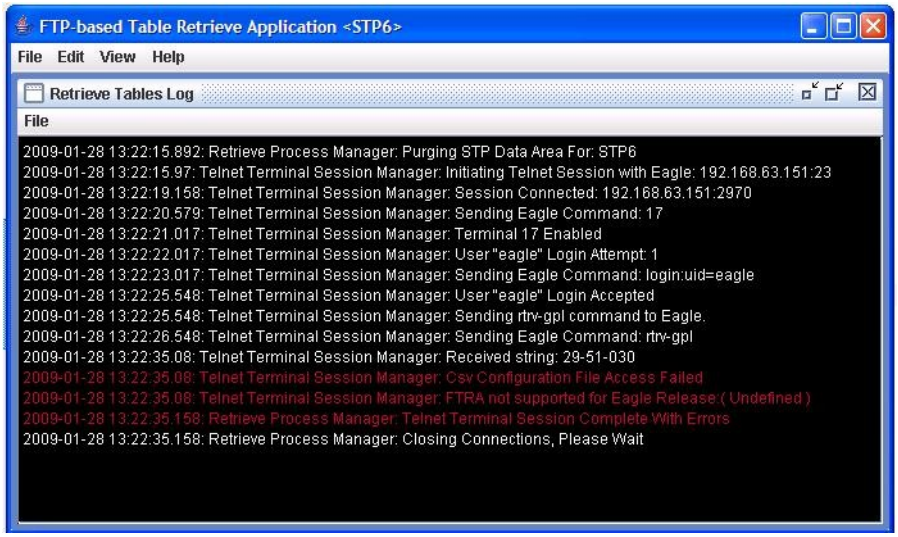
Item	Description
Fields	
Command List	Contains a predefined list of retrieve commands.
Selected Commands	These commands are used to determine which database tables are retrieved from the selected STP. From one to all of the retrieve commands can be selected for retrieval.
Buttons	
Add	Moves the highlighted 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 and places them in the **Command List** box in alphabetical order.

Item	Description
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 4.0 and later, the EAGLE 5 ISS release 32.0 and later are supported if that release supports CSV file output.

When a Retrieve Tables command is performed, FTRA 4.0 and later verifies that the EAGLE 5 ISS is running one of the supported releases. If the EAGLE 5 ISS is not supported, an error message is displayed and the Retrieve Tables command is terminated. See *Figure 42: Retrieve Table Log - Release Not Supported Error* on page 44.

Figure 42: Retrieve Table Log - Release Not Supported Error



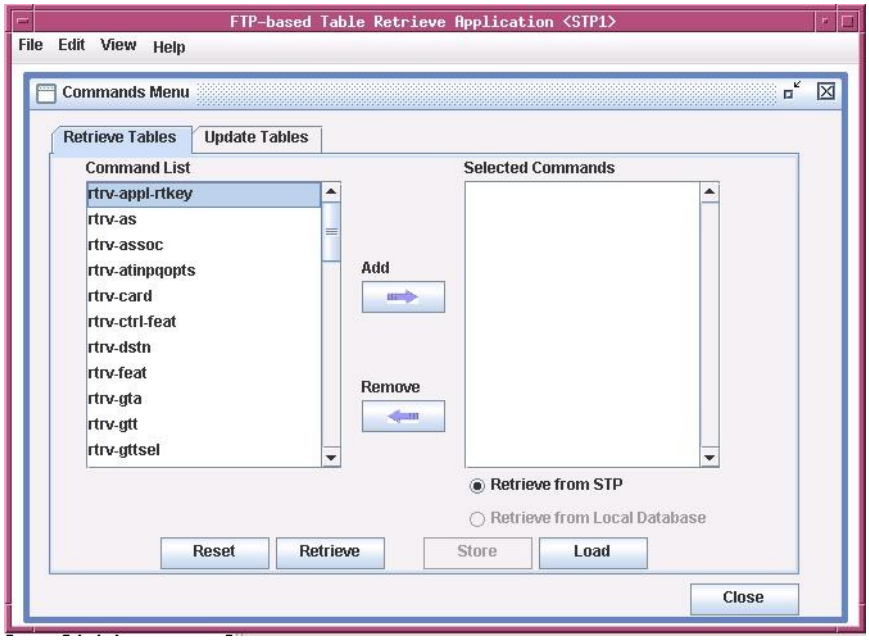
If the EAGLE 5 ISS release is supported, the Retrieve Tables command is performed and operations on the FTRA can continue.

1. Select **Edit > Commands > Retrieve Tables** from the **FTP-Based Table Retrieve Application** window. See *Figure 43: Commands Menu in the FTP-Based Table Retrieve Application Window* on page 45. The **Retrieve Tables** window opens. See *Figure 41: Retrieve Tables Window* on page 42.

   Figure 43: Commands Menu in the FTP-Based Table Retrieve Application Window

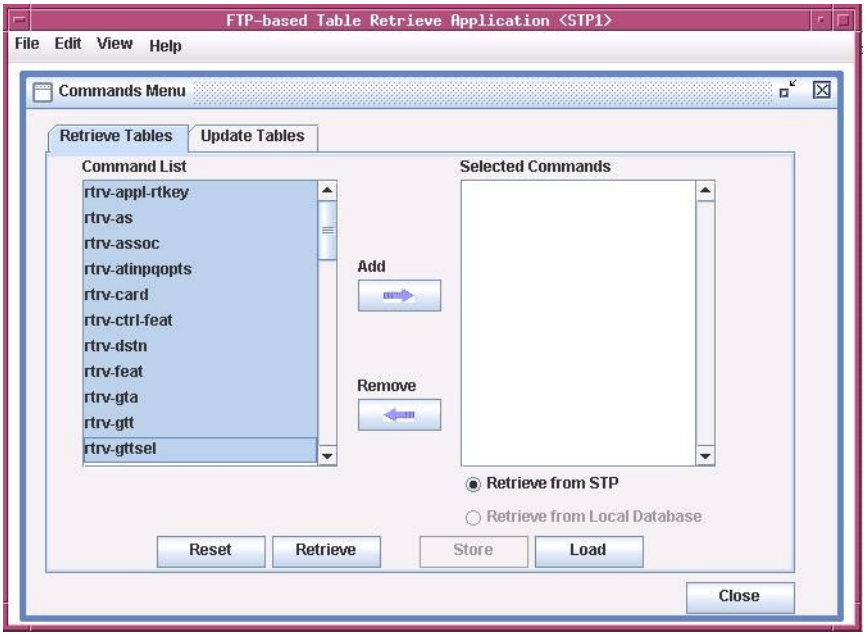
2. To select commands in the **Command List** box of the **Retrieve Tables** window, perform one of these steps: To select a single command, click on the command and it is highlighted. See *Figure 44: Selecting a Command* on page 45.

   Figure 44: Selecting a Command



a. 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 45: Selecting a Range of Commands* on page 46

Figure 45: Selecting a Range of Commands

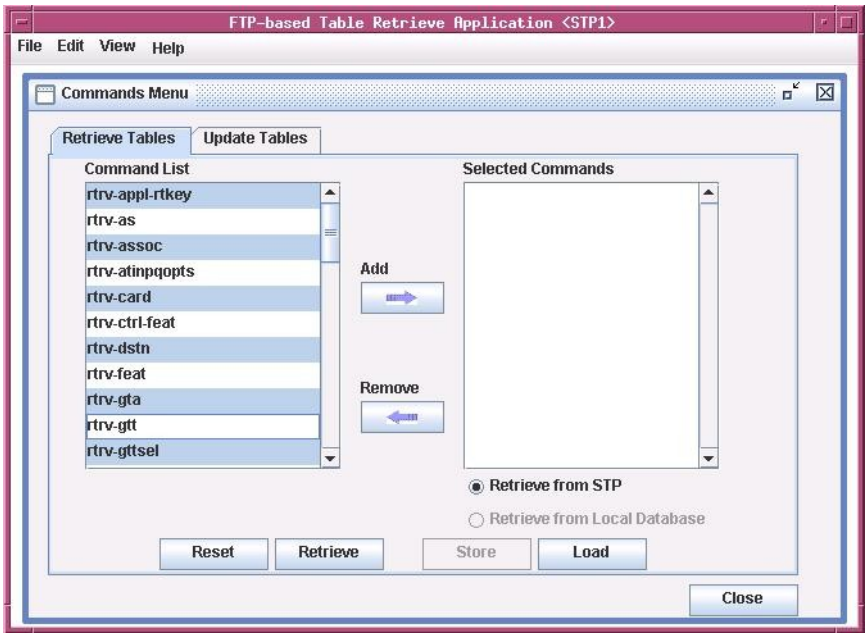


b. To select multiple commands, select the first command, then hold down the Ctrl key and click on each of the commands to be selected. The selected commands are highlighted. See Figure 2-44.

Note:

If you have selected any of these GTT commands (`rtrv-tt`, `rtrv-gtt`) and these E GTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`) in substeps a or b, see the *Caution* on page 42.

Figure 46: Selecting Multiple Commands



3. 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 47: Adding a Command to the Selected Commands Box* on page 47, *Figure 48: Adding a Range of Commands to the Selected Commands Box* on page 48, and *Figure 49: Adding Multiple Commands to the Selected Commands Box* on page 48

Figure 47: Adding a Command to the Selected Commands Box

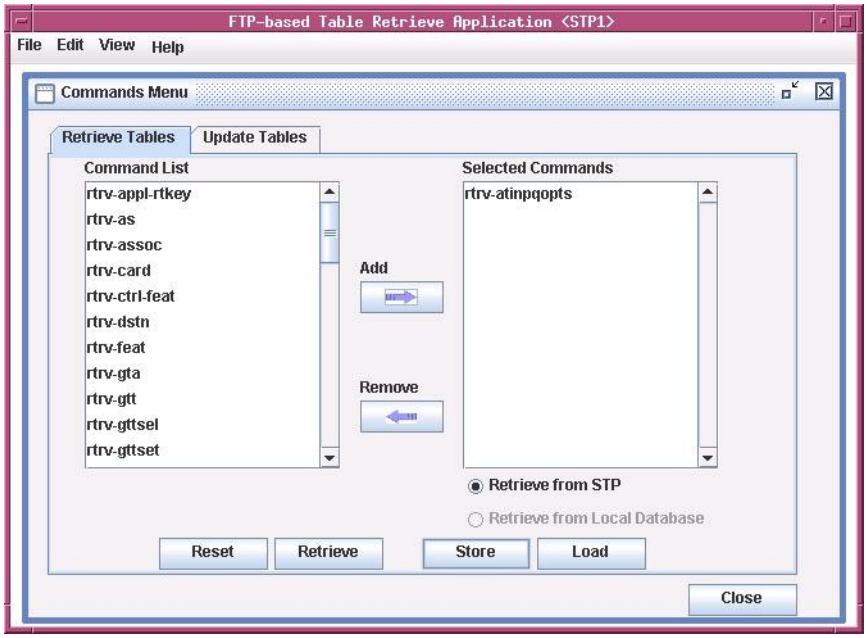


Figure 48: Adding a Range of Commands to the Selected Commands Box

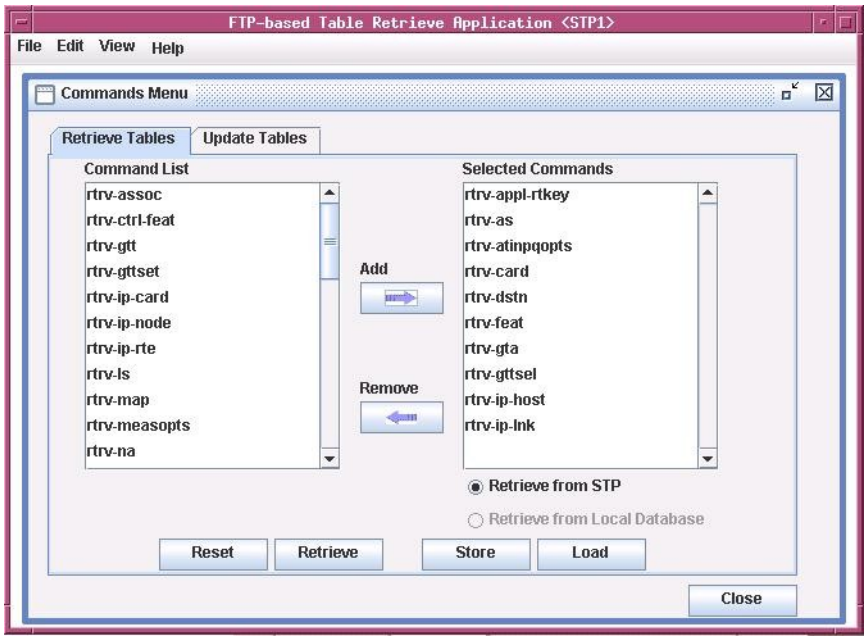
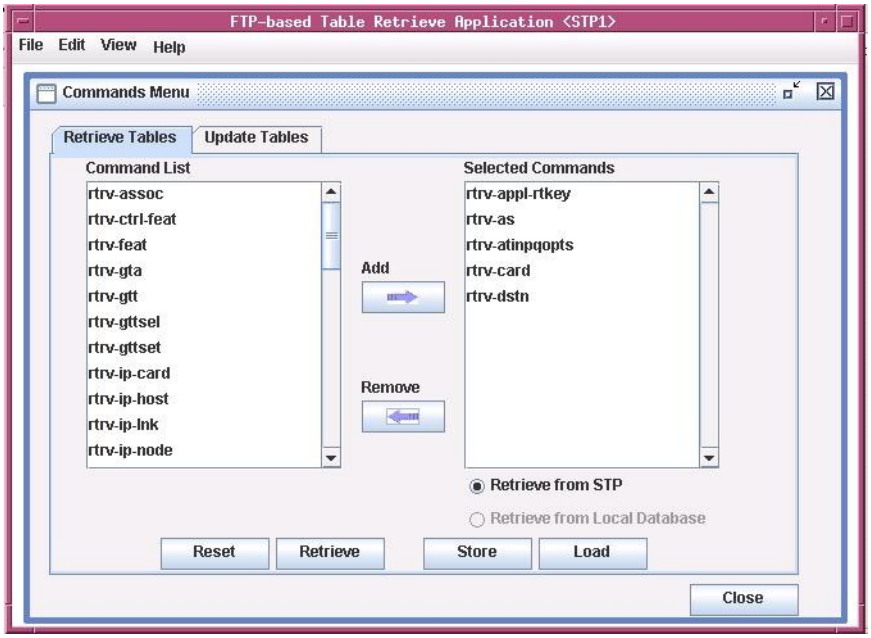


Figure 49: Adding Multiple Commands to the Selected Commands Box



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 50: Command Selected to be Removed in the Selected Commands Box* on page 49.

   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 51: Command Removed from the Selected Commands Box* on page 50.

   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.

Figure 50: Command Selected to be Removed in the Selected Commands Box

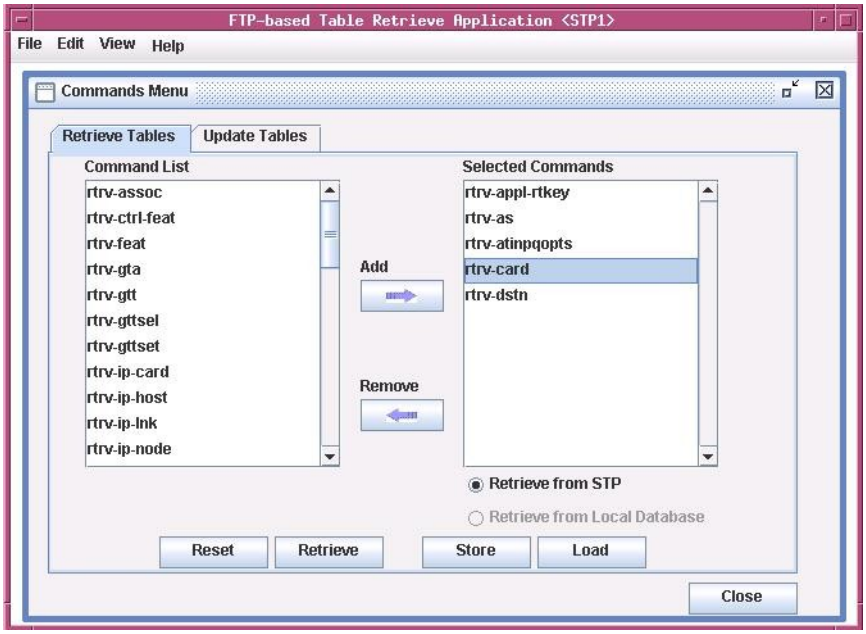
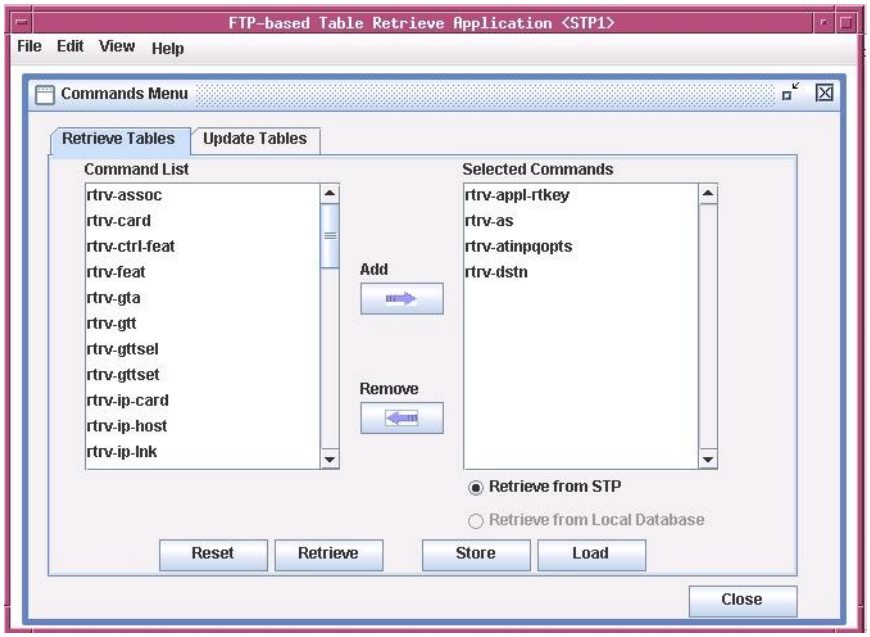


Figure 51: Command Removed from the Selected Commands Box



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 52: Command Data Stored Window* on page 50

Figure 52: Command Data Stored Window

Click **OK** to continue.

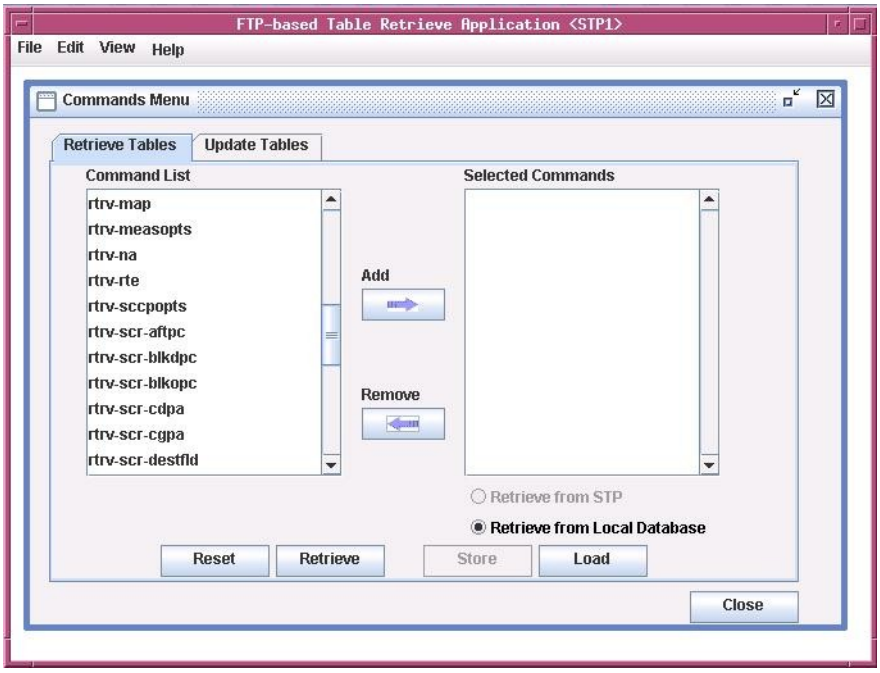
Fo verify what retrieve commands are stored, click the **Load** button. The stored commands appear in the **Selected Commands** box, as shown in *Figure 47: Adding a Command to the Selected Commands Box* on page 47, *Figure 48: Adding a Range of Commands to the Selected Commands Box* on page 48, or *Figure 49: Adding Multiple Commands to the Selected Commands Box* on page 48.

To use the Command Line Interface, go to the *Command Line Interface* on page 59.

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 53: Retrieving Database Tables from the Local Database* on page 51. Click the **Retrieve** button.

Figure 53: Retrieving Database Tables from the Local Database



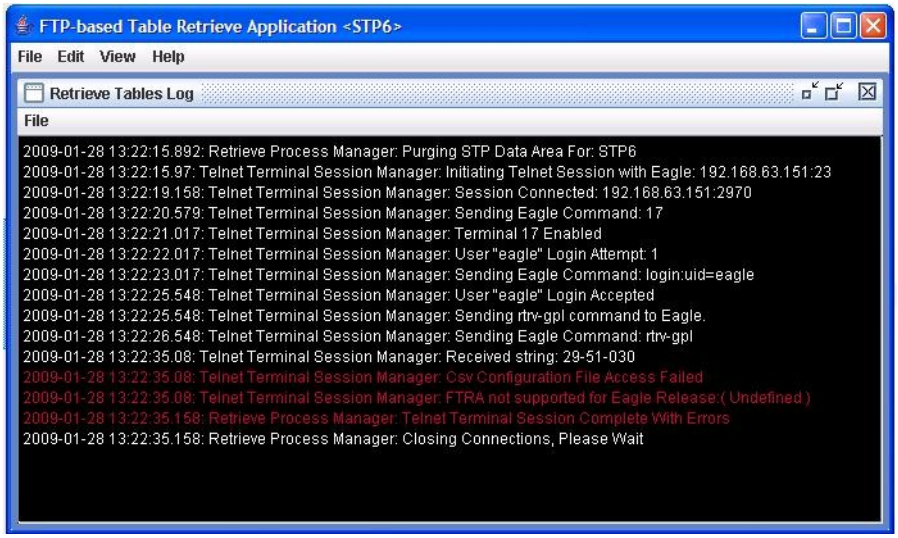
Note: If step 6 was performed, skip step 7. This procedure is finished.

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 54: Retrieve Tables Log Window - Processing Retrieve Request* on page 52) and displays the message "Processing Retrieve Request, Please Wait" until the retrieve process completes.

Note: The telnet terminals on the EAGLE 5 ISS to which FTRA will be connecting should have their terminal settings set to `all=no` (use the EAGLE 5 ISS command `chg-trm:trm=<telnet terminal>:all=no` to make this setting; use the EAGLE 5 ISS command `rtrv-trm` to verify the EAGLE 5 ISS terminal settings). On an STP with heavy U IM 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 E GTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`), see the *Caution* on page 42.

Figure 54: 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 the *Figure 55: Command Complete Window Without Errors* on page 52.

Figure 55: 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 56: Command Complete Window With Errors* on page 52.

Figure 56: Command Complete Window With Errors

The **Retrieve Table Log** window opens. See *Figure 57: Retrieve Tables Log Window without Errors* on page 53 and *Figure 58: Retrieve Table Log with Errors* on page 54. 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 57: Retrieve Tables Log Window without Errors* on page 53).

The Retrieve Tables Log displays the information of the CSV files generated for the selected retrieve commands. The filenames of the CSV files are displayed in ascending order except for the filename of the `rtrv-stp` CSV file. Since the `rtrv-stp` command CSV is not generated by the CSVGEN(X) utility, the CSV filename for the `rtrv-stp` command is not displayed in the sorted order with other CSV filenames, but it is displayed as the last entry in the filenames list. Since the Retrieve Tables Log is generated by the CSVGEN(X) utility, no record of processing the `rtrv-stp` command is displayed in this log. See *Figure 59: Retrieve Table Log with the RTRV-STP Command CSV Example* on page 54 for an example of the Retrieve Tables Log when the `rtrv-stp` command is processed.

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 57: Retrieve Tables Log Window without Errors* on page 53 and *Figure 58: Retrieve Table Log with Errors* on page 54.

Figure 57: Retrieve Tables Log Window without Errors

Figure 58: Retrieve Table Log with Errors

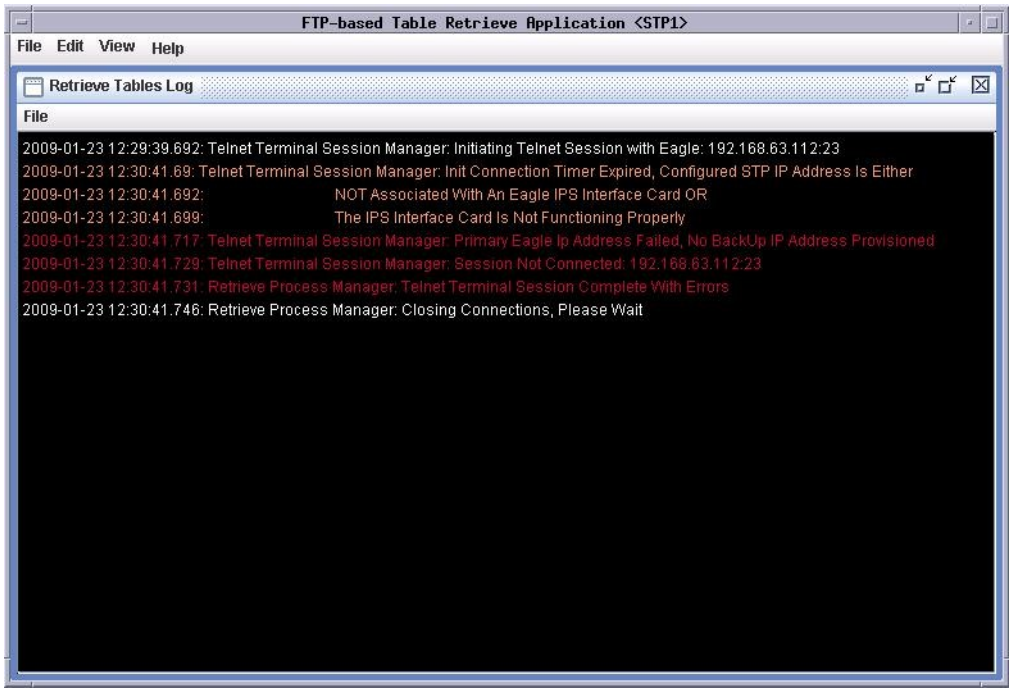
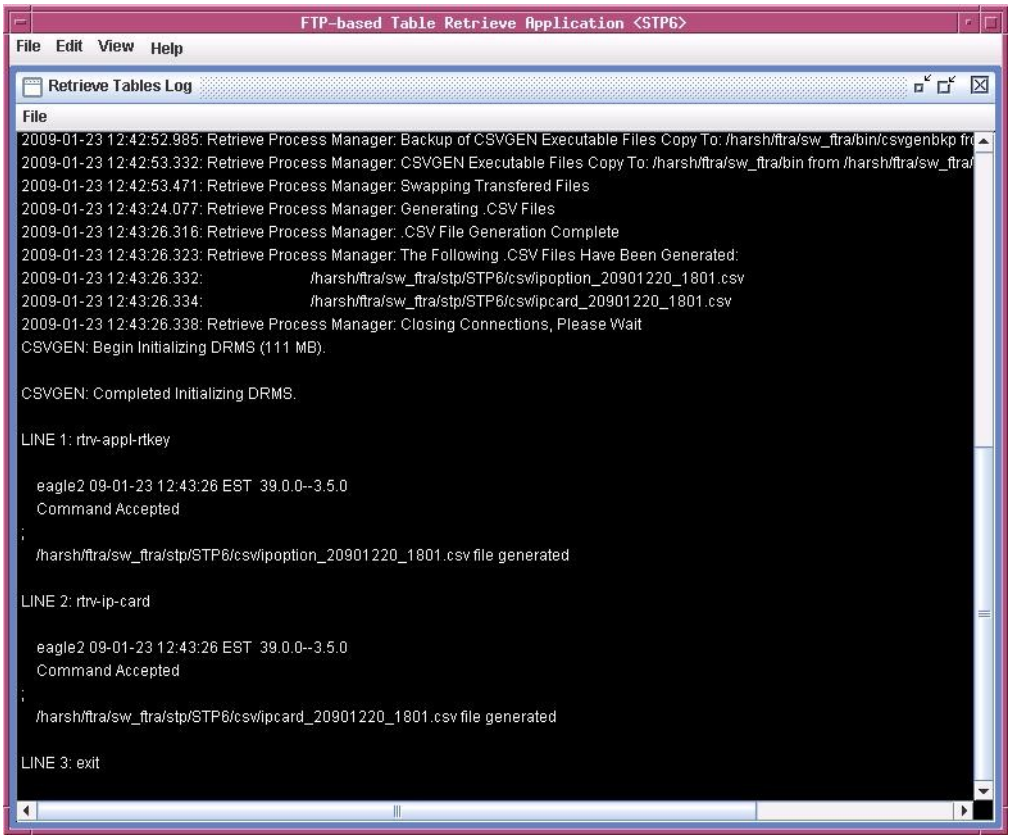


Figure 59: Retrieve Table Log with the RTRV-STP Command CSV Example

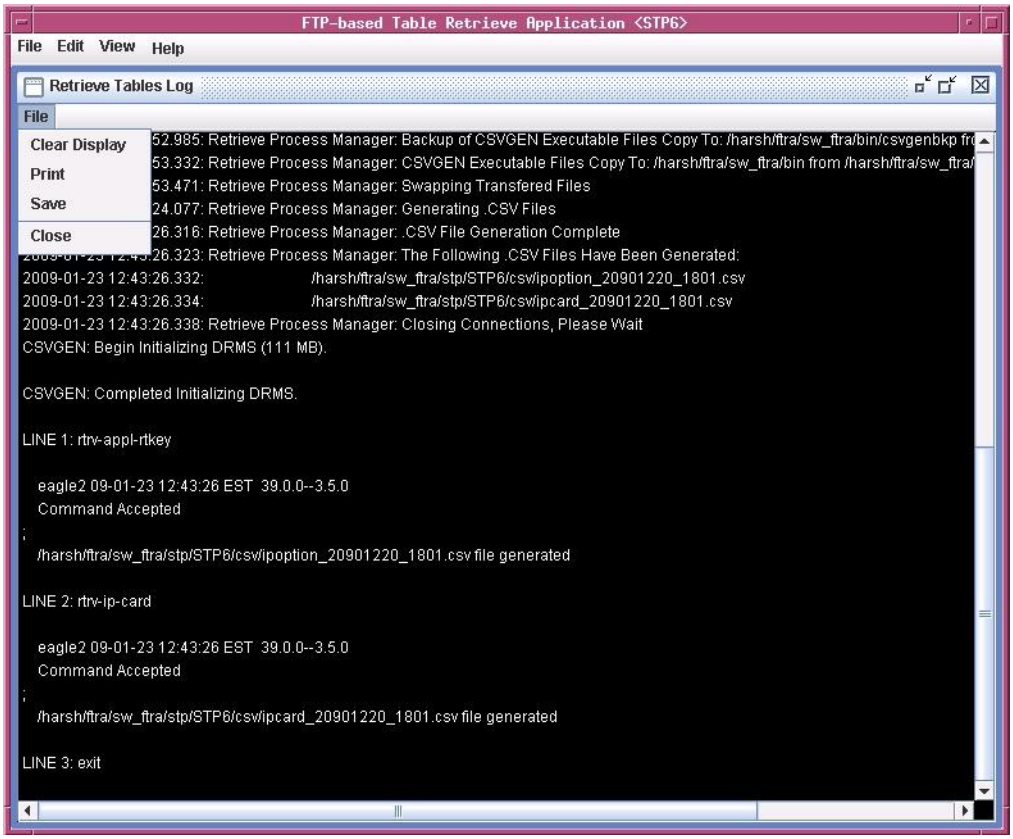


Retrieve Tables Log File Menu

The **File** menu in the **Retrieve Tables Log** window, shown in *Figure 60: File Menu in the Retrieve Tables Log Window* on page 55, provides these selections:

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

Figure 60: 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.

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

1. Select **File > Clear Display** in the **Retrieve Tables Log** window.
2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window.

   See *Figure 61: View Menu* on page 56. The **Retrieve Tables Log** window opens

   Figure 61: View Menu

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

   The Retrieve Tables Log display clears

Printing the Retrieve Tables Log

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

1. Select **File > Print** in the **Retrieve Tables Log** window.

   See *Figure 60: File Menu in the Retrieve Tables Log Window* on page 55.

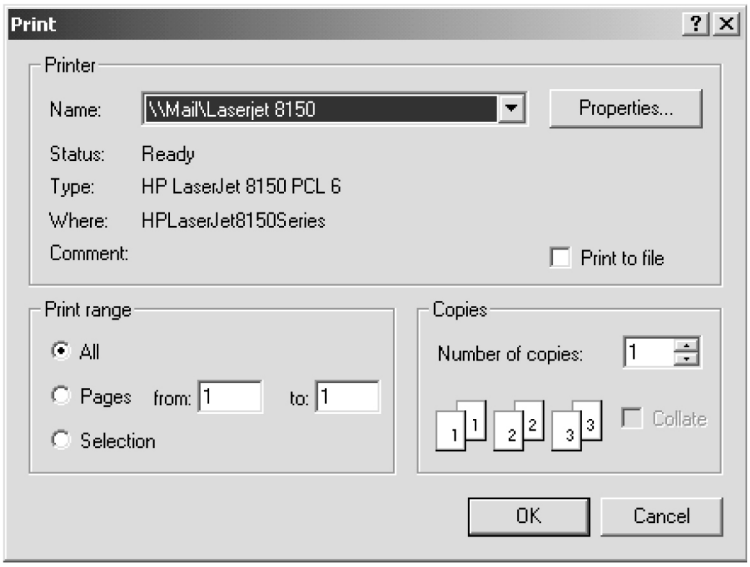
2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window.

   See *Figure 61: View Menu* on page 56. The Retrieve Tables Log opens.

3. Select **File > Print** in the **Retrieve Tables Log** window.

   The **Print** window opens. See *Figure 62: Print Window* on page 57.

   Figure 62: 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

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

1. Select **File > Save** in the **Retrieve Tables Log** window.

   See *Figure 60: File Menu in the Retrieve Tables Log Window* on page 55.

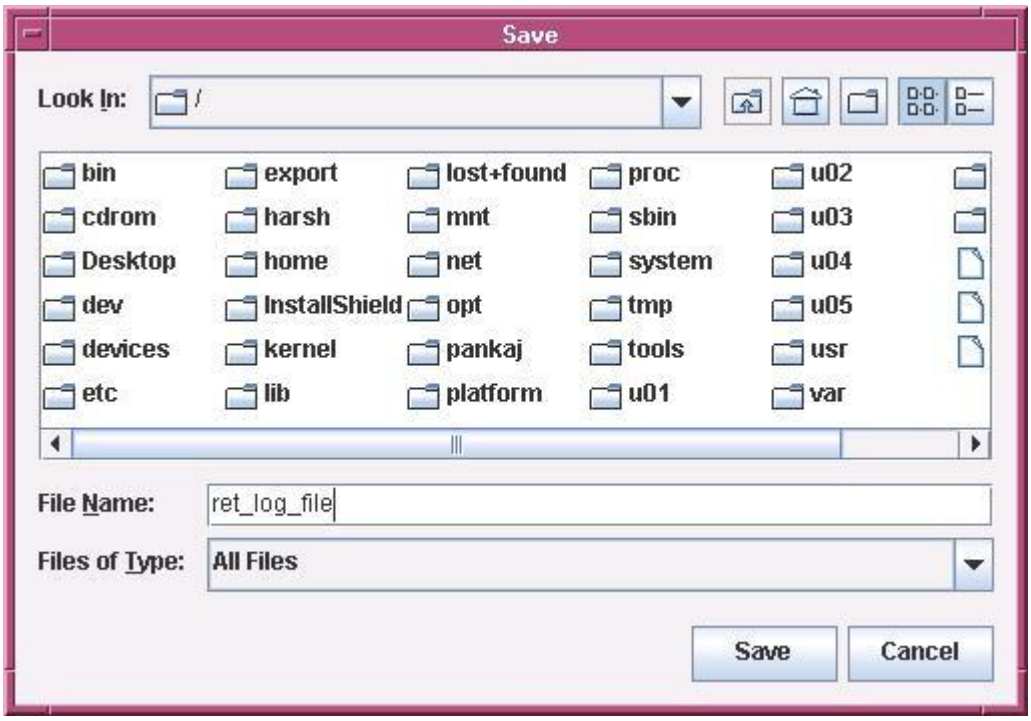
2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window.

   The **Retrieve Tables Log** window opens.

3. Select **File > Save** in the **Retrieve Tables Log** window.

   The **Save** window opens. See *Figure 63: Save Window* on page 58.

   Figure 63: 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:

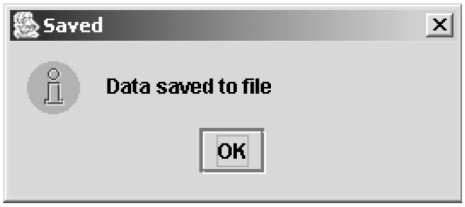
   The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.

   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 64: Saved File Confirmation Window* on page 58.

   Figure 64: 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

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 60: File Menu in the Retrieve Tables Log Window* on page 55. The **Re trieve 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 ISS'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.

The Command Line Interface for FTRA 4.2 allows the user to change the STP Username and Password for an STP already configured in the system.

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)` at the DOS command prompt (in Windows) or at a shell command prompt (in UNIX).

For modifying the Username and Password for an STP, three command line arguments have to be specified with the "-c" option (`ftra –c stpname username password`).

The user can automate this retrieve process through the use of external scheduling software such as Task Scheduled (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.

1. Exit the FTRA application. See *Exit the FTRA* on page 11.
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 stpname username password` command (see *Figure 65: FTRA Windows Command Line Interface* on page 59 or *Figure 66: FTRA Windows Command Line Interface to modify STP data* on page 60). The stored `rtrv` commands are then sent to the provisioned STP. The data tables are retrieved and converted to the CSV file format.

   Result: The username and password shall be modified in the STP configuration for the specified stpname.

   Note: The parameters specified in the command line are case sensitive. For example, an `stpname` specified as EAGLE, Eagle or eagle shall be treated separately.

Figure 65: FTRA Windows Command Line Interface

Figure 66: FTRA Windows Command Line Interface to modify STP data

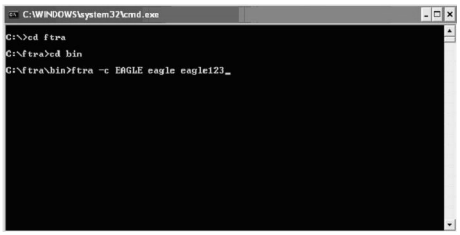


Figure 67: FTRA UNIX Command Line Interface

Figure 68: FTRA UNIX Command Line Interface to modify STP data

Figure 69: FTRA Windows Scheduled Task

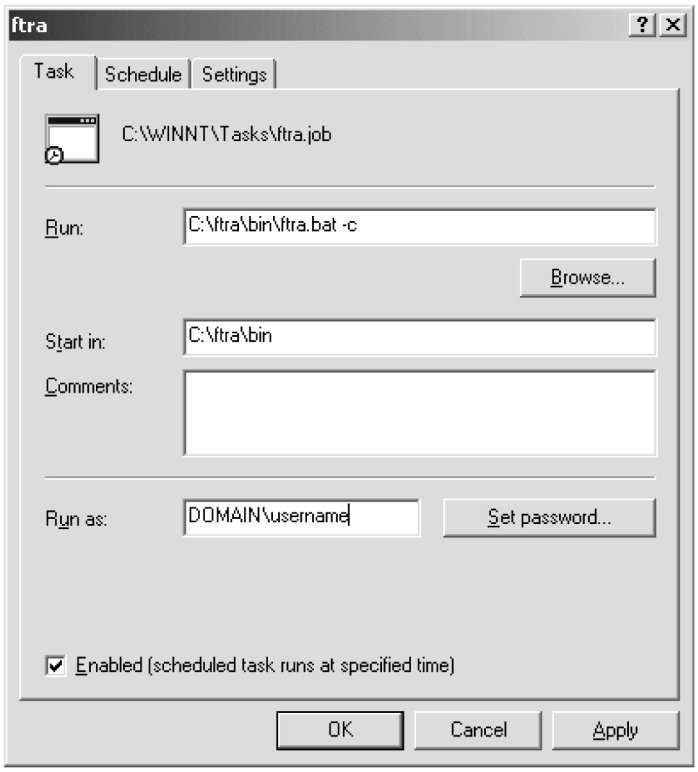


Figure 70: FTRA Windows Scheduled Task to modify STP data

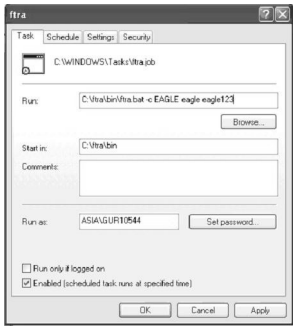


Figure 71: UNIX `cron` job scheduled via `crontab`

Note: Last line shows FTRA scheduled to run at 3am Monday through Friday.

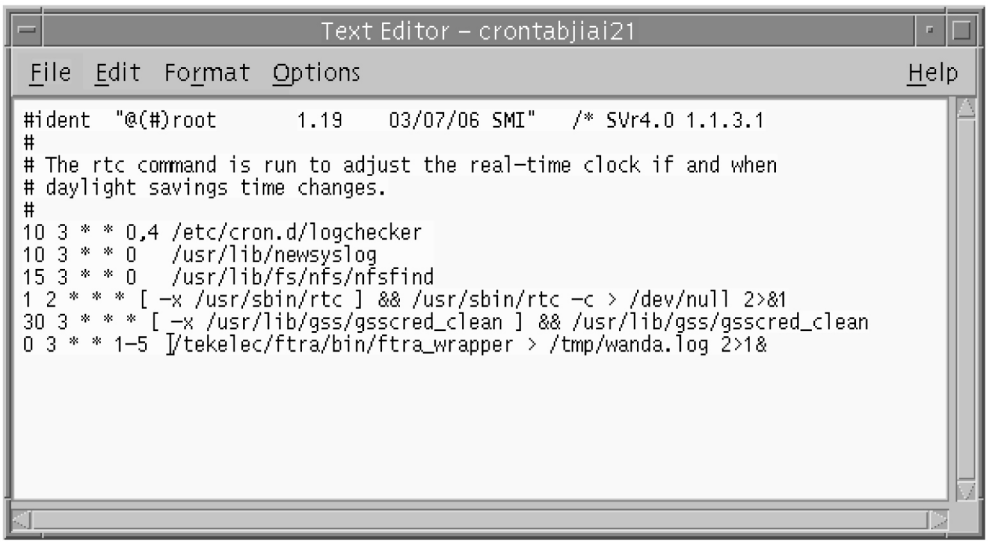


Figure 72: FTRA wrapper script example for UNIX

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.

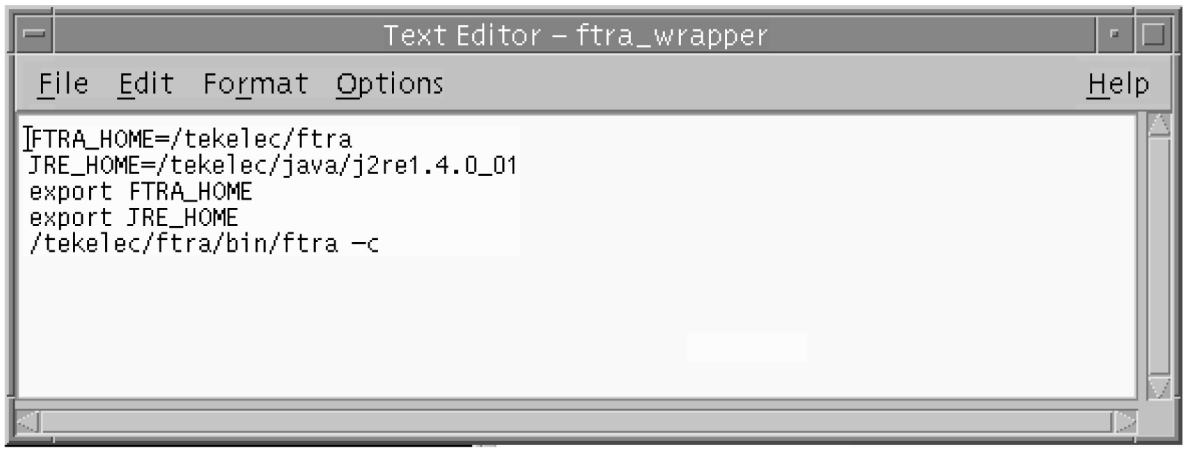
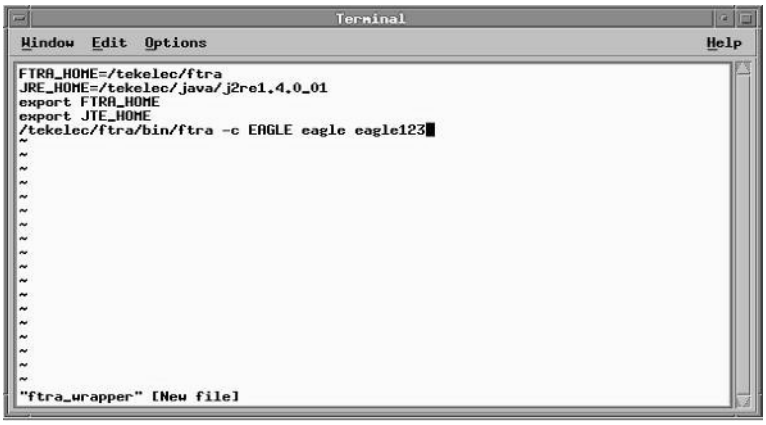


Figure 73: FTRA wrapper script example on UNIX for modifying STP configuration

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.



To automate the FTRA retrieve process, enter the `ftra -c` command, the path to the `bin` directory of FTRA i.e. <*install_directory*> and the start time in the external scheduling software such as Scheduled Task (in Windows, see *Figure 69: FTRA Windows Scheduled Task* on page 61) or "cron" (in UNIX, see *Figure 71: UNIX cron job scheduled via crontab* on page 62).

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

However, to automate the FTRA retrieve process using three command line parameters, enter the `ftra -c stpname username password` command, the path to the bin directory of the FTRA such as <*install_directory*>, and the start time in the external scheduling software such as Scheduled Tasks (on Windows) or "cron" (on UNIX).

Result: The username and password shall be modified in the STP configuration for the specified stpname. When the start time is reached, the stored `rtrv` commands are sent to all provisioned STPs. The data tables will be retrieved and converted to CSV file format for the stored rtrv commands.

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.

Table 7: FTRA - Eagle Compatibility Matrix

	FTRA 1.0	FTRA 1.1	FTRA 2.0	FTRA 2.1	FTRA 2.2	FTRA 3.0	FTRA 4.0	FTRA 4.2
Eagle 28x and earlier	N	N	N	N	N	N	N	N
Eagle 29.0	Y	N	N	N	N	Y	Y	Y
Eagle 30.0	N	Y	Y	N	N	Y	Y	Y
Eagle 30.2	N	N	Y	N	N	Y	Y	Y
Eagle 31.3	N	N	N	Y	N	Y	Y	Y
Eagle 31.6	N	N	N	N	Y	Y	Y	Y
Eagle 31.9	N	N	N	N	Y	Y	Y	Y
Eagle 32.0	N	N	N	N	N	Y*	Y*	Y*
Eagle 35.0 and later	N	N	N	N	N	Y*	Y*, Y**	Y*,Y**
Eagle 41.0	N	N	N	N	N	Y*	Y*, Y**	Y**, Y***

Legend:

N - Not supported.

Y - Supported. (CSVGen installed from FTRA install CD.)

Y* - Supported. (CSVGen transferred from Eagle TDM.)

Y** - Supported. (`rtrv-stp` command support, command line support for modifying STP data.)

Y*** - Supported. (New rtrv commands have been added.)

All other releases of Eagle that are not listed are not officially supported by any release of FTRA.

Note: FTRA 4.1 is partially compatible with EAGLE releases 40.1 and 41.0 only, if E5-OAM is not present. Otherwise, it FTRA 4.1 is not compatible.

Updating Database Tables in the Selected STP

The **Update Tables** window (see *Figure 74: Update Tables Window* on page 65) is used to send EAGLE 5 ISS 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 74: Update Tables Window

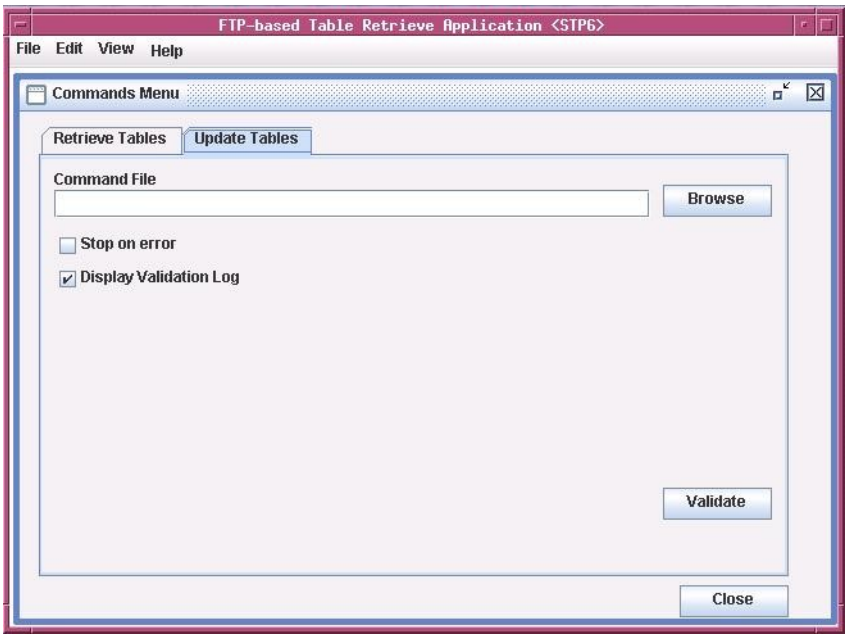


Table 8: Update Tables Window Description on page 65 shows the description of the fields and buttons in the **Update Tables** window.

Table 8: 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

Item	Description
	EAGLE 5 ISS 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 ISS commands using the offline database.
Close	Closes the **Commands Menu** window.

Validating a Command File

1. Select **Edit > Commands > Update Tables** in the **FTP-based Table Retrieve Application** window.

   See *Figure 75: Edit Menu* on page 66. The **Update Tables** window opens. See *Figure 74: Update Tables Window* on page 65.

   Figure 75: Edit Menu

2. Perform one of these steps.
   a) Enter the path and name of the command file in the **Command File** field.
   b) Click the **Browse** button.

      The **Select** window is opened. See *Figure 76: Select Window* on page 67. 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 9: Select Window Descriptions on page 67 shows the description of the buttons in the **Select** window.

Figure 76: Select Window

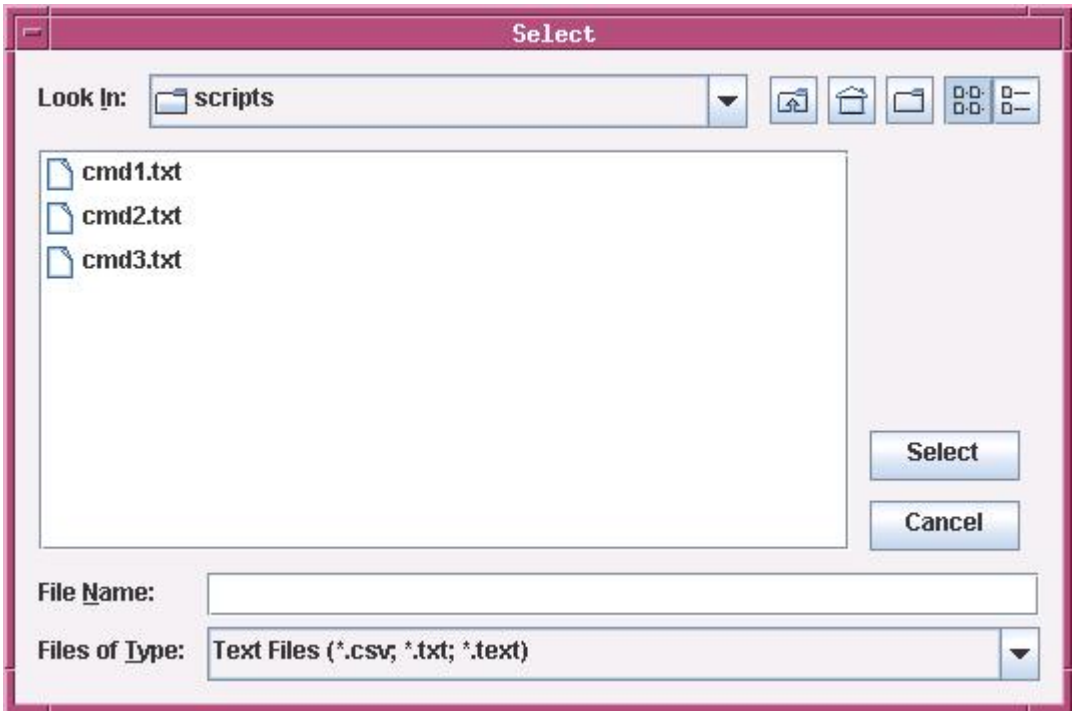


Table 9: Select Window Descriptions

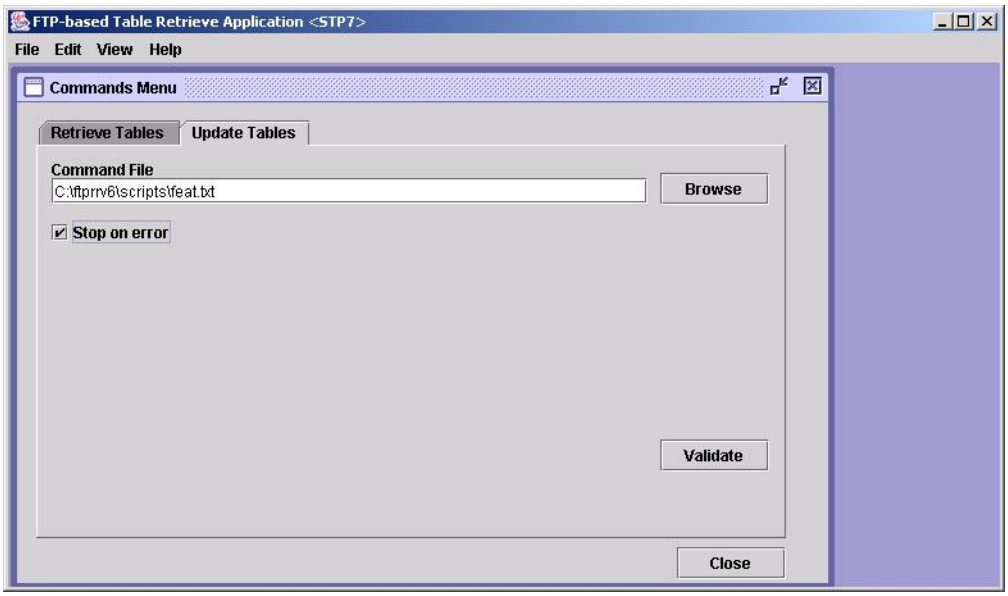
Item	Description
Fields	
Look in:	A drop down menu allowing the user to browse through the directory structures.
File Name:	The name of the file to be selected.
Files of type:	A drop down menu that selects all files.
Buttons	

Item	Description
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 77: Update Tables Window with a Command File Selected and Stop on Error Box Checked* on page 68. 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.

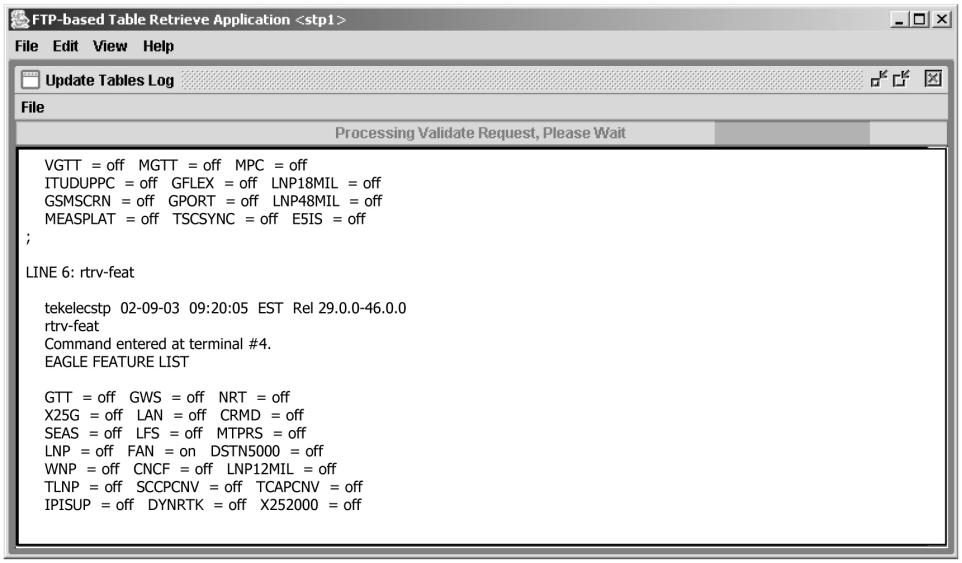
   Figure 77: Update Tables Window with a Command File Selected and Stop on Error Box Checked



4. 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 78: Update Tables Log Window - Processing Retrieve Request* on page 68.

   Figure 78: Update Tables Log Window - Processing Retrieve Request



The **Update Validation Complete** window opens. See *Update Validation Complete Window* on page 69.

5. The **Update Tables Log** window opens.

   It contains the events and error messages generated during the validation. See *Figure 88: Update Tables Log Window after the Commit Command Completed* on page 74, *Figure 89: Update Tables Log* on page 75, and *Figure 90: Update Tables Log with Stop on Error Box Checked in the Update Tables Window* on page 75 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 79: Must Enter Command Script File Name Message* on page 69.

Figure 79: 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 80: Update Validation Complete Window without Errors* on page 69.

Figure 80: Update Validation Complete Window without Errors

Table 10: Update Validation Complete Window Description on page 70 shows the description of the buttons in the **Update Validation Complete** window.

Table 10: 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* on page 71section.
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* on page 71. 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 81: Update Validation Complete Window with Errors* on page 70. 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* on page 71section.

Figure 81: 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 80: Update Validation Complete Window without Errors* on page 69. 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 82: Command Complete Window* on page 71. Click **OK** , to continue. The Update Tables Log contains the commit processing events. See *Figure 88: Update Tables Log Window after the Commit Command Completed* on page 74.

Figure 82: Command Complete Window

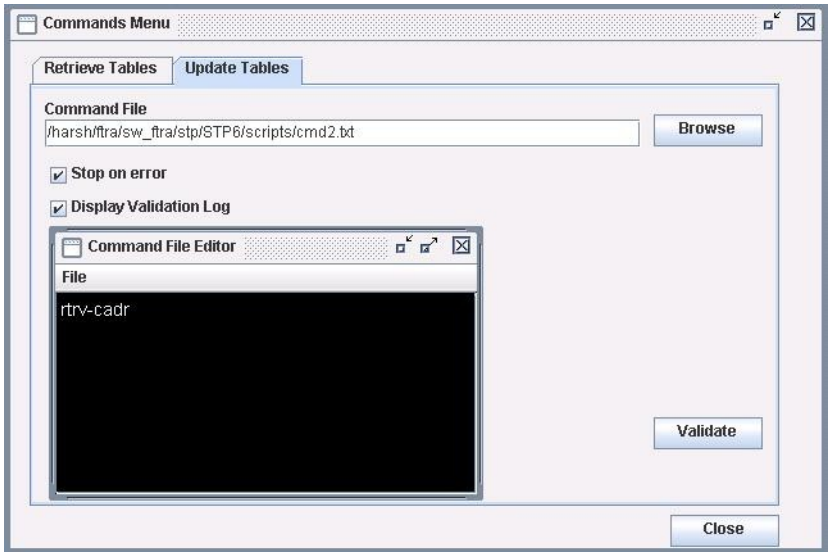
Stop Without Sending or Editing a Command File

To stop the process without sending or editing a command file, click the **Stop** button in the **Update Validation Complete** window. See *Figure 80: Update Validation Complete Window without Errors* on page 69. 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 80: Update Validation Complete Window without Errors* on page 69.

Figure 83: 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.

1. Click the **Edit** button in the **Update Validation Complete** window.

   See *Figure 80: Update Validation Complete Window without Errors* on page 69. The **Command File Editor** window opens. See *Figure 89: Update Tables Log* on page 75.

   Note:

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

   Note:

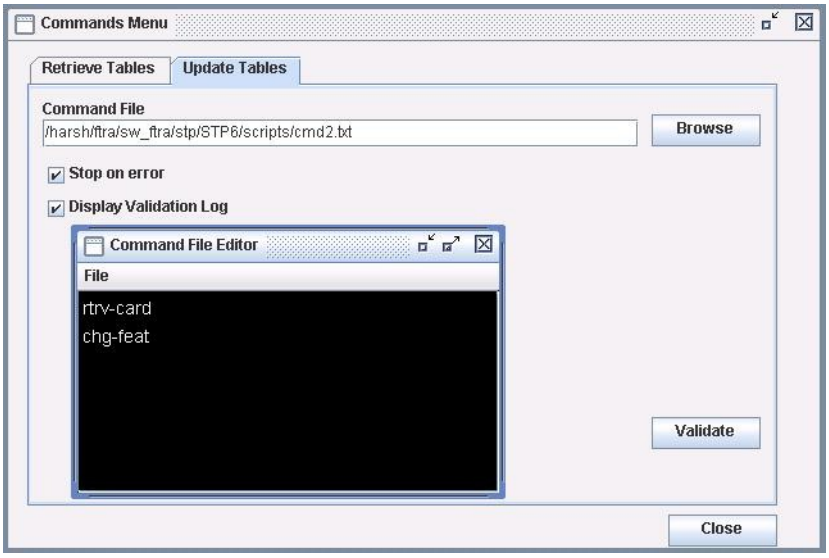
   If an attempt is made to close the Update Tables window while the Command File Editor window is opened, the Command In progress, Cannot Close Window warning message is displayed. See *Figure 84: Command In progress, Cannot Close Window* on page 72.

   Figure 84: Command In progress, Cannot Close Window

2. Edit the command file.

   Figure 85: Command File Editor with Invalid Command on page 72 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.

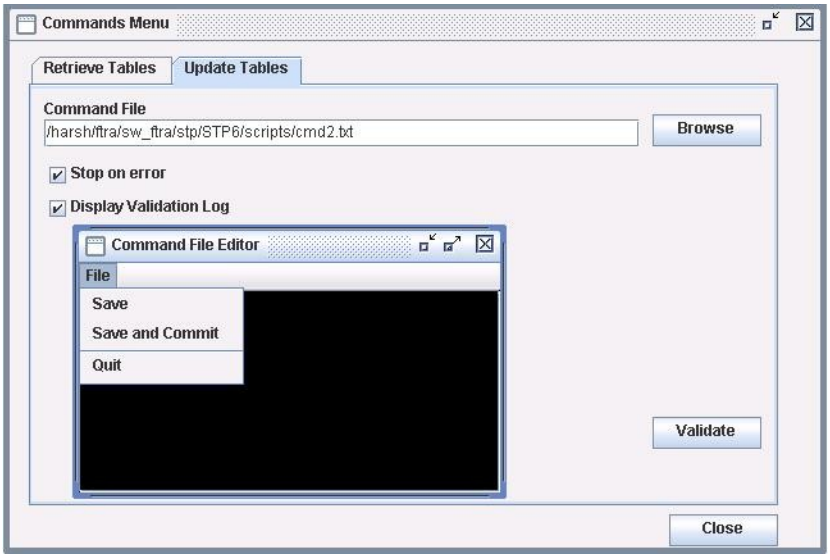
   Figure 85: Command File Editor with Invalid Command



3. When the editing is complete, perform one of these steps.
   a) Select **File > Save** from the **Command File Editor** window (see *Figure 86: File Menu in the Command File Editor Window* on page 73).

      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 86: File Menu in the Command File Editor Window



   b) Select **File > Save and Commit** from the **Command File Editor** window (see *Figure 86: File Menu in the Command File Editor Window* on page 73).

      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 87: Command Complete Window* on page 74. The command file is sent to the selected STP. The

Update Tables Log contains the commit processing events. See *Figure 89: Update Tables Log* on page 75

Figure 87: Command Complete Window

c) Select **File > Quit** from the **Command File Editor** window (see *Figure 86: File Menu in the Command File Editor Window* on page 73).

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" 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 88: Update Tables Log Window after the Commit Command Completed* on page 74, *Figure 89: Update Tables Log* on page 75, *Figure 90: Update Tables Log with Stop on Error Box Checked in the Update Tables Window* on page 75, and *Figure 91: Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window* on page 76 for the **Update Tables Log** window examples.

Figure 88: Update Tables Log Window after the Commit Command Completed

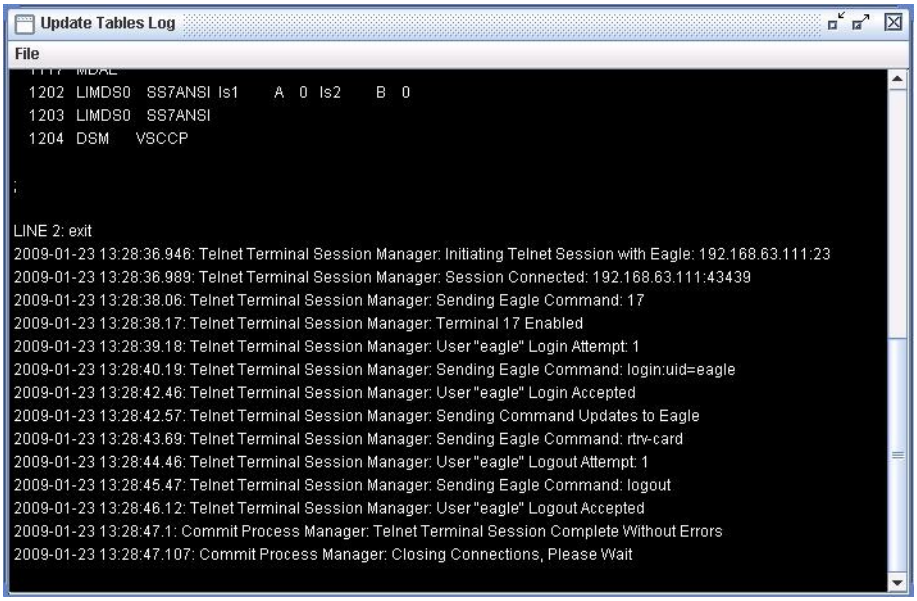


Figure 89: Update Tables Log

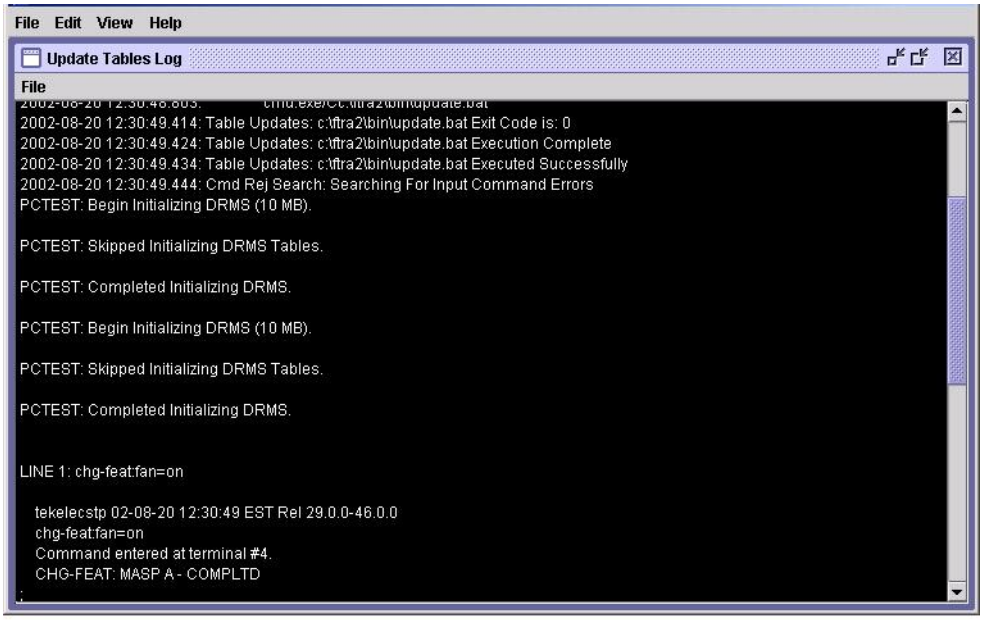


Figure 90: Update Tables Log with Stop on Error Box Checked in the Update Tables Window

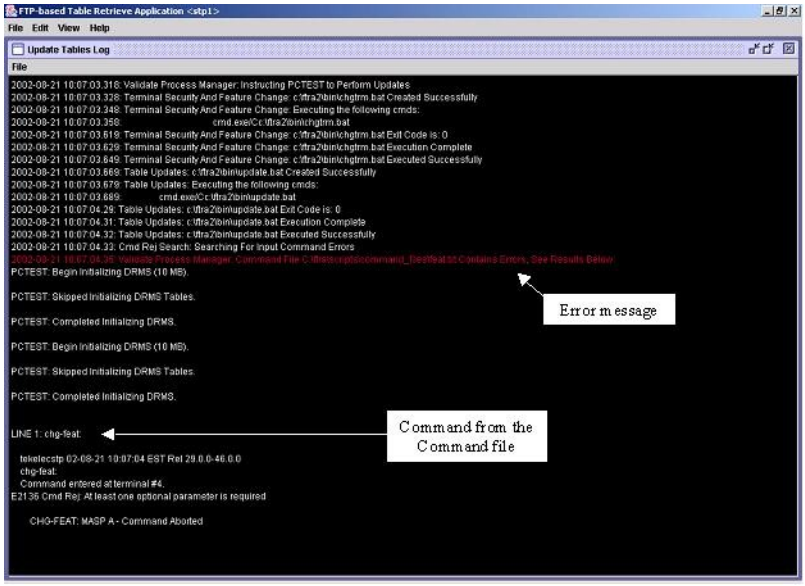
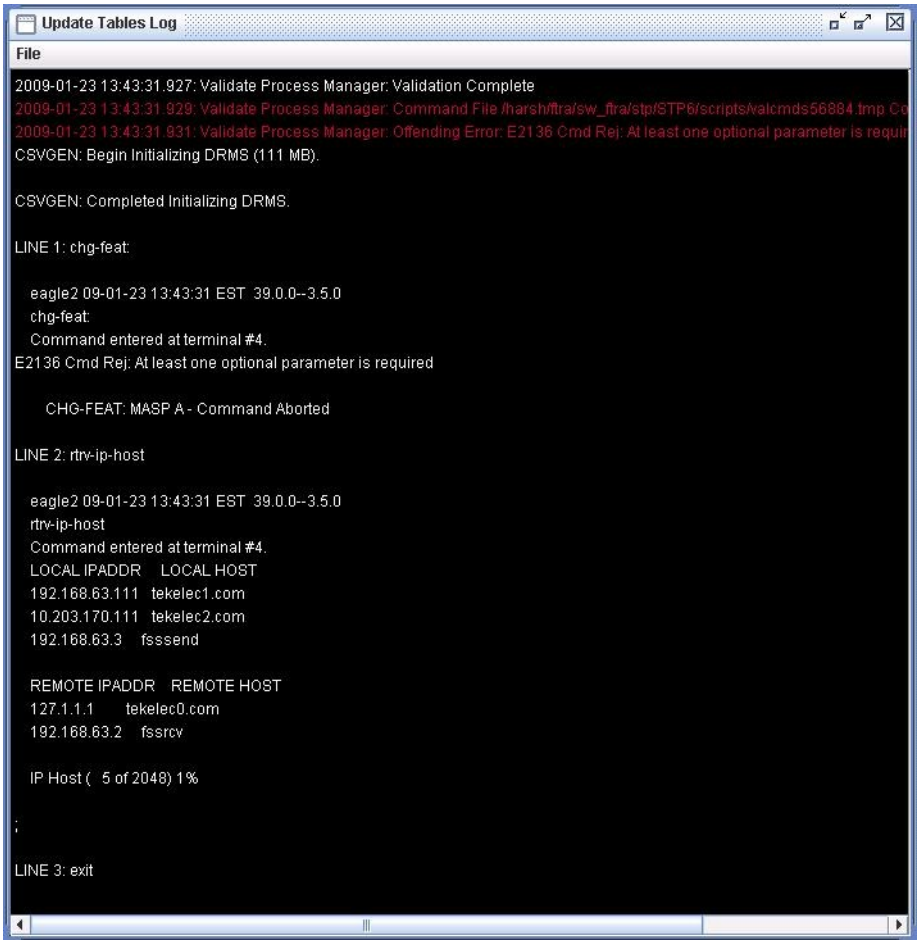
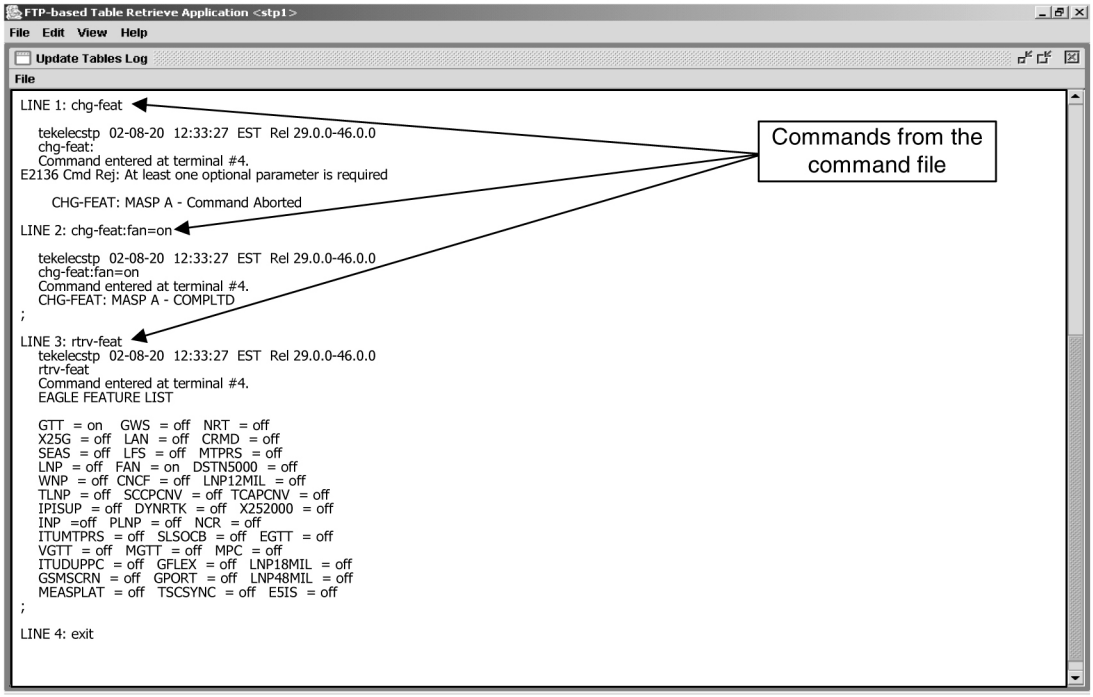


Figure 85: Command File Editor with Invalid Command on page 72 shows an example of a command file that produced the error shown in *Figure 91: Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window* on page 76.

Figure 91: Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window


Update Tables Log
File
2009-01-23 13:43:31.927: Validate Process Manager: Validation Complete
2009-01-23 13:43:31.929: Validate Process Manager: Command File /harsh/ftra/sw_ftra/stp/STP6/scripts/valcmds56884.tmp Co
2009-01-23 13:43:31.931: Validate Process Manager: Offending Error: E2136 Cmd Rej: At least one optional parameter is requir
CSVGEN: Begin Initializing DRMS (111 MB).
CSVGEN: Completed Initializing DRMS.
LINE 1: chg-feat:
eagle2 09-01-23 13:43:31 EST 39.0.0--3.5.0
chg-feat:
Command entered at terminal #4.
E2136 Cmd Rej: At least one optional parameter is required
CHG-FEAT: MASP A - Command Aborted
LINE 2: rtrv-ip-host
eagle2 09-01-23 13:43:31 EST 39.0.0--3.5.0
rtrv-ip-host
Command entered at terminal #4.
LOCAL IPADDR LOCAL HOST
192.168.63.111 tekelec1.com
10.203.170.111 tekelec2.com
192.168.63.3 fsssend
REMOTE IPADDR REMOTE HOST
127.1.1.1 tekelec0.com
192.168.63.2 fssrcv
IP Host (5 of 2048) 1%
;
LINE 3: exit

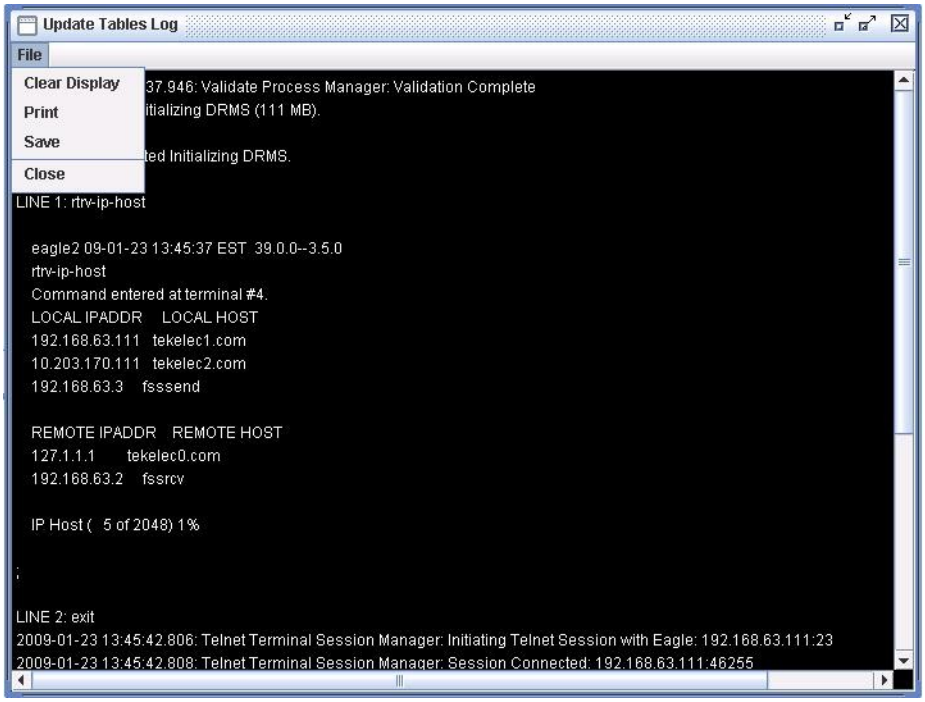

FTP-based Table Retrieve Application <stp1>
File Edit View Help
Update Tables Log
File
LINE 1: chg-feat
tekelecstp 02-08-20 12:33:27 EST Rel 29.0.0-46.0.0
chg-feat:
Command entered at terminal #4.
E2136 Cmd Rej: At least one optional parameter is required
CHG-FEAT: MASP A - Command Aborted
LINE 2: chg-feat:fan=on
tekelecstp 02-08-20 12:33:27 EST Rel 29.0.0-46.0.0
chg-feat:fan=on
Command entered at terminal #4.
CHG-FEAT: MASP A - COMPLTD
;
LINE 3: rtrv-feat
tekelecstp 02-08-20 12:33:27 EST Rel 29.0.0-46.0.0
rtrv-feat
Command entered at terminal #4.
EAGLE FEATURE LIST
GTT = on GWS = off NRT = off
X25G = off LAN = off CRMD = off
SEAS = off LFS = off MTPRS = off
LNP = off FAN = on DSTN5000 = off
WNP = off CNCF = off LNP12MIL = off
TLNP = off SCCPCNV = off TCAPCNV = off
IPISUP = off DYNRTK = off X252000 = off
INP =off PLNP = off NCR = off
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 TSCSYNC = off E5IS = off
;
LINE 4: exit
Commands from the command file

File Menu in the Update Tables Log Window

The **File** menu in the **Update Tables Log** window, shown in *Figure 92: File Menu in the Update Tables Log Window* on page 78, 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 92: 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 saved to a file or printed before the display is cleared.

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

1. Select **File > Clear Display** in the **Update Tables Log** window.
2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window.

   See *Figure 93: View Menu* on page 78. The **Update Tables Log** window opens.

   Figure 93: View Menu

3. Select **File > Clear Display** in the **Update Tables Log** window.

   The Update Tables Log display clears.

Printing the Update Tables Log

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

1. Select **File > Print** from the **Update Tables Log** window.

   See *Figure 92: File Menu in the Update Tables Log Window* on page 78.

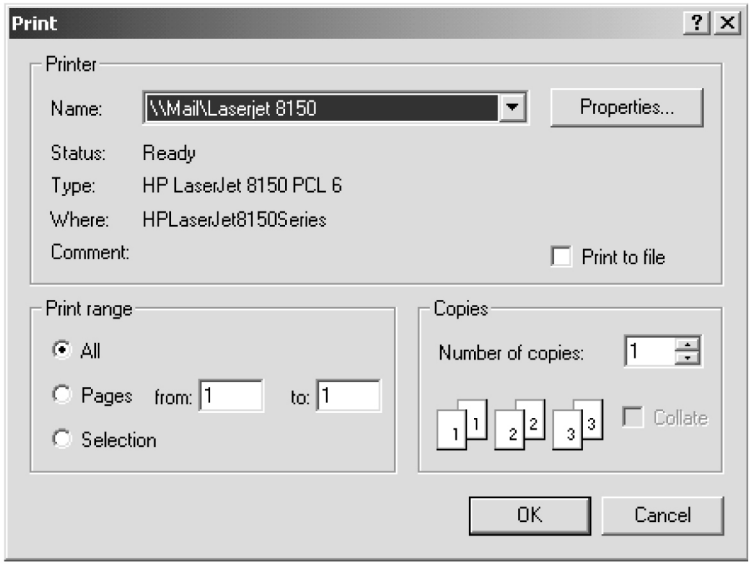
2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window.

   See *Figure 93: View Menu* on page 78. The Update Tables Log opens.

3. Select **File > Print** from the **Update Tables Log** window.

   The **Print** window opens. See *Figure 94: Print Window* on page 79.

   Figure 94: 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

Note:

Perform either step 1 or steps 2 and 3.

1. Select **File > Save** from the **Update Tables Log** window.

   See *Figure 89: Update Tables Log* on page 75.

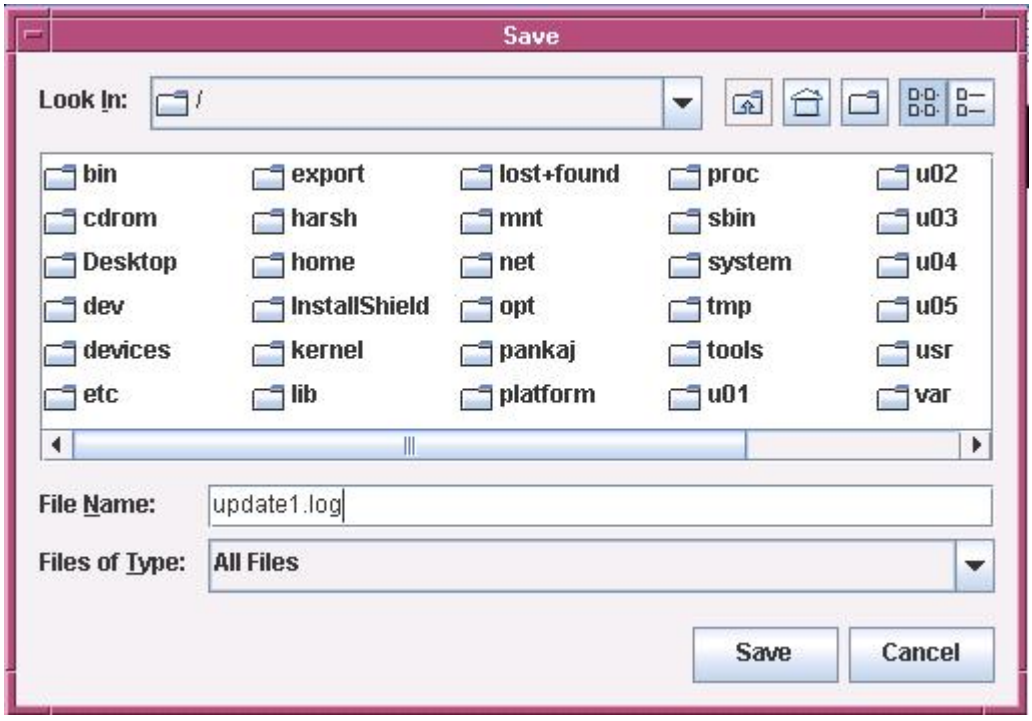
2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window.

   See *Figure 99: View Menu* on page 82. The Update Tables Log opens.

3. Select **File > Save** in the **Update Tables Log** window.

   The **Save** window opens. See *Figure 95: Save Window* on page 80.

   Figure 95: 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 96: Saved Confirmation Window* on page 81. Click **OK** , to continue.

   Figure 96: 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

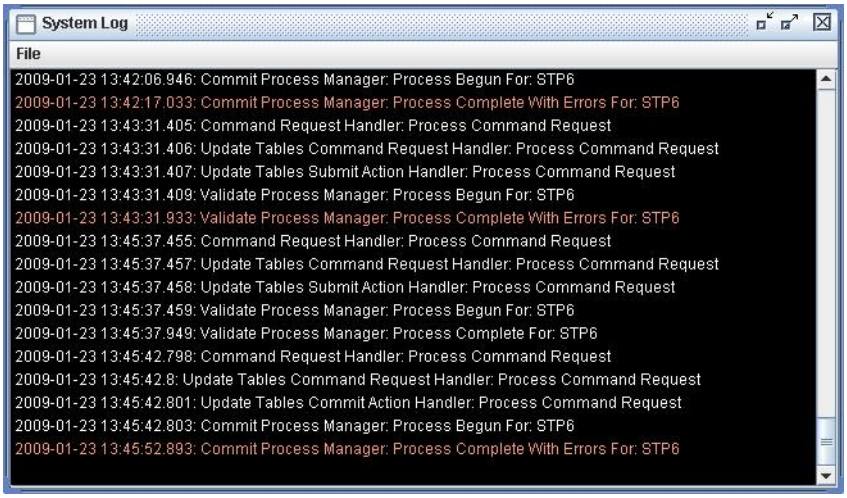
Select **File > Close** in the **Update Tables Log** window, or click the close window button in the upper right hand corner of the **Update Tables Log** window.

See *Figure 89: Update Tables Log* on page 75. 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 97: System Log Window* on page 81.

Figure 97: System Log Window

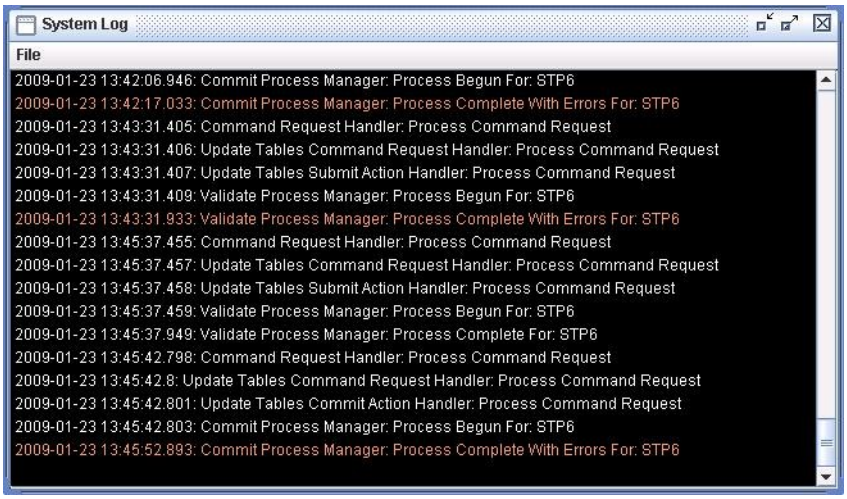


File Menu in the System Log Window

The **File** menu in the **System Log** window, shown in *File Menu in the System Log Window* on page 82, 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 98: 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.

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window.

   See *Figure 99: View Menu* on page 82. The **System Log** window opens.

   Figure 99: View Menu

2. Select **File > Clear Display** in the **System Log** window.

   See *File Menu in the System Log Window* on page 82. The System Log display clears.

Printing the System Log

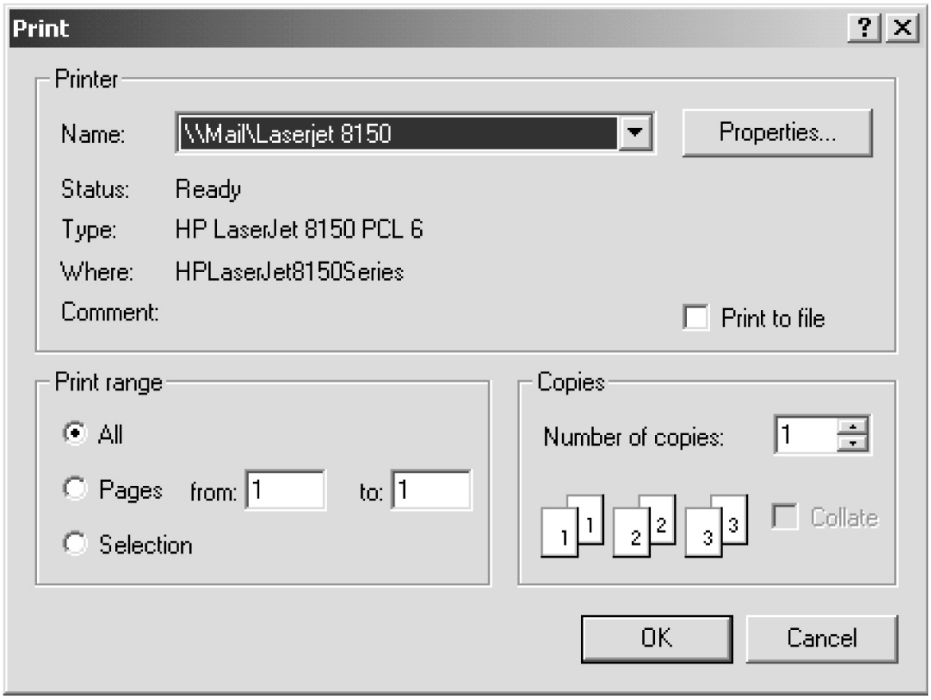
1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window.

   See *Figure 97: System Log Window* on page 81. The **System Log** window opens.

2. Select **File > Print** in the **System Log** window.

   The **Print** window opens. See *Figure 100: Print Window* on page 83.

   Figure 100: 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

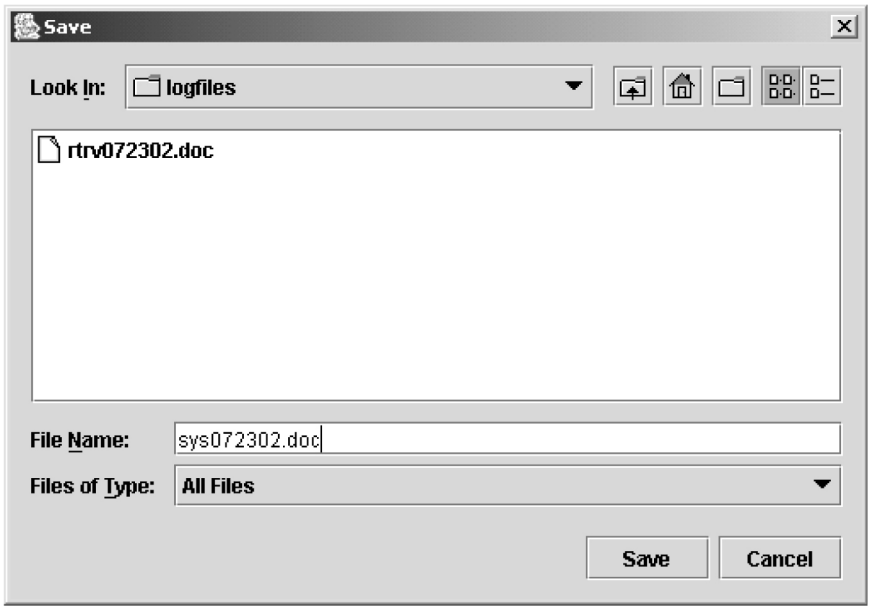
1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window.

   See *Figure 97: System Log Window* on page 81. The System Log opens.

2. Select **File > Save** in the **System Log** window.

   The **Save** window opens. See *Figure 101: Save Window* on page 83.

   Figure 101: Save Window



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

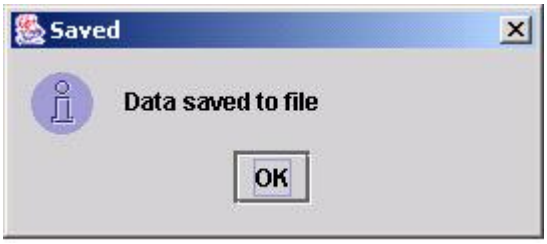
   Note:

   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 102: Saved Confirmation Window* on page 84. Click **OK** to continue.

   Figure 102: 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

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.

Figure 103: Help Menu

The **About FTRA** window opens. Click **OK** to continue.

Figure 104: Typical About FTRA Window

FTRA release 4.2

The following enhancements have been included in FTRA Release 4.2.

- A new IP group has been added to support new RTRV commands.
  - CSVGEN support for the following RTRV commands has been added under this new group:
    - RTRV-IP-LNK
    - RTRV-IP-HOST
    - RTRV-IP-CARD
    - RTRV-ASSOC

- RTRV-APPL-RTKEY
- RTRV-NA
- RTRV-IP-RTE

- CSVGEN support for the following RTRV commands has been added under the MTP group:
  - RTRV-AS
  - RTRV-IPNODE
  - RTRV-SCCPOPTS
  - RTRV-SS-APPL
  - RTRV-MEASOPTS
- CSVGEN support for the RTRV command RTRV-MEASOPTS has been added under the GTT group:
- CSVGEN support for the following RTRV commands has been added under the VFLEX group:
  - RTRV-VFLX-RN
  - RTRV-VFLX-VMSID
  - RTRV-VFLX-CD
  - RTRV-VFLX-OPTS
- The RTRV-ATINPQOPTS command has been added under the MTP group.

- The FTRA (UNIX version) has been rebaselined to work with Solaris 10.

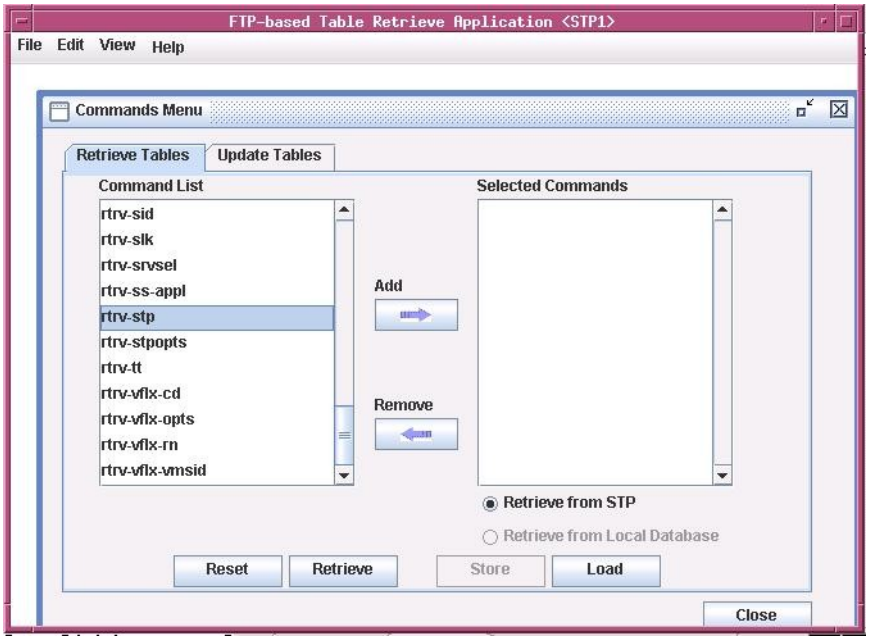
RTRV-STP Command

The rtrv-stp command is added to the list of rtrv commands supported on FTRA. The rtrv-stp command provides a consolidated report of STP configuration on a system-wide basis.

Note: The rtrv-stp functionality is supported on Eagle Release 35.0 or later.

Retrieve Tables

Figure 105: Retrieve Tables window with rtrv-stp command selected for retrieval



RTRV-STP Command Retrieval Session

The FTRA retrieval session when `rtrv-stp` command is supported on EAGLE is shown in *Successful Retrieval Session for rtrv-stp Command* on page 88. If the command is not supported on EAGLE, an error will be displayed and the retrieval session will be terminated (refer "STP data modified through CLI").

Retrieve Tables

Figure 106: Successful Retrieval Session for rtrv-stp command

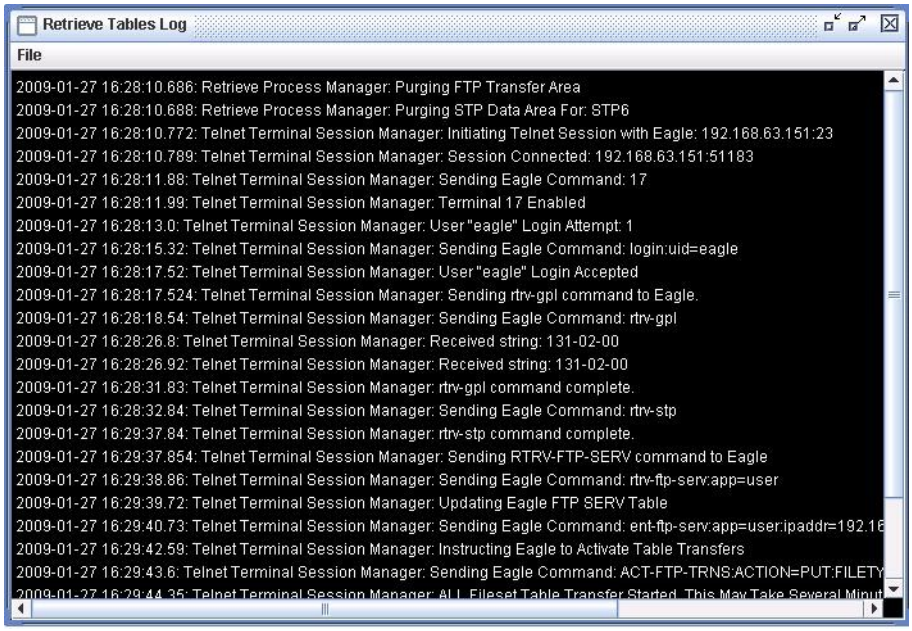
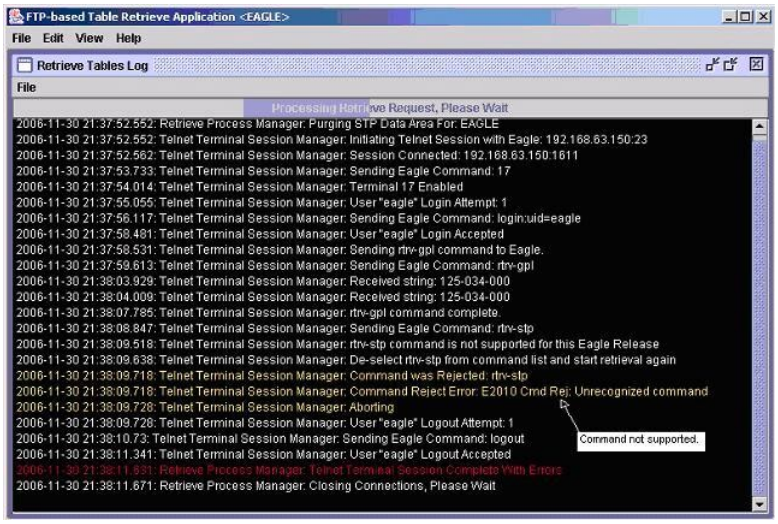


Figure 107: Rtrv-stp Command unsupported on EAGLE release



Version Information

FTRA Release 4.2 displays an "About FTRA" window. Figure 149 shows the new FTRA Version string and updated copyright information.

Figure 108: About FTRA Display Window

SSH/SFTP Error Codes

Table 11: FTP/SFTP/SSH Error Codes on page 89 and *Table 12: Generic Network Error Codes* on page 101 contain a list of the error codes that can be generated when making a secure connection between the FTRA, version 4.0 or greater, and the EAGLE 5 ISS. Each error code contains a brief description of the error and the suggested recovery action.

This section also contains procedures, following *Table 11: FTP/SFTP/SSH Error Codes* on page 89 and *Table 12: Generic Network Error Codes* on page 101, 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 ISS 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 ISS before performing any of the actions in *Table 11: FTP/SFTP/SSH Error Codes* on page 89 and *Table 12: Generic Network Error Codes* on page 101. 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 11: FTP/SFTP/SSH Error Codes* on page 89 or *Table 12: Generic Network Error Codes* on page 101 are encountered after the recovery procedure is verified, contact the *Customer Care Center* on page 4.

Table 11: 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 34: FTP Server Configuration Menu Window* on page 37).

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
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* on page 105 and the *Connectivity Test - II* on page 106). If the IP address exists on network then verify that SSHD daemon is running on the destination machine using the `ps -ef|grep sshd` command.
629	The SFTP daemon is not running	Verify that the subsystem entry in the `sshd_config` file on the destination station is specified and points to the SFTP daemon.
633	User login failure.	Verify that the Username and Password in the **STP Connection Configuration Menu** window, (see *Table 3: STP Connection Configuration Menu Description* on page 14) 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* on page 4 immediately.
596	The file name is already specified.	Report this issue to the *Customer Care Center* on page 4immediately. (Internal SFTP implementation error).
SFTP Client Errors		
597	SFTP client packet send failure	Perform these tests: • *FTP Server Verification* on page 104
598	The SFTP connection is closed.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
599	SFTP packet read failure	• *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
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* on page 106. If the error persists, report the issue to the *Customer Care Center* on page 4.
601	Undefined	Notify the *Customer Care Center* on page 4.
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* on page 106. If the error persists, report the issue to the *Customer Care Center* on page 4.
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.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
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* on page 106.
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 34: FTP Server Configuration Menu Window* on page 37) 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* on page 106.
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.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
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* on page 4 immediately.
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* on page 4 immediately.
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* on page 4 immediately.
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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105
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.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
		• *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
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 ISS is compatible with **openSSH 3.0.2p1**.	Report the issue to the *Customer Care Center* on page 4 if the problem persists after the SSHD configuration file is verified.
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* on page 4.
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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106
640	A bad message was received during the SSH authentication.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
		Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
641	Missing authentication context, encountered during the SSH user authorization.	Report this issue to the *Customer Care Center* on page 4 immediately.
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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
645	A bad option was specified in the SSH client on the EAGLE 5 ISS.	
646	An unsupported escape character was used in the SSH client on the EAGLE 5 ISS.	
647	An unsupported cipher type was used in the SSH client on the EAGLE 5 ISS.	Report this issue to the *Customer Care Center* on page 4 immediately.

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 ISS.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
649	A bad port was used in the SSH client on the EAGLE 5 ISS.	Report this issue to the *Customer Care Center* on page 4 immediately.
656	Bad forwarding was used in the SSH client on the EAGLE 5 ISS.	
657	Bad forwarding ports were specified in the SSH client on the EAGLE 5 ISS.	
658	A bad dynamic port was specified in the SSH client on the EAGLE 5 ISS.	
659	The host was not specified in the SSH client on the EAGLE 5 ISS.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests:

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
		• *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
660	An invalid option or argument was specified in the SSH client on the EAGLE 5 ISS.	Report this issue to the *Customer Care Center* on page 4 immediately.
661	The hostname was not specified in the SSH client on the EAGLE 5 ISS.	
663	The SSH client was unable to load the cipher type on the EAGLE 5 ISS.	
664	Asynchronous IO is not supported on IPSM, SSH client error.	
665	Compression is already enabled in the SSH client on the EAGLE 5 ISS.	
666	Unknown cipher number on the SSH client on the EAGLE 5 ISS.	
667	The SSH client key length is invalid.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
668	No key is available on the SSH client on the EAGLE 5 ISS.	Report this issue to the *Customer Care Center* on page 4 immediately.
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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
670	Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network.	
671	An unexpected packet type was received from the SFTP/SSHD server.	
672	A bad packet length was received from the SSHD/SFTP server.	
673	A cryptographic attack was detected by the SSH client. Please notify the local system administrator.	Report the issue to the *Customer Care Center* on page 4. This is not a software problem but there is a security threat. The keys/authentication may have to be updated immediately.
674	The SSH/SFTP client on the EAGLE 5 ISS 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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105
675	Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 ISS.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
		• *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
676	Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 ISS.	Verify that the `sshtools.xml` file provided with FTRA software has the field as shown: <!-- The Message Authentication Code configuration, add or override default mac implementations --> <MacConfiguration> <DefaultAlgorithm>hmac-md5</DefaultAlgorithm> </MacConfiguration>
677	Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 ISS.	Report this issue to the *Customer Care Center* on page 4 immediately.
678	SSH/SFTP tried to close a connection that is already closed.	
679	The SSH/SFTP client on the EAGLE 5 ISS failed to write to 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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
		• *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
680	SSH/SFTP tried to set the packet size twice.	Report this issue to the *Customer Care Center* on page 4 immediately.
681	A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 ISS.	
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: • *FTP Server Verification* on page 104 • *SFTP /SSHD Server Verification* on page 105 • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
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.	

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
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 12: 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 ISS using the `rtrv-ftp-serv` command, and re-try the connection
41	Protocol wrong type for socket	Report this issue to the *Customer Care Center* on page 4.
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.	

SFTP/SSH/Generic Network Client Error Code	Description	Action/Recovery
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: • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
52	The network dropped the connection on reset.	
53	Software caused the connection to abort.	Report this issue to the *Customer Care Center* on page 4.
54	The connection was reset by the peer.	Verify that the connection tests pass and network outage numbers are within the allowed limits as shown in these sections: • *Connectivity Test – I* on page 105

SFTP/SSH/Generic Network Client Error Code	Description	Action/Recovery
		• *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
55	No buffer space available.	Report this issue to the *Customer Care Center* on page 4.
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.	Perform these tests and verify that the FTP server address responds to the ping command from the ISPM. • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106
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* on page 104test.
62	The network is down.	Verify that the connection tests pass and network outage numbers are within the allowed
65	There is no route to the host.	

SFTP/SSH/Generic Network Client Error Code	Description	Action/Recovery
67	The host is down.	limits as shown in these sections: • *Connectivity Test – I* on page 105 • *Connectivity Test - II* on page 106 • *Network Outage Trouble Shooting* on page 106 Make any fixes necessary and retry the connection. If the problem persists, report the issue to the *Customer Care Center* on page 4.
30	Read-only file system	
32	Broken pipe	Report the issue to the *Customer Care Center* on page 4.
35	Unsupported value	

Troubleshooting Procedures

FTP Server Verification

Component: The FTP server IP address shown in the **FTP Server Configuration Menu** window (see *Figure 34: FTP Server Configuration Menu Window* on page 37).

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 34: FTP Server Configuration Menu Window* on page 37).

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 34: FTP Server Configuration Menu Window* on page 37).

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 in 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 ISS and the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see *STP Connection Configuration Menu* on page 12).

On an EAGLE 5 ISS 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 *STP Connection Configuration Menu* on page 12), and `yy.yy.yy.yy` is the IP address of the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see *Figure 34: FTP Server Configuration Menu Window* on page 37).

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 ISS and FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see *Figure 34: FTP Server Configuration Menu Window* on page 37).

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 ISS shown in the **STP Connection Configuration Menu** window (see *STP Connection Configuration Menu* on page 12).

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 ISS, enter the `pass:loc=xxxx:cmd="netstat -p tcp"` command at the EAGLE 5 ISS terminal, where `xxxx` is location of the IPSM associated with the IP address entered in the **STP Connection Configuration Menu** window, (see *STP Connection Configuration Menu* on page 12), 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 unsent 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
        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 13: TCP Fault Tolerance Table for FTP/SFTP* on page 108, fix the network problems and retry the connection.

Table 13: 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.

Glossary

C

CSV

Comma-separated value

The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

daemon

A process that runs in the background (rather than under the direct control of a user) and performs a specified operation at predefined times or in response to certain events. Generally speaking, daemons are assigned names that end with the letter "d." For example, sentryd is the daemon that runs the Sentry utility.

Database

All data that can be administered by the user, including cards, destination point codes, gateway screening tables, global title translation tables, links, LNP services, LNP service providers, location routing numbers, routes, shelves, subsystem applications, and 10 digit telephone numbers.

E

EGTT

Enhanced Global Title Translation

A feature that is designed for the signaling connection control part (SCCP) of the SS7 protocol. The EAGLE 5 ISS uses this feature to determine to which service database to send the query

E

message when a Message Signaling Unit (MSU) enters the system.

F

FTP	File Transfer Protocol A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.
FTRA	FTP-based Table Retrieve Application An application that runs in a PC outside of the EAGLE 5 ISS and that communicates with the EAGLE 5 ISS through the IPUI feature and the FTP Retrieve and Replace feature.

G

GTT	Global Title Translation A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE 5 ISS uses to determine which service database to send the query message when an MSU enters the EAGLE 5 ISS and more information is needed to route the MSU. These service databases also verify calling card numbers and credit card numbers. The service databases are identified in the SS7 network by a point code and a subsystem number.

I

ID	Identity, identifier
IETF	Internet Engineering Task Force

I

IM	Instant Messaging A protocol for realtime communication using text messages over the Internet which was standardized via the IEFT and based on TCP or SIP.
IP	Internet Protocol IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
IP Address	The location of a device on a TCP/IP network. The IP Address is a number in dotted decimal notation which looks something like [192.168.1.1].
IPSM	IP Services Module A card that provides an IP connection for Telnet and FTP-based Table Retrieve applications. The IPSM is a GPSM-II card with a one Gigabyte (UD1G) expansion memory board in a single-slot assembly running the IPS application.
ISS	Integrated Signaling System

M

MAC	Media Access Control Address

M

The unique serial number burned into the Ethernet adapter that identifies that network card from all others.

MAN — Metropolitan Area Network

O

OA — Onboard Administrator

The management processor for an HP c-Class enclosure.

P

PC — Point Code

The identifier of a signaling point or service control point in a network. The format of the point code can be one of the following types:

- ANSI point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Non-ANSI domestic point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Cluster point codes in the format network indicator-network cluster-* or network indicator-*-*.
- ITU international point codes in the format **zone-area-id**.
- ITU national point codes in the format of a 5-digit number (**nnnnn**), or 2, 3, or 4 numbers (members) separated by dashes (**m1-m2-m3-m4**) as defined by the Flexible Point Code system option. A group code is required (**m1-m2-m3-m4-gc**)

P

when the ITUDUPPC feature is turned on.

- 24-bit ITU national point codes in the format main signaling area-subsignaling area-service point (**msa-ssa-sp**).

The EAGLE 5 ISS LNP uses only the ANSI point codes and Non-ANSI domestic point codes.

R

RFC	Request for Comment RFCs are standards-track documents, which are official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group the IESG.
RTT	Round Trip Time

S

SFTP	SSH File Transfer Protocol (sometimes also called Secure File Transfer Protocol) A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network over any reliable data stream. It is typically used over typically used with version two of the SSH protocol.
SSH	Secure Shell A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate

S

	eavesdropping, connection hijacking, and other network-level attacks.
STP	Signal Transfer Point STPs are ultra-reliable, high speed packet switches at the heart of SS7 networks, which terminate all link types except F-links. STPs are nearly always deployed in mated pairs for reliability reasons. Their primary functions are to provide access to SS7 networks and to provide routing of signaling messages within and among signaling networks.

T

TCP	Transfer Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

U

UIM	Unsolicited Information Message

Index

.doc file extension 27, 58, 80, 84

30 - Read-only file system 104
32 - Broken pipe 104
35 - Unsupported value 104
40 - A destination address is required 101
41 - Protocol wrong type for socket 101
42 - The protocol is not available 101
43 - The protocol is not supported 101
44 - The socket type is not supported 101
45 - The operation is not supported on the socket 101
46 - The protocol family is not supported 102
47 - The address family is not supported 102
48 - The address is already in use 102
49 - The requested address cannot be assigned 102
50 - Socket operation on non-socket 102
51 - The network is unreachable 102
52 - The network dropped the connection on reset 102
53 - Software caused the connection to abort 102
54 - The connection was reset by the peer 102
55 - No buffer space available 103
56 - The socket is already connected 103
569 - The file name is already specified 90
57 - The socket is not connected 103
58 - Can't send after socket shutdown 103
59 - Too many references\
can't splice 103
595 - File open failed 90
597 - SFTP client packet send failure 90
598 - The SFTP connection is closed 90
599 - SFTP packet read failure 91
60 - The connection timed out 103
600 - SFTP protocol error 91
601 - Undefined 91
608 - SFTP received a invalid ID in the response received during a read operation on remote directory 91
609 - SFTP\
Handle mismatch error 91
61 - The connection was refused 103
610 - Unexpected SSH2_FXP_ATTRS 91
611 - Unexpected SSH_FXP_NAME 92
612 - SSH_FXP_REALPATH request failure 92
613 - SSH_FXP_READLINK request failure 92
614 - unexpected SSH_FXP_NAME 92
615 - The SFTP client received more data than expected 93
616 - The SFTP client failed to read the data from the file descriptor 93
617 - Excessive identity files 93
62 - The network is down 103
624 - The debug levels allowed for SSH protocol in openSSH is 0-9 93
625 - Failure to read the client configuration file 93
626 - Invalid compression level is specified in the client configuration file 93
627 - SSH failure to setup the IO with the server 93
628 - SSH failure to open the channel for the SSH connection with the server 93
629 - SSH failure to setup the channel for the SSH connection with the server 93
630 - SSH failure to verify the SSH client host key 93
631 - SSH user authentication failure 94
632 - The authentication method is NULL in the client software 94
633 - Permission is denied by the server due to authentication failure 94
633 - User login failure 90
640 - A bad message was received during the SSH authentication 94
641 - Missing authentication context, encountered during the SSH user authorization 95
642 - Failure during the public key read/verification operation 95
643 - Undefined SFTP/SSH error 95
644 - Unexpected SSH_FXP_STATUS error 95
645 - A bad option was specified in the SSH client on the EAGLE 5 ISS 95
646 - An unsupported escape character was used in the SSH client on the EAGLE 5 ISS 95
647 - An unsupported cipher type was used in the SSH client on the EAGLE 5 ISS 95
648 - An unsupported MAC type was used in the SSH client on the EAGLE 5 ISS 96
649 - A bad port was used in the SSH client on the EAGLE 5 ISS 96
65 - There is no route to the host 103
656 - Bad forwarding was used in the SSH client on the EAGLE 5 ISS 96
657 - Bad forwarding ports were specified in the SSH client on the EAGLE 5 ISS 96
658 - A bad dynamic port was specified in the SSH client on the EAGLE 5 ISS 96
660 - An invalid option or argument was specified in the SSH client on the EAGLE 5 ISS 97
661 - The hostname was not specified in the SSH client on the EAGLE 5 ISS 97
663 - The SSH client was unable to load the cipher type on the EAGLE 5 ISS 97
664 - Asynchronous IO is not supported on IPSM, SSH client error 97

665 - Compression is already enabled in the SSH client on the EAGLE 5 ISS 97
666 - Unknown cipher number on the SSH client on the EAGLE 5 ISS 97
667 - The SSH client key length is invalid 97
668 - No key is available on the SSH client on the EAGLE 5 ISS 98
669 - The secure connection was closed by the remote server 98
67 - The host is down 104
670 - Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network 98
671 - An unexpected packet type was received from the SFTP/SSHD server 98
672 - A bad packet length was received from the SSHD/SFTP server 98
673 - A cryptographic attack was detected by the SSH client 98
674 - The SSH/SFTP client on the EAGLE 5 ISS failed to read from the remote side 98
675 - Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 ISS 98
676 - Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 ISS 99
677 - Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 ISS 99
678 - SSH/SFTP tried to close a connection that is already closed 99
679 - The SSH/SFTP client on the EAGLE 5 ISS failed to write to the remote side 99
680 - SSH/SFTP tried to set the packet size twice 100
681 - A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 ISS 100
682 - The connection timed out when SSH tried to connect to SSHD 100
683 - The SSH connection was refused by the remote server 100
684 - The SSHD server is unreachable 100
685 - The network has reset 100
686 - The SSH/SFTP connection has been aborted 100
687 - The SFTP/SSH connection has been reset by the peer 100
688 - Failed to allocate network buffers 100
689 - The SSH/SFTP socket is already connected 101
690 - The SSH/SFTP socket is not connected 101
691 - The network channel is down 101
692 - The SSHD/SFTP server connection host is down 101
693 - SFTP client channel read failure 101
694 - SFTP client channel write failure 101
695 - SFTP client channel open failure 101

A

Activating the Eagle OA&M IP Security Enhancements Controlled Feature procedure 16, 20, 89
Add button 2, 15, 17, 20, 43, 47
    Retrieve Tables 43
Adding
    STP Configuration Record 36
admonishments, documentation 3
alw-card command 32
availability, documentation 3

B

Box
    Command List 42, 43, 44, 45, 49
    Selected Commands 42, 43, 44, 47, 49, 51
Browse button
    FTP Server Configuration Menu 38, 39
    Update Tables 66
Button 42, 43, 44, 47, 49, 50, 51, 68
    Add 43, 47
    Load 44, 51
    Remove 43, 49
    Reset 44, 49
    Retrieve 42, 44, 51
    Retrieve from Local Database 42, 44, 51
    Retrieve from STP 42, 44, 51
    Store 44, 50

C

Cancel
    Select window 68
Cancel button 26, 40, 57, 58, 67, 68, 80, 81, 83, 84
    Select Starting Directory window 40
    Select window 67, 68
CAUTION admonishment 3
chg-trm command 34
chmod command 38, 39
Clearing
    Retrieve Tables Log 55
Clearing the display
    Retrieve Tables Log 55
Clearing the Display 78, 82
Close
    Retrieve Tables 44
Close button
    FTP Connection Configuration Menu 39
    Retrieve Tables window 44
    STP Connection Configuration Menu 15
    Update Tables 66
Closing 25, 55, 78, 82
    Connectivity Test Log window 25
    Retrieve Tables Log window 55
    Update Tables Log window 78
cmd= 105, 106
Command 42, 44, 47, 52
Command Complete 42, 52, 70, 71, 73
    Retrieve Tables window 42, 52
    Update Tables window 71, 73

Command File
Editing 2
Editor window 70, 71, 72, 73, 74
Field, Update Tables window 66, 67, 68, 69
Command In progress, Cannot Close Window message 72
Command Line Interface 2, 44, 50, 51, 59
Command List 42, 43, 44, 45, 49, 65
Box 42, 43, 44, 45, 49
Retrieve Tables 43
Side 49
Commands 42, 44, 47, 50, 52, 66
Menu window 44, 50, 66
Commit button, Update Validation Complete window 70, 71
Configuration record, STP 32
Connectivity Test Log 23, 25, 26, 28, 33, 36
Clearing the Display 25
window 23, 25, 26, 28, 33, 36
Connectivity Test Log window 25
cron 59, 62, 63
CSR, See Customer Service Request (CSR)
CSV file format 2, 42, 44, 51, 59, 63
Current STP 30, 31
Selected 31
Customer Care Center
contact information 4
emergency response 6
Customer Service Request (CSR) 4

D

DANGER admonishment 3
Database Administration Manual - System Management 16, 20
Delete button 15
Display 55
documentation 2, 3
availability, packaging, and updates 3
Documentation Bulletins 3
electronic files 3
printed 3
Related Publications 2
Release Notice 3
DOS command prompt 59
DSA Key Fingerprint 35
Duplicate packets 107

E

EAGLE 5 ISS 35, 42, 44, 47, 52, 59
rtrv 44, 59
rtrv-feat 42
rtrv-gta 42, 47, 52
rtrv-gtt 42, 47, 52
rtrv-gttsel 42, 47, 52
rtrv-gttset 42, 47, 52
EAGLE 5 ISS *(continued)*
rtrv-trm 52
rtrv-tt 42, 47, 52
Telnet 52
Telnet terminals 52
UIM - Unsolicited Information Message 35, 52
EAGLE 5 ISS chg-ftp-serv command 38
EAGLE 5 ISS chg-trm\
trm= 52
EAGLE 5 ISS command
rtrv 44
rtrv-ctrl-feat 89
rtrv-feat 42
rtrv-gta 42, 47, 52
rtrv-gtt 42, 47, 52
rtrv-gttsel 42, 47, 52
rtrv-gttset 42, 47, 52
rtrv-trm 52
rtrv-tt 42, 47, 52
EAGLE 5 ISS commands 2, 65, 66
EAGLE 5 ISS EGTT commands
rtrv-gta 42, 47, 52
rtrv-gttsel 42, 47, 52
rtrv-gttset 42, 47, 52
EAGLE 5 ISS ent-ftp-serv command 38
EAGLE 5 ISS feature 89
Eagle OA&M IP Security Enhancements 89
EAGLE 5 ISS Feature
EGTT 42
GTT 42
EAGLE 5 ISS GTT commands
rtrv-gtt 42, 47, 52
rtrv-tt 42, 47, 52
EAGLE 5 ISS Manual, Database Administration Manual - System Management 89
EAGLE 5 ISS pass\ 105, 106
EAGLE 5 ISS Public Host Key Fingerprint 32, 35, 36
EAGLE 5 ISS Public Key Fingerprint 16, 35
EAGLE 5 ISS release 30.2 or greater 20
EAGLE 5 ISS rtrv-ctrl-feat command 16, 20
EAGLE 5 ISS rtrv-feat command 42
EAGLE 5 ISS rtrv-ftp-serv command 101
EAGLE 5 ISS rtrv-gta command 42, 47, 52
EAGLE 5 ISS rtrv-gtt command 42, 47, 52
EAGLE 5 ISS rtrv-gttsel command 42, 47, 52
EAGLE 5 ISS rtrv-gttset command 42, 47, 52
EAGLE 5 ISS rtrv-secu-dflt command 19
EAGLE 5 ISS rtrv-stp command 53
EAGLE 5 ISS rtrv-trm command 52
EAGLE 5 ISS rtrv-tt command 42, 47, 52
Eagle OA&M IP Security Enhancements 89
Eagle OA&M IP Security Enhancements feature 15, 16, 20
Edit button, Update Validation Complete window 70, 71, 72
EGTT
rtrv-gta 42, 47, 52

EGTT *(continued)*
rtrv-gttsel 42, 47, 52
rtrv-gttset 42, 47, 52
EGTT commands 42, 47, 52
EGTT Feature 42
electronic files, documentation 3
emergency response, Customer Care Center 6
Error code 96, 104
659 - The host was not specified in the SSH client on the EAGLE 5 ISS 96
Exit Confirmation window 11
Exit window 11

F

Feature
EGTT 42
GTT 42
Field 43
Retrieve Tables window 43
Selected Commands, Retrieve Tables 43
File
Retrieve Tables Log window 55
File format
CSV 42, 44, 51
File menu 11, 55, 82
FTP-Based Table Retrieve Application window 11
Retrieve Tables Log 55
File Name\ 40, 67, 68
Files of type\ 40, 67
FTP Password Field 14, 19
FTP server 37, 104
FTP Server Configuration 2, 19, 37, 39, 89, 92, 104, 105
Menu 37
Menu window 19, 37, 39, 89, 92, 104, 105
FTP Server Data Set window 41
FTP UserName Field 14, 19
FTP-Based Table Retrieve Application 11, 16, 23, 37, 45, 56, 57, 66, 78, 79, 80, 82, 83
Edit Menu 37
window 11, 23, 45, 56, 57, 66, 78, 79, 80, 82, 83
FTRA 59, 63
ftra -c command 59, 63
ftra file 33
FTRA window 42, 43, 45, 59, 65, 73
Retrieve Tables 42, 43, 45
Update Tables 73
FTRA_HOME environment variable 3
ftra.bat 33

G

GTT
rtrv-gtt 42, 47, 52
rtrv-tt 42, 47, 52
GTT commands 42, 47, 52
GTT Feature 42

H

hexadecimal 35
hosts.xml 32, 33, 34, 35, 36

I

init-card command 32, 35
Invalid FTP Password warning window 19
Invalid FTP User Name warning window 19
Invalid IP Address warning window 39
Invalid STP Name warning window 17
Invalid STP Password warning window 18
Invalid STP User Name warning window 18
IP Address 15, 37, 104, 105
IP Address Field 38, 39
IPSM 32, 33, 34, 35, 105, 106
IPSM IP Address 34, 35

J

JRE_HOME environment variable 3

L

Load button 44, 51, 59
loc=xxxx 105, 106
Log 42, 52, 55, 81
Retrieve Tables 42, 52, 55
System 81
Look in\ 40, 67

M

Menu 55
Modify button 15, 28
Modify Warning window 30
Modifying an Existing STP Configuration Record 32, 36

N

netstat -a\|grep 21 104
Network latency 107

O

openSSH 3.0.2p1 91, 92, 93, 94, 95, 96, 98, 99, 100, 105

P

packaging, documentation 3
Packet drop 107
pass\ 105, 106

Path Field 38
path parameter 38
Print window 26, 57, 83
    Connectivity Test Log 26
    Retrieve Tables Log 57
printed documentation 3
Printing
    Retrieve Tables Log 55
    System Log 82
Processing Validate Request, Please Wait message 68, 74
ps 105
ps -ef\|grep sshd 90
ps -f\|grep sshd 105

R

Refresh button 15, 30
Related Publications 2
Release Notice 3
Remove button 43, 49
Reset button 44, 49
Retrieve button 42, 44, 51
Retrieve from Local Database button 42, 44, 51
Retrieve from STP button 42, 44, 51
Retrieve Tables
    Add button 43, 47
    Close button 44
    Command Complete 42, 52
    Command List Box 42, 43, 44, 45, 49
    Command List Field 43
    Load button 44, 51
    Remove button 43, 49
    Reset button 44, 49
    Retrieve button 42, 44, 51
    Retrieve from Local Database button 42, 44, 51
    Retrieve from STP button 42, 44, 51
    Selected Commands Box 42, 43, 44, 47, 49, 51
    Selected Commands Field 43
    Store button 44, 50
    window, File Menu 55
Retrieve Tables Log 42, 52, 53, 55, 57, 58
    Clearing the Display 55
    closing 55
    File Menu 55
    Print window 57
    Printing 55
    Save window 58
    saving to a file 55
Retrieve Tables Log window 51, 53, 55, 56, 57, 58, 59
    File Menu 55
Retrieve Tables window 42, 43, 44, 45, 47, 49, 50, 51
    Add button 43, 47
    Close button 44
    Load button 44, 51
    Remove button 43, 49
    Reset button 44, 49
Retrieve Tables window *(continued)*
    Retrieve button 42, 44, 51
    Retrieve from Local Database button 42, 44, 51
    Retrieve from STP button 42, 44, 51
    Store button 44, 50
Retrieving EAGLE 5 ISS database tables 2
rst-card command 32
rtrv commands 44, 59, 63
rtrv-feat EAGLE 5 ISS command 42
rtrv-gta EAGLE 5 ISS command 42, 47, 52
rtrv-gtt EAGLE 5 ISS command 42, 47, 52
rtrv-gttsel EAGLE 5 ISS command 42, 47, 52
rtrv-gttset EAGLE 5 ISS command 42, 47, 52
rtrv-ip-lnk command 34, 35
rtrv-trm command 33, 34
rtrv-trm EAGLE 5 ISS command 52
rtrv-tt EAGLE 5 ISS command 42, 47, 52

S

Save button 58, 81, 84
    System Log Save window 84
    Update Tables Log Save window 81
Save window 26, 83
    Connectivity Test Log 26
Saved File Confirmation window 27, 58, 81, 84
    Connectivity Test Log 27
    Retrieve Tables Log 58
    Update Tables Log 81
Saving to a file 25, 55, 78, 82
    Connectivity Test Log 25
    Retrieve Tables Log 55
    Update Tables Log 78
secure connection 16, 32
Secure Connection Box - FTRA 2.0 or greater 36
Secure FTP server 37
secure IP connection between FTRA and STP 15, 20
Security Administration 34
Select button 15, 40, 66, 68
    Select Starting Directory window 40
    Select window 66, 68
Select Starting Directory window 38, 39, 40
Select window
    Cancel button 68
    Update Tables 65, 66, 67, 68
Selected Commands
    Box 42, 43, 44, 47, 49, 51
    Field, Retrieve Tables window 43
Selected STP 2, 31, 42, 43, 44, 50, 51, 65, 66, 69, 70, 71, 72, 73, 74
Set button 39, 41
    FTP Server Configuration Menu 39
SFTP Client Errors 90
SFTP Errors 90
SFTP Server 98, 105
Shell command prompt 59
SSH Client Errors 93

SSH Connection Errors 100
SSH, the Secure Shell\
The Definitive Guide 108
SSHD Server 98, 105
sshtools.xml 99
Stop button, Update Validation Complete window 70
Stop on error box
Update Tables window 66, 68
Store button 44, 50, 59
STP Added window 20
STP Configuration Record 12, 14, 15, 17, 23, 28, 30, 31, 32, 36
STP Connection Configuration 2, 12, 13, 15, 16, 17, 20, 23, 30, 31, 37, 90, 105, 106
Database 12, 15, 16, 17, 20
Menu window 12, 13, 15, 16, 23, 90, 105, 106
STP Connection Configuration Menu
IP Address 105, 106
STP Connectivity Test 2
STP Data Modified window 28
STP Name 14, 15, 16, 17, 20, 28, 31
STP Name Field 14, 16, 17
STP Password Field 14, 18, 19
STP Selection Change window 15
STP UserName Field 14, 18
strict host key checking 32, 33
strict host key flag 33
Subpath Field 38
System 82
System Log 81, 82, 83, 84
System Log window 82, 83, 84

T

TAC Regional Support Office 4
TCP Out of Order 107, 108
TCP Packet Delay 107, 108
TCP Packet Error 107
TCP Packet Errors 108
TCP Packet Loss 107, 108
telnet server 32
Telnet terminals 15, 35, 52
Terminals 52
Test button 15, 23
TOPPLE admonishment 3

U

UIM - Unsolicited Information Message
EAGLE 5 ISS 52
Undefined - Error code 601 91
Update Tables
Update Validation Complete with errors 70
Update Tables Log 66, 68, 69, 70, 71, 73, 74, 78, 79, 80, 81
Print window 79
Printing 78
Save window 80, 81
Update Tables Log window 68, 69, 74, 78, 79, 80
Update Tables processing completed without errors message 73
Update Tables window 65, 66, 68, 72
Update Validation Complete window 65, 69, 70, 71, 72
without errors 71
updates, documentation 3
Use STP and FTP UserNames, Passwords for all STPs Box 16, 17, 28

V

Validate button
Update Tables 66, 68, 69
Update Tables window 65
Validating command files 2
Viewing log files 2

W

WARNING admonishment 3
window 82
Window 28, 42, 43, 44, 45, 47, 49, 50, 51, 52, 53, 55, 56, 67
Commands Menu 44, 50
FTP-Based Table Retrieve Application 45, 56
Retrieve Tables 42, 43, 45
Retrieve Tables Log 51, 53, 55, 56
STP Connection Configuration Menu 28
Windows Task Scheduler 59, 63