# Oracle® Communications

# EAGLE FTP Table Base Retrieval User's Guide

Release 5.1
G49481-01
December 2025

ORACLE

Oracle Communications EAGLE FTP Table Base Retrieval User's Guide, Release 5.1

G49481-01

# Contents

## 3 Glossary

# My Oracle Support (MOS)

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support**:
  The generic product related information and resolution of product related queries.
- **Critical Situations**
  A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:
  - 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 Oracle.
- **Training Need**
  Oracle University offers training for service providers and enterprises.

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

# What's New in This Guide

This section introduces the documentation updates for Release 5.1 in Oracle Communications EAGLE FTP Table Based Retrieval (FTRA) User Guide

**Release 5.1 - G49481-01, December 2025**

There is no update for this release in this document.

1

# Overview

The EAGLE FTP Table Base Retrieval (FTRA) was designed in conjunction with the FTP Retrieve and Replace feature to transfer EAGLE 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 selected EAGLE using the EAGLE's retrieve commands. The output of these retrieve commands is converted to CSV (comma separated value) files. The EAGLE 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 (GUI).

- STP Connection Configuration STP Connectivity Test.
- FTP Server Configuration.
- Retrieving the EAGLE 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 command files before being sent to the STP.
- Command file editing.
- Viewing the log files for event tracking and error message display.

## Overview

The FTP-Based Table Retrieve Application (FTRA) was designed in conjunction with the FTP Retrieve and Replace feature to transfer EAGLE database tables to a remote server for offline processing by using an FTP session. The FTRA is a stand-alone application that interfaces with one or more Signal Transfer Points (STPs). The FTRA can read database tables from the selected EAGLE node using the retrieve commands. The EAGLE converts the output of these retrieve commands into CSV (comma separated value) format files that FTRA ultimately collects. The FTRA also uses a local list of EAGLE commands. FTRA reads the contents of the commands file, validates the commands, and finally uses the commands to collect data from the selected STP. FTRA also collects logs for event tracking and displaying error messages.

The FTRA provides the following functionalities through a Graphical User Interface (GUI):

- Configuration of STP Connections
- Testing of STP Connectivity
- Configuration of FTP Server
- Retrieving the EAGLE database tables from multiple STPs manually or automatically, using the command-line interface, with the results converted to CSV files
- Validation of command files before sending them to the STP
- Command file editing
- Display of log files for event tracking and displaying error messages

# User Guide Conventions

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

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

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

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

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

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

  `SET FTRA_HOME=”C:\<download_directory> ”`

  `SET JRE_HOME="C:\Program Files\Java\<Java directory>"`

- 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*>.

# References

For information about additional publications related to this document, see the Oracle Help Center site.

# 2
# Using the FTRA

This chapter contains information regarding the various ways to use the FTRA.

## FTRA Initialization

To start the FTRA, double-click the **FTRA** icon on the desktop. When the application starts, the **FTRA** window is displayed.

## 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 in the STP Connection Configuration database.

Select **Edit > STP Connection Configuration**.

The below figure shows the description of the fields, buttons, and boxes in the **STP Connection Configuration Menu** window.

**Figure 2-1 STP Configuration**

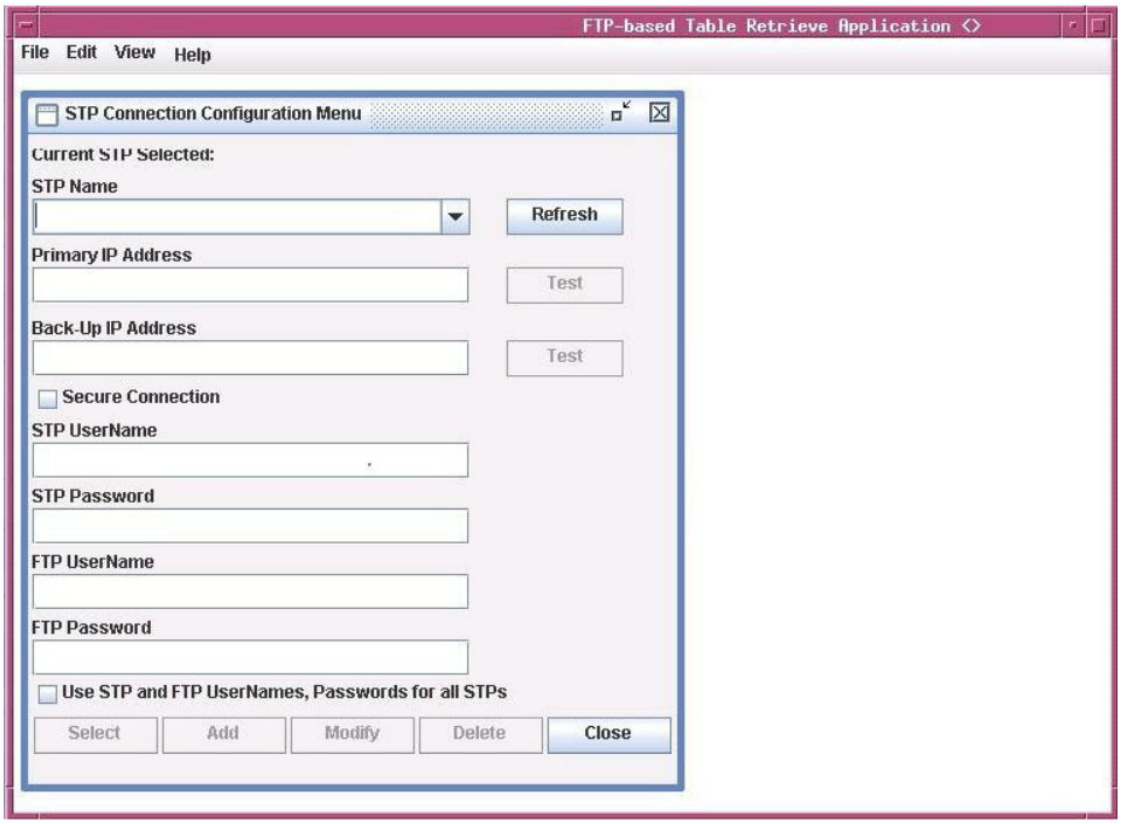


**Table 2-1 STP Connection Configuration Menu Description**

| Item | Description |
|---|---|
| Fields | |
| **STP** Name | The **STP** name must contain at least one alphanumeric character and a maximum of 64 upper-case alphanumeric characters. The STP Name must always be entered in uppercase regardless of the Caps Lock key setting on your keyboard.<br>This field also provides a drop down list for selecting stored STP configuration records. |
| Primary **IP** Address | It is the primary IP Terminal card address of the associated STP (used for telnet sessions). The FTRA uses this IP Terminal card address first when connecting to the STP. The primary IP Terminal card address is the IP address of a service module in the associated EAGLE. |
| Backup **IP** Address | It is the backup IP Terminal card 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 is the IP address of anotherservice module in the same EAGLE.<br>The FTRA does not attempt to make a Telnet connection with the backup IP address (if the backup IP address is configured) of the alternate service module on the EAGLE if the connection with the primary IP address is established but no IP terminal is available. |
| **STP** UserName | It is the user name assigned to the user by the STP system administrator (used for telnet sessions). |
| **STP** Password | It is the password assigned to the user by the STP system administrator (used for telnet sessions). |
| **FTP** UserName | It is the username 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 | It is the FTP password assigned to the user by the administrator (used for FTP) |
| Buttons | |
| Refresh | It 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 | It verifies that the FTRA can successfully connect and login to the EAGLE through an available telnet terminal at the specified IP Terminal card address.<br>The STP Connection Configuration Menu window has two **Test** buttons, one for the Primary IP address, and one for the Backup IP address. |
| Select | It selects the displayed STP name to be connected to the FTRA. |
| Add | It adds a newly entered STP configuration record and associated data to the STP Connection Configuration database. |
| Modify | It modifies the fields of the displayed STP configuration record. |
| Delete | It deletes the displayed STP configuration record and associated data from the STP Connection Configuration database. |
| Close | It closes the **STP Connection Configuration Menu** window. |
| Boxes | |

**Table 2-1 (Cont.) STP Connection Configuration Menu Description**

| Item | Description |
|---|---|
| Secure Connection | It enables the FTRA to use a secure IP connection to the STP.<br>To use a secure connection for the FTRA to EAGLE communication, make sure the EAGLE OA&M IP Security Enhancements feature is enabled and activated, and SSH and SECURITY parameters are ON. The OA&M IP security feature can be verified by entering the `rtrv-ctrl-feat` command at the EAGLE.<br>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 *Database Administration - System Management User's Guide* and enable and activate the EAGLE OA&M IP Security Enhancements feature.<br>The SSH and SECURITY parameters can be verified by following the below mentioned procedures:<br>1. To verify the SSH parameter, enter the command `rtrv-secu-dflt`. If it is not ON, enter `chg-secu-dflt:ssh=on` command to turn it ON.<br>2. To verify the SECURITY parameter, enter the command `rtrv-ftp-serv`. If the SECURITY feature for the required FTP Server entry is not ON, use `chg-ftp-serv` command to turn it ON.<br>**Note**<br>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, or either of SSH and SECURITY parameter is not ON.<br>If this box is checked, the public key fingerprint for the EAGLE specified in this window must be installed onto the FTRA for the FTRA and the specified EAGLE to use a secure connection. After the STP is added to the STP Connection Configuration database, add the public key fingerprint to the FTRA. For this, see the "Secure EAGLE Host Key Provisioning' section. |
| 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. |

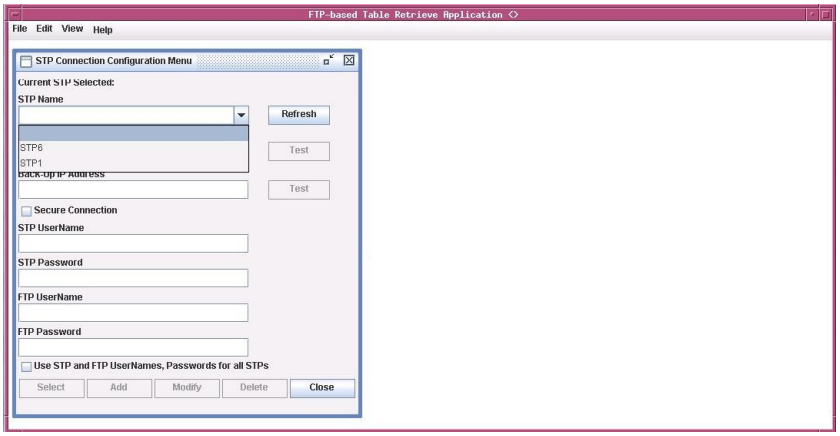
# Displaying an Existing STP Configuration Record

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

**To Use the STP Name Drop Down List**

1. In the **STP Connection Configuration Menu** window, click on the STP Name drop down list and select the appropriate STP name.

**Figure 2-2 Selecting an STP Name from the STP Name Drop Down List**

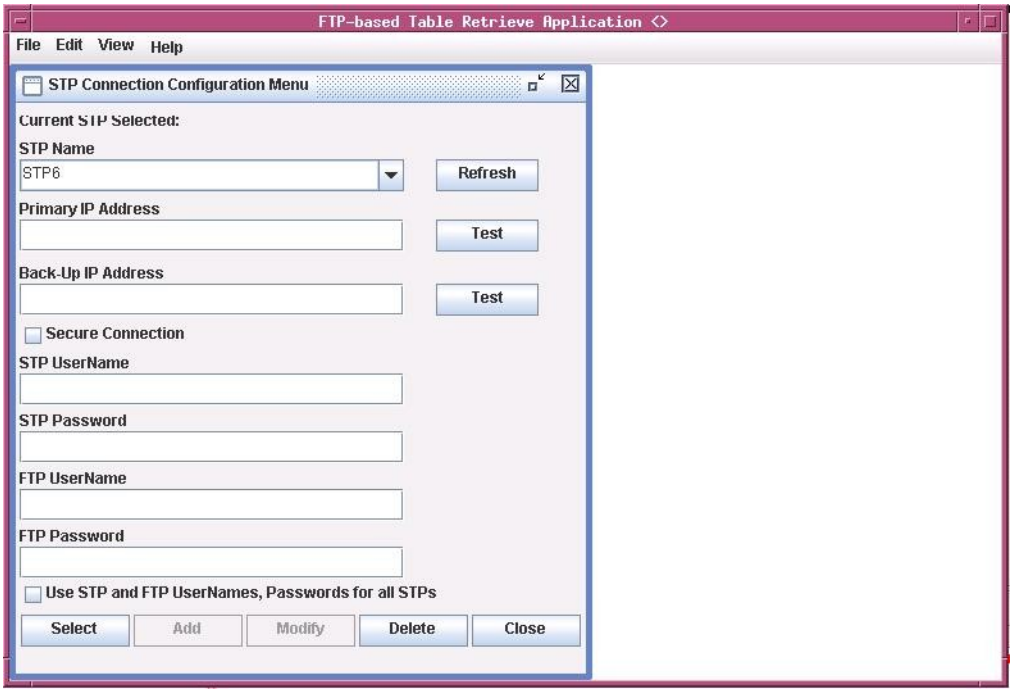



2. When the STP name is selected, the STP configuration record for the specified STP is displayed. The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

# Entering the STP Name

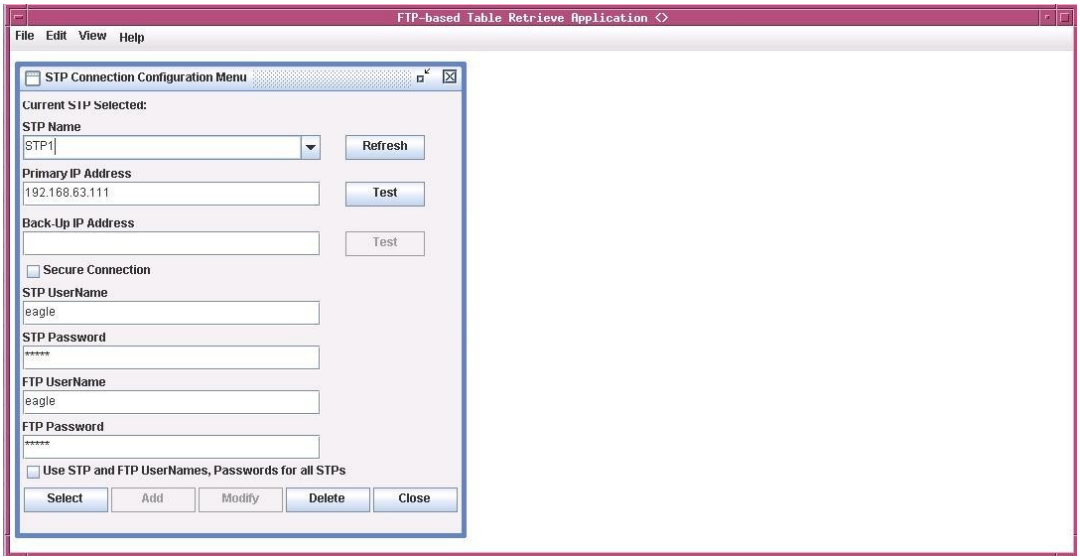
1. Type the STP name in the STP Name field in the **STP Connection Configuration Menu** window. The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

**Figure 2-3 Selecting an STP Configuration Record by Typing in the STP Name Field**




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

**Figure 2-4 STP Configuration Record**




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.

# Testing an STP Configuration Record

1. Select **Edit > STP Connection Configuration** from the **FTRA** window.

   The **STP Connection Configuration Menu** window opens.

2. Display the STP configuration record to be modified.

   For more information, see "Displaying an Existing STP Configuration Record" procedure.

3. Click the **Test** button.

   The **Connectivity Test Log** window opens. See Figure 2-5 and Figure 2-6.

   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 2-5 Connectivity Test Log Window with No Errors**

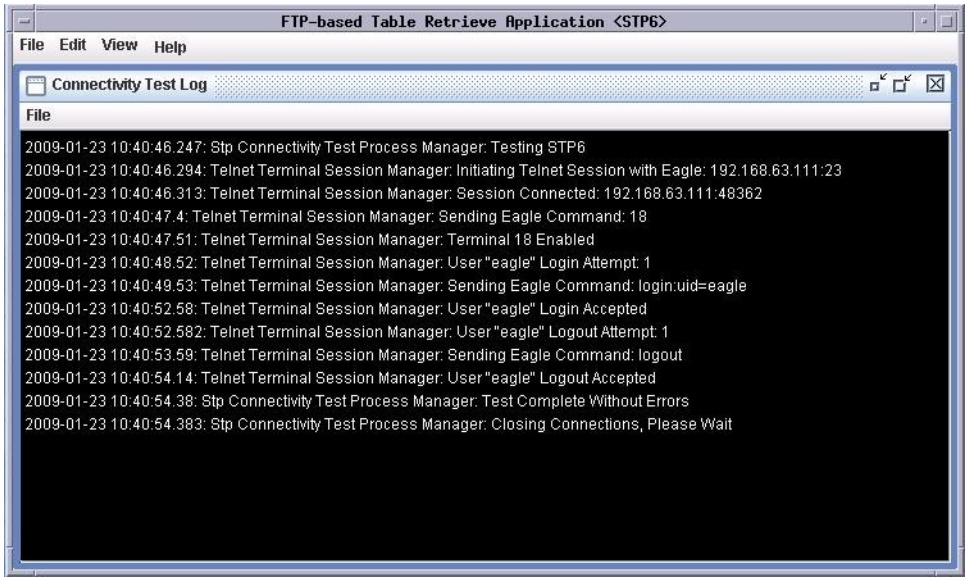
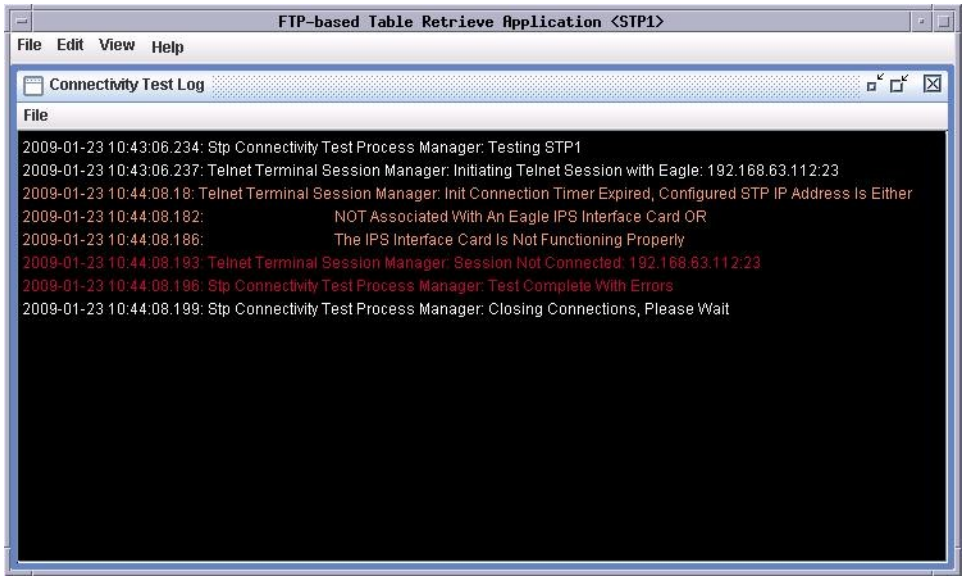



**Figure 2-6 Connectivity Test Log Window with Errors**




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

   Click **OK** to continue.

# 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 saved 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

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

  The **Print** window opens.

## Saving the Connectivity Test Log to a File

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

   The **Save** window opens.
2. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).
3. Select **Save**.

   A saved file confirmation window opens with “Data saved to file.”

# Modifying an Existing STP Configuration Record

1. Select **Edit > STP Connection Configuration** from the **FTRA** window.

   The **STP** Connection Configuration Menu window opens.
2. Display the **STP** configuration record being modified.

   For more information, see the "Displaying an Existing STP Configuration Record" 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.

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

   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. Click **OK** in the **STP Data Modified** window to continue.

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

> **⚠ 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, and SSH and SECURITY parameters 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. If the EAGLE OA&M IP Security Enhancements feature is not enabled or activated, or either SSH or SECURITY parameter is turned OFF, the Secure Connection box should be unchecked. If the EAGLE OA&M IP Security Enhancements feature is enabled and activated, and SSH and SECURITY parameters are turned ON, 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 *Database Administration - System Management User's Guide*.
>
> To change the state of SSH parameter, use `chg-secu-dflt` command. To turn it ON, use `chg-secu-dflt:ssh=on`. To turn it OFF, use `chg-secu-dflt:ssh=off`.
>
> To change the state of SECURITY parameter, use `chg-ftp-serv` command with required server entry and change the SECURITY parameter appropriately.

> **ⓘ Note**
>
> If the **STP** configuration record being changed is shown in the Current STP Selected field, a Modify Warning window is displayed.

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.

# Deleting an STP Configuration Record

1. Select **Edit >STP Connection Configuration** from the FTRA window.

   The **STP Connection Configuration Menu** window opens.

2. To display the **STP** configuration record being deleted, see "Displaying an Existing STP Configuration Record" 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.

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

4. Verify the **STP** name is no longer in the **STP** Connection Configuration database.

See "Displaying an Existing STP Configuration Record" procedure for same.

# Selecting the Current STP

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

   See "Displaying an Existing STP Configuration Record" 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**.
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 Host Key Provisioning

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

This procedure adds the IP addresses of the EAGLE to the FTRA in the **hosts.xml** file placed in the `cfg` directory under the FTRA installation directory.

This procedure must be performed for each IP Terminal card on each EAGLE that the FTRA will connect to, but only for EAGLE using secure connections to connect to the FTRA. This procedure must be performed before any secure connection between the EAGLE and the FTRA is initiated.

If an IP address has not been added to the FTRA's **hosts.xml** file and you try to initiate a secure connection to the EAGLE, you will receive the **STP Primary IP address is missing from host.xml file. To use this IP address with security. check the secure connection checkbox and add IP address in hosts.xml file.** warning message.

If the warning message is received, either clear the **Secure Connection** check box in the **STP** Configuration Record for the STP or add the IP address to the FTRA's **hosts.xml** file.

> **Note**
>
> Once the IP Terminal card is installed into the EAGLE, the public host key fingerprint for the service module will change only when power to the service module is disrupted by removing the service module from the shelf, then reinserting the service module into the shelf, or as the result of any event that interrupts power to the service module. Re-initializing the service module will not change the public host key fingerprint for the service module. This procedure will have to be performed for each public host key fingerprint on the EAGLE 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, you will receive the **STP Primary IP address is missing from host.xml file. To use this IP address with security either clear the secure connection checkbox or add it's host key to this hosts.xml file.** warning message.

If the above warning message is received, then either clear the **Secure Connection** check box in the **STP** Configuration Record for the STP, 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) strong authentication, designed to provide security between the FTRA and the EAGLE. This also prevents a hostile server from tricking the FTRA into exposing any EAGLE 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 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 **Linux** platform, open the `ftra` file.
2. Insert the below mentioned text strings in the application start file, 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.
4. Use the `rept-stat-card:appl=ips` command to see the location of IPS cards in the system. On the EAGLE, enter the `rtrv-trm` command.

   The location of the **service module** is shown in the `LOC` column with the `TELNET` terminal type.

   This is an example of the possible output.

   ```
   rlghncxa03w 13-09-25 16:07:48 GMT  EAGLE 45.0.0
   CARD   VERSION      TYPE      GPL       PST          SST        AST
   1111   131-010-000  IPSM      IPSHC     IS-NR        Active     -----
   1317   -----------  IPSM      IPS       OOS-MT       Isolated   -----
   2217   131-010-000  IPSM      IPS       IS-NR        Active     -----
   ```

```
Command Completed.


rlghncxa03w 05-09-17 15:08:45 GMT EAGLE 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
```

5. Display the **IP** address assigned to the **service module** using the `rtrv-ip-lnk` command, specifying the card location of the **service module** shown in **Step 4** 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 14-01-17 15:08:45 GMT EAGLE5 40.0.0
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 **service module** specified in this procedure is set to YES, see the `rtrv-trm` output in EAGLE and skip this step .

6. Change the Security Administration setting on the terminals assigned to the **service module** with the `chg-trm` command and specify 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 gets 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 **service module** is installed into the EAGLE, UIM 1493 is generated. The EAGLE IP addresses must be added to the FTRA in the **hosts.xml** file.**UIM** 1493 contains the **DSA** key fingerprint that needs to be added to the hosts.xml file. If you recorded the **DSA** key fingerprint for the **service module** when UIM 1493 was generated, skip **Step 7** and go to My Oracle Support (MOS).

> **Caution**
>
> If you are performing **Step 7** from a telnet terminal, make sure the step is being performed from a telnet terminal that is not assigned to the **service module** being initialized. When the **service module** is initialized, you will lose all telnet connections supported by the service module.

7. Obtain the **DSA**key fingerprint for the**service module** by performing the `init-card` command and specifying the location of the **service module**.

   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 is 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 **service module**, remove and reinsert the service module. The public host key fingerprint does not change until the service module loses power. However, contact the My Oracle Support (MOS) before removing and reinserting the service module.

8. Edit the FTRA **hosts.xml** file (in the **$FTRA_HOME/cfg** directory on Linux, or **%FTRA_HOME%\cfg** folder on Windows), using any text file editor. Add the Service Module IP address from the `rtrv-ip-lnk` output shown in **Step 5**.

   - To allow or deny host access, use the HostAuthorizations, AllowHost, and DenyHost elements and specify the appropriate Service Module IP address as shown in the following example:

     ```
     <HostAuthorizations>
     <!-- Add AllowHost elements here -->
     <AllowHost>10.248.13.56</AllowHost>

     <!-- Add DenyHost elements here -->
     <DenyHost>10.248.13.56</DenyHost>
     </HostAuthorizations>
     ```

   - To allow a host access, use the following format:

     ```
     <AllowHost>="<Service Module IP Address>"</AllowHost>
     ```

   - To deny a host access, use the following format:

     ```
     <DenyHost>="<Service Module IP Address>"</DenyHost>
     ```

   - **DSA** public key fingerprint is shown in the output of **UIM 1493** when the service module is installed and in the output of**UIM 1494** when the init-card command is performed in **Step 7**. It has the following format:

   ```
   <AllowHost>="<Service Module IP Address>"</AllowHost>
   ```

> **Note**
>
> The value 767 preceding the DSA public key fingerprint is the length of the key in bytes. On your EAGLE, this value may be different. See 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.

9. Save the file and exit the text editor.
10. 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, 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. While adding a new **STP** record, or changing an existing **STP** record, make sure the **Secure Connection** check box is checked.

11. After the STP record has been added or changed to use a secure connection, test the connection by performing the procedure.

    If the connection test is passed, the IP address is successfully installed.

    If the connection is refused, the Connectivity Test Log indicates there is a mismatched key entry as shown in the following example, and the Host Key Mismatch! pop-up window is displayed.

```
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: Host 192.168.53.71 cannot be
authenticated due to mismatched key entry!.
```

    The options in the Host Key Mismatch! pop-up window are as follows:

    **Allow Once**
    The key is temporarily stored for the current session and the connection is made.

    **Always Allow**
    The key is permanently stored and the connection is made.

    **Don't Allow**
    The key is not added and the connection is not made.

    If the connection test is passed, the public host key fingerprint is successfully installed. If the connection is refused, make sure that the information for the EAGLE and the FTRA shown in the Connectivity Test Log matches. The Connectivity Test Log shows the key received from the EAGLE host and the one contained in the **hosts.xml** file for the EAGLE host. The following is an example from the Connectivity Test Log containing a host key mismatch. The key received from the EAGLE 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 using the FTP Server Configuration menu before database tables can be retrieved from the EAGLE, or command files can be sent to the EAGLE.

**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.
- Any firewall between the FTRA and the FTP server configured in the FTP Server Configuration Menu window, must allow FTPs to the IP address specified in the FTP Server Configuration Menu window.

1. Select **Edit > FTP Server Configuration** from the **FTRA** menu.

   The **FTP Server Configuration Menu** window opens.

**Figure 2-7 FTP Server Configuration Menu**

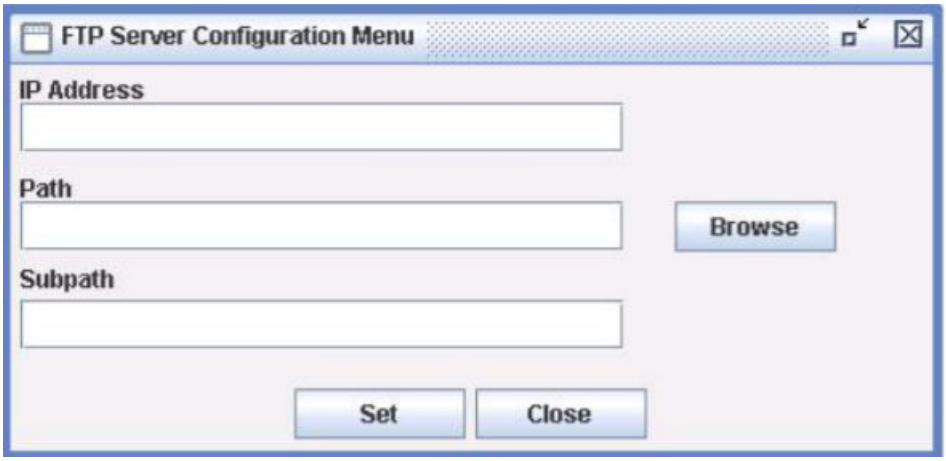



**Table 2-2 FTP Server Configuration Menu Window Descriptions**

| Item | Description |
|---|---|
| **Fields** | |
| **IP** Address | The IP Address of the associated FTP Server. |

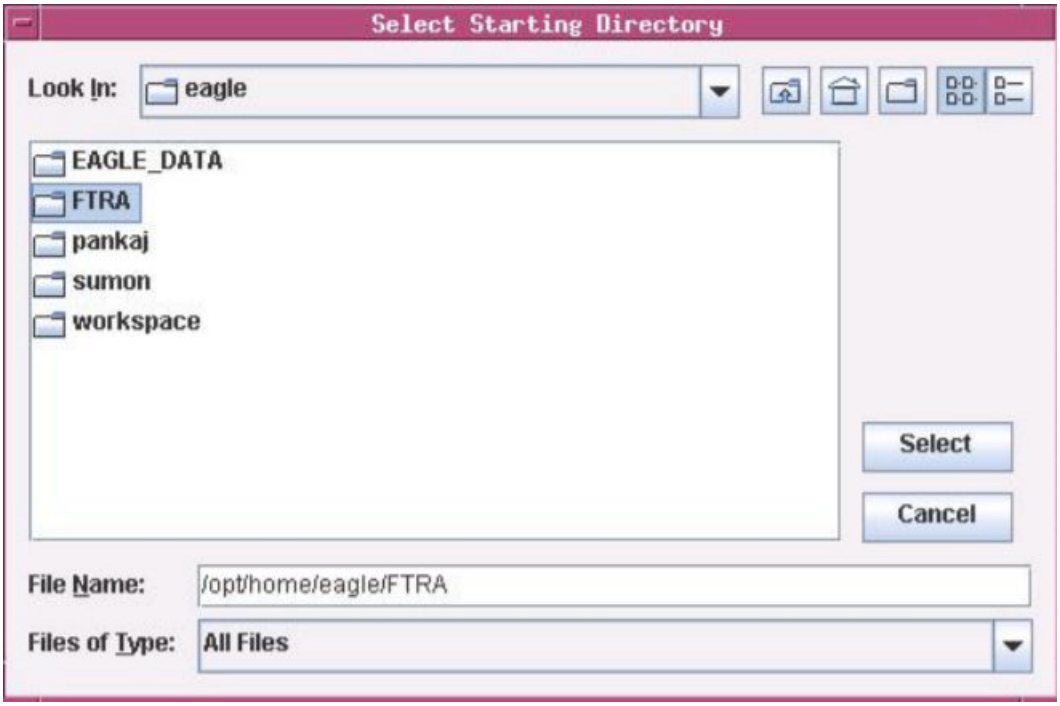
**Table 2-2 (Cont.) FTP Server Configuration Menu Window Descriptions**

| Item | Description |
|---|---|
| Path | The complete path to the data tables transfer directory on the FTP Server.<br>This directory must be the FTP user's default directory. 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 Linux, this is done with the `chmod` command. See your PC system documentation Linux `man` pages for full details on setting directory permissions. |
| Subpath | The subpath value used to inform EAGLE about the directory of data transfer. The subpath is the path of the data tables transfer directory relative to the user's default directory upon FTP login. A file separator ('\' or '/') is not used to begin the subpath string.<br>For example, if `C:\root\ftp` is the FTP user's default directory and `C:\root\ftp\data` is the path of the data tables transfer directory, then the path and the subpath of the FTP Server Configuration should be set as:<br>`path = C:\root\ftp\data`<br>`subpath = data` |
| **Buttons** | |
| Browse | Opens the **Select Starting Directory** window to initiate a directory/file selection for the data tables. |
| 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.
3. Enter the path for the FTP temporary data table storage area or click the **Browse** button.

   The **Browse** button opens the **Select Starting Directory** window to select the location for the temporary data table storage area.

**Figure 2-8 Select Starting Directory**




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 Linux, this is done with the `chmod` command. Please see your PC system documentation or Linux `man` pages for full details on setting directory permissions.

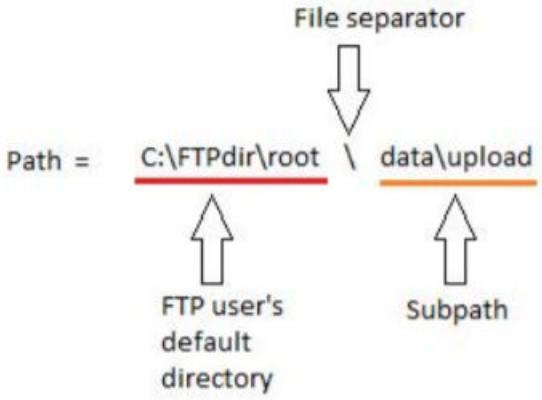
**Table 2-3 Select Starting Directory Window Descriptions**

| 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 image below shows the relationship between the path and the subpath:

**Figure 2-9 FTP Server Path and Subpath Relationship**




Consider the following points when setting the subpath:

- The subpath must always be the last part of the path, starting after the user's default directory upon FTP login. If the value of subpath is not the last part of the path, the **Invalid Sub Path** warning is issued. For example, if the path value is set as `C:\user\ftp\data` and the subpath value is set as `ftp\admin`, the warning window is displayed and the FTP configuration data is not saved.
- A file separator ('\' or '/') is not used to begin the subpath string. If a file separator is entered to begin the subpath, the same warning window is displayed and again the FTP configuration data is not saved.
- The subpath is not a mandatory field only when the path is set as the FTP user's default directory. For example, if the FTP user's default directory is `C:\root\ftp` and the path is `C:\root\ftp`, then the subpath should be blank.

5. Click **Set**.

   The **FTP Server Data Set** information window opens.

   Click **OK** to continue.

# Retrieving Database Tables from an STP

## Retrieve Tables Window

The Figure 2-10 is used to select the database tables to be retrieved from the selected STP. The **Retrieve Tables** window contains a list of predefined retrieve commands.

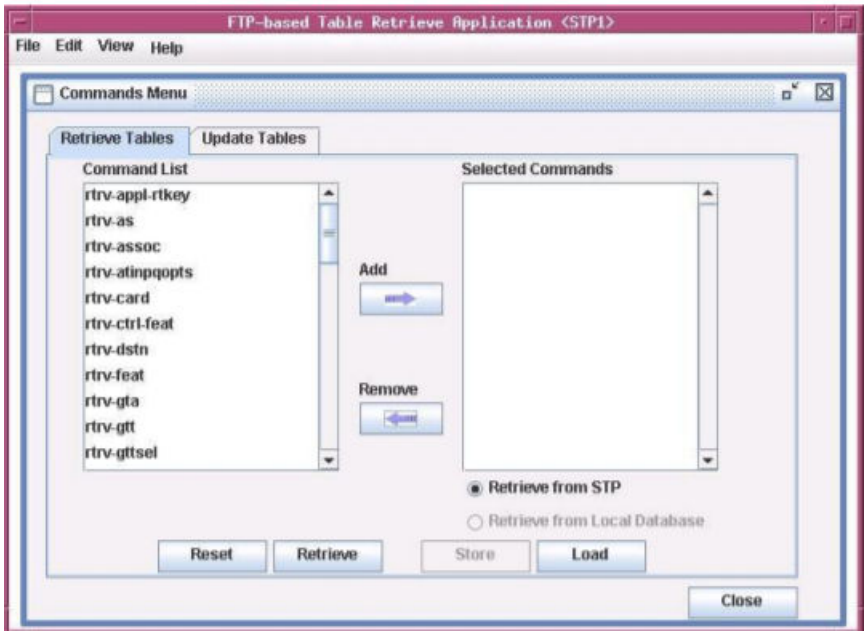
The **Retrieve from STP** and **Retrieve from Local Database** buttons determine whether new database tables are retrieved from the selected STP or if existing tables already retrieved from that STP will be used. If no tables exist for the selected STP, the **Retrieve from Local Database** button will 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 retrieval was executed with or without errors. The Retrieve Tables Log opens allowing the user to view the events.

**Note**

- If you attempt to retrieve and convert the database tables for the GTT commands (`rtrv-tt`, `rtrv-gtt`) and the EGTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`) in the same retrieve tables request, you will receive a warning that errors can be caused by attempting to retrieve and convert the **GTT** and **EGTT** database tables from the same EAGLE. Click **Yes** to continue.
- 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 and converted. The error will occur when the attempt is made to convert the database tables that could not be retrieved.

**Figure 2-10 Retrieve Tables Window**




The following Table shows the description of the fields and buttons in the **Retrieve Tables** window.

**Table 2-4 Retrieve Tables Window Description**

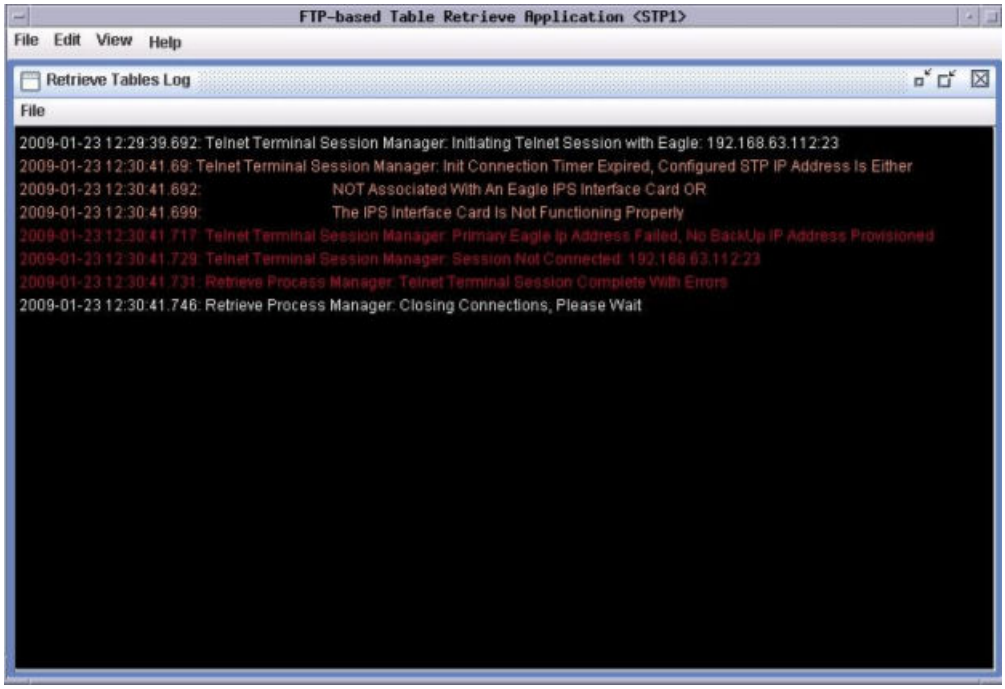
| Item | Description |
|---|---|
| Fields | |
| Command List | Contains a predefined list of retrieve commands. |

**Table 2-4 (Cont.) Retrieve Tables Window Description**

| Item | Description |
|---|---|
| Selected Commands | These commands are used to determine which database tables are retrieved from the selected STP.<br>Any number of 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. |
| 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 the `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. |

When a Retrieve Tables command is performed, the FTRA verifies that the EAGLE is running one of the supported releases. If the EAGLE is not supported, an error message is displayed and the Retrieve Tables command is terminated.

**Figure 2-11 Retrieve Table Log - Release Not Supported Error**




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

1. Select **Edit > Commands > Retrieve Tables** from the **FTRA** window. The **Retrieve Tables** window opens.
2. To select commands in the **Command List** box of the **Retrieve Tables** window, click on a single command, a range of commands, or 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.

   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. It gets highlighted. Click the **Remove** button. The highlighted command is moved to the **Command List** box.
   b. To select a range of multiple commands to be removed, click on the first command and while holding down the Shift key, click on the last command to be removed. Click the **Remove** button. All highlighted commands are moved to the **Command List** box.
   c. Hold down the **Ctrl** key and click on each of commands to be removed. Click the **Remove** button. Only the highlighted commands are moved to **Command List** side.
   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.
5. To store the selected commands for the Command Line Interface, click the **Store** button on the **Commands Menu** window. Click **OK** to continue. To verify which retrieve commands

are stored, click the **Load** button. The stored commands appear in the **Selected Commands** box.

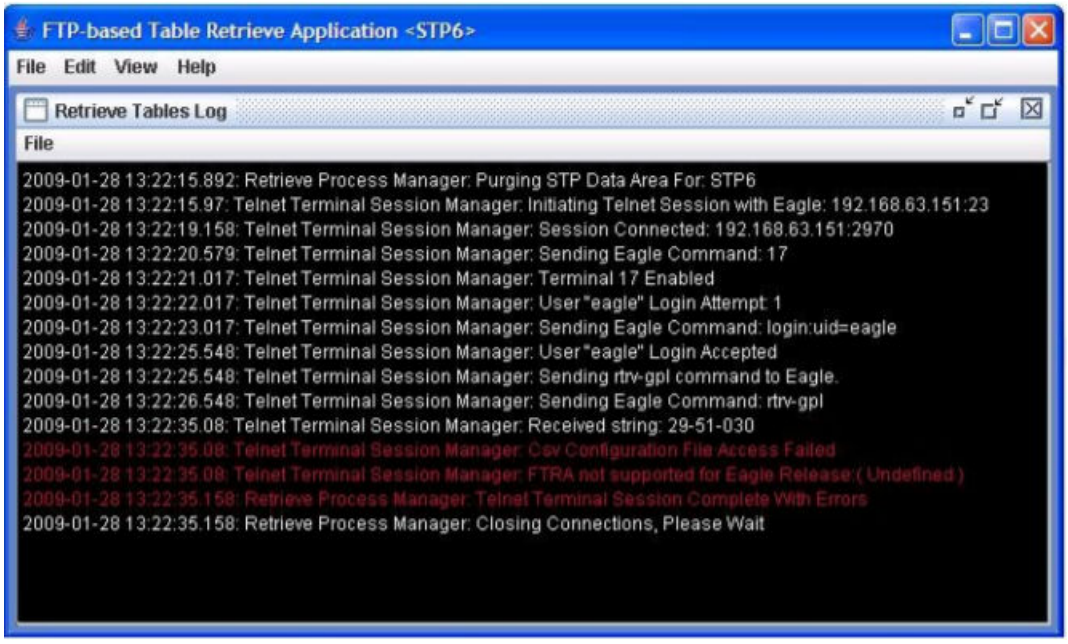
If database tables are to be retrieved from the selected STP, skip **Step 6** and go to **Step 7**.

6. To generate **CSV** files from database tables that are already retrieved from the selected STP, select the **Retrieve from Local Database** button after selecting the desired commands. Click the **Retrieve** button.
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 and displays the message “Processing Retrieve Request, Please Wait” until the retrieve process completes.

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

> **Note**
>
> If you are retrieving the database tables for any of these **GTT** commands (`rtrv-tt`, `rtrv-gtt`) and any of these EGTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`), see the beginning of this section.

**Figure 2-12 Retrieve Tables Log Window - Processing Retrieve Request**



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

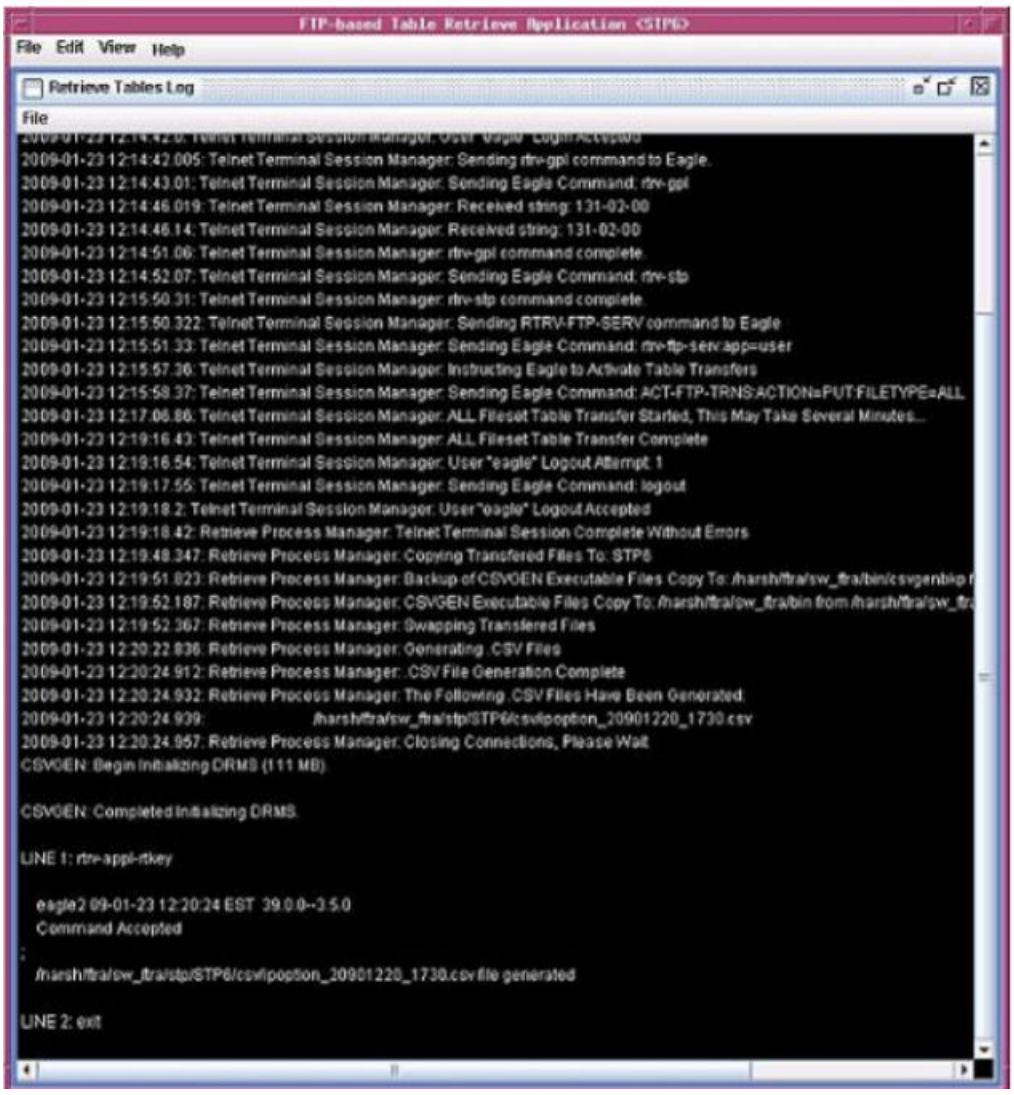
a. If no errors occurred, the text ”Retrieve Tables processing completed without errors” “Please check Retrieve Tables Log for Results” appears in the **Command Complete** window.
Click **OK** to continue.

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. The **Retrieve Table Log** window opens. Click **OK** to continue.

# Retrieve Tables Log

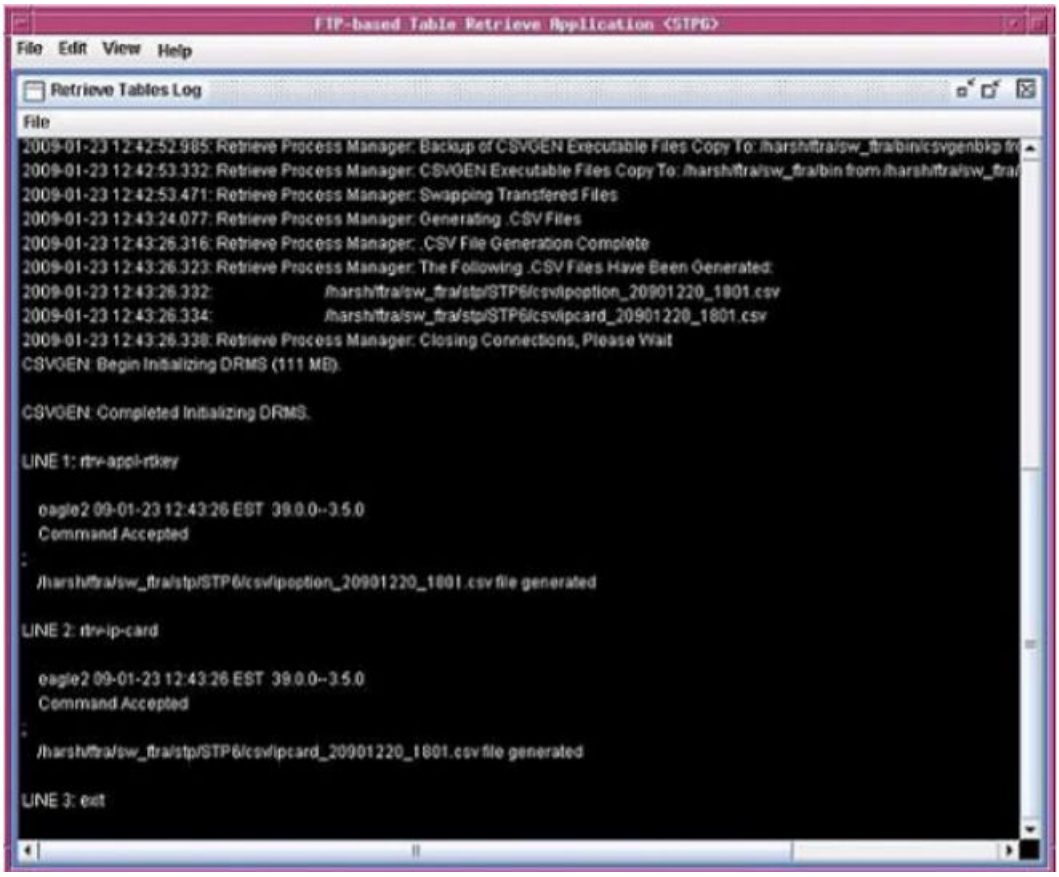
The Retrieve Tables Log contains the events of the retrieve processing and any error messages that may have occurred. The **Retrieve Tables Log** window opens after database tables have been retrieved from an STP and is displayed until the retrieve processing is complete. See the following figure:

**Figure 2-13 Retrieve Tables Log Window without Errors**



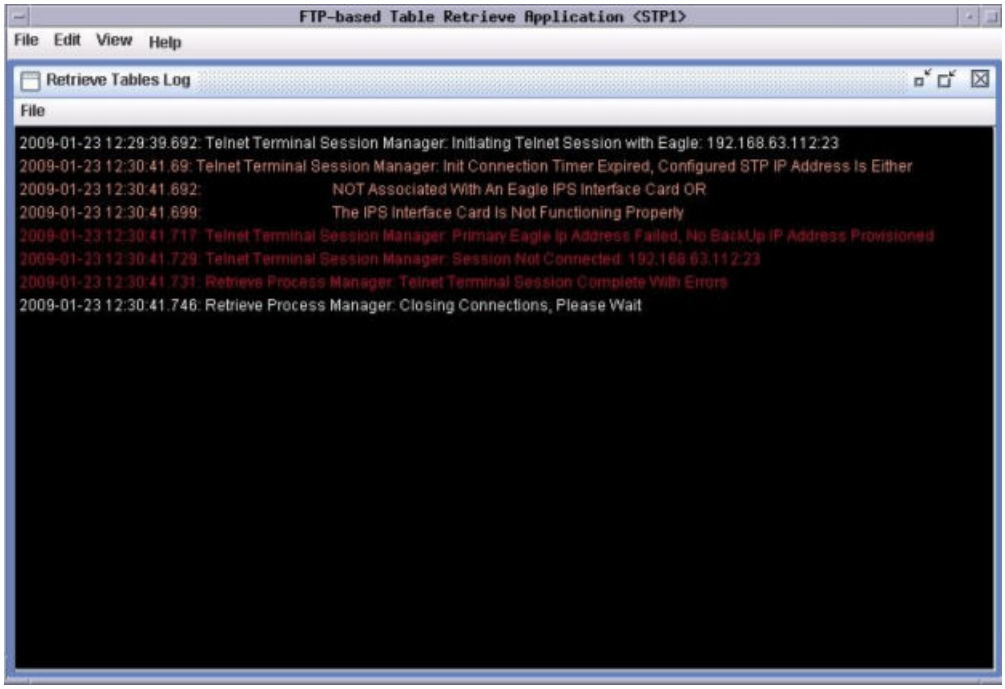
The Retrieve Tables Log displays the information of the **CSV** files generated for the selected retrieve commands. The filenames of the **CSV** files are displayed in ascending order except for the filename of the `rtrv-stp` **CSV** file. Since the `rtrv-stp` command **CSV** is not generated by the **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 the following figure as an example of the Retrieve Tables Log when the `rtrv-stp` command is processed

**Figure 2-14 Retrieve Table Log with the RTRV-STP Command CSV Example**




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 the following figure:

**Figure 2-15 Retrieve Table Log with Errors**




## 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 saved to a file or printed before the display is cleared.

- From the **Retrieve Tables Log** window, select **File > Clear Display**.
- From the **FTRA** window, select **View > Retrieve Tables Log**. Select **File > Clear Display** in the **Retrieve Tables Log** window.

## 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.
2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTRA** window.
3. Select **File > Print** in the **Retrieve Tables Log** window.

   The **Print** window opens.

## 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.
2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTRA** window.

   The **Retrieve Tables Log** window opens.
3. Select **File > Save** in the **Retrieve Tables Log** 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. The user can use Microsoft Word to open the file, even if it is saved as a .txt file.

5. Click **Save**.

   A saved file confirmation window opens with “Data saved to file.”
6. To save the file, click **OK** in the **Saved** file confirmation window to continue.

# Command Line Interface

The FTRA Command Line Interface allows the user to retrieve the same database tables, using the EAGLE 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 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 Linux).

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 Linux platform). Please see the platform's scheduling program for specifics on how to use the external scheduling software. For example, on the Linux platform, enter the `man crontab` command.

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

3. On the Linux 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. 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.

**Figure 2-16 FTRA Windows Scheduled Task**


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

**Figure 2-17 LINUX cron job scheduled via crontab**

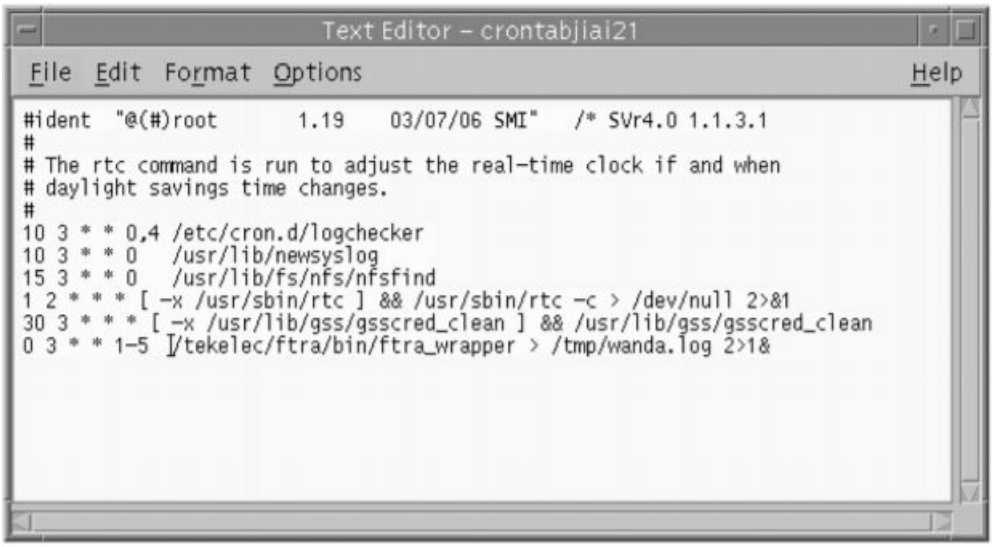



**Figure 2-18 FTRA wrapper script example for LINUX**

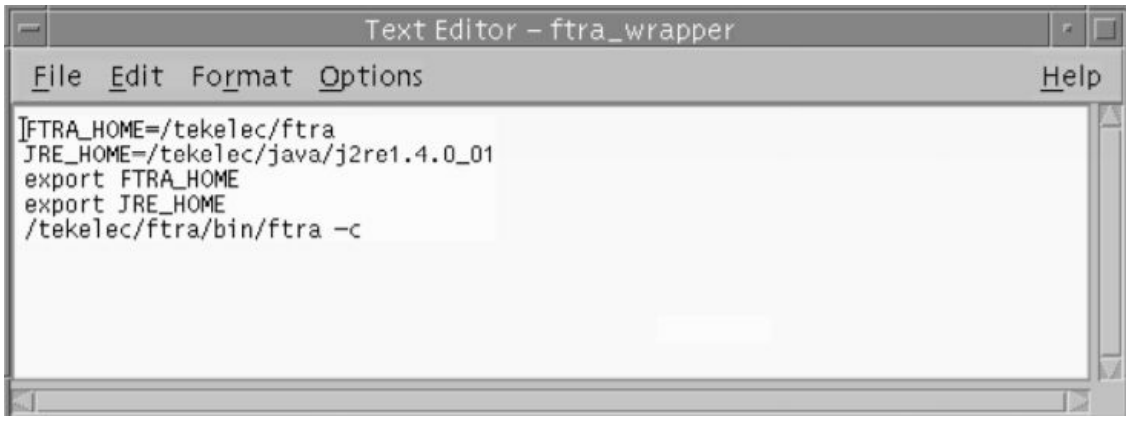
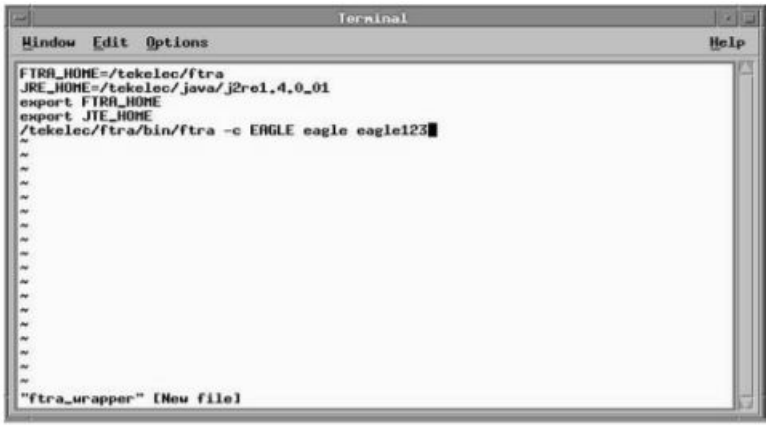



**Figure 2-19 FTRA wrapper script example on LINUX for modifying STP configuration**



- 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 ) or “cron” (in Linux).

  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 Linux).

  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 Linux workstation, it might be necessary to create a wrapper script for FTRA to set environmental variables correctly

# Updating Database Tables in the Selected STP

The **Update Tables** window is used to send **EAGLE** 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.

The following table shows the description of the fields and buttons in the **Update Tables** window.

**Figure 2-20 Update Table Window**

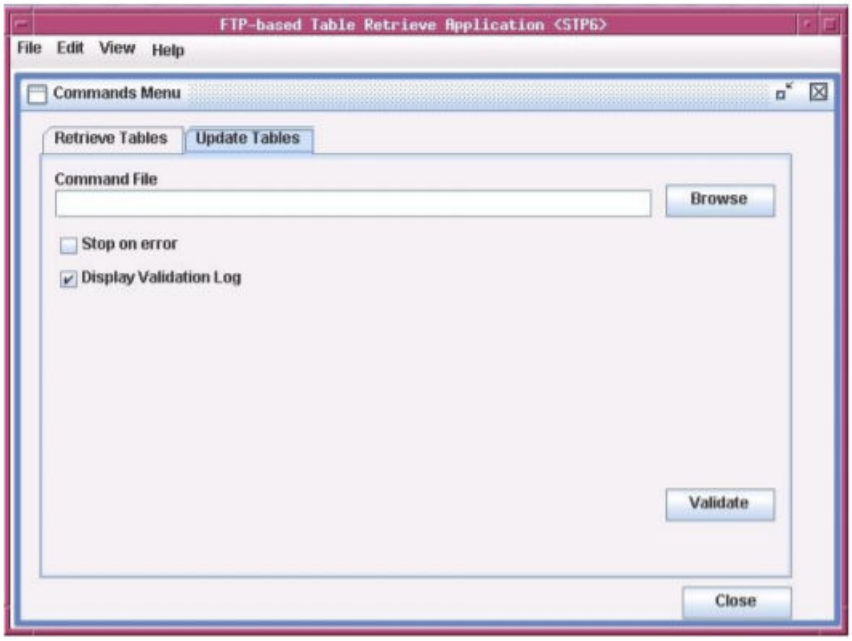



**Table 2-5 Update Tables Window Description**

| Item | Description |
|---|---|
| **Fields** | |
| Command File | The path and file name of the command file are entered here. A command file contains the **EAGLE** 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** commands using the offline database. |
| Close | Closes the **Commands Menu** window. |

# Validating a Command File

1. Select **Edit > Commands > Update Tables** in the **FTRA** window.

   The **Update Tables** window opens.

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 opens. Locate 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.

The following table shows the description of the buttons in the **Select** window.

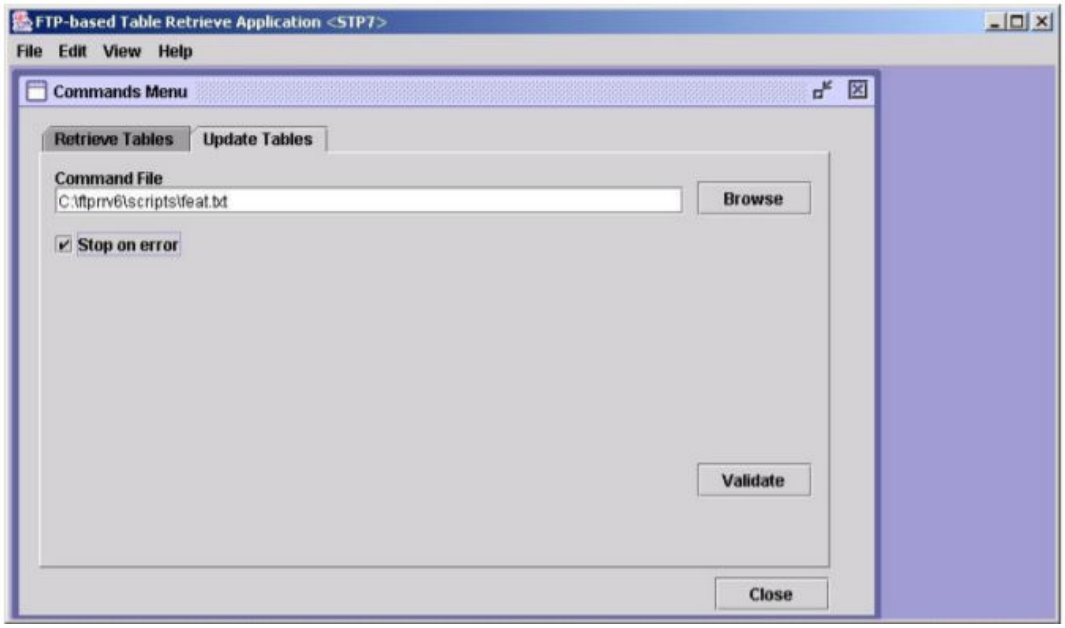
**Table 2-6 Select Window Descriptions**

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

3. To have the command validation stop if any errors are found, check the **Stop on error** box in the **Update Tables** window.

   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 2-21 Update Tables Window with a Command File Selected and Stop on Error Box Checked**

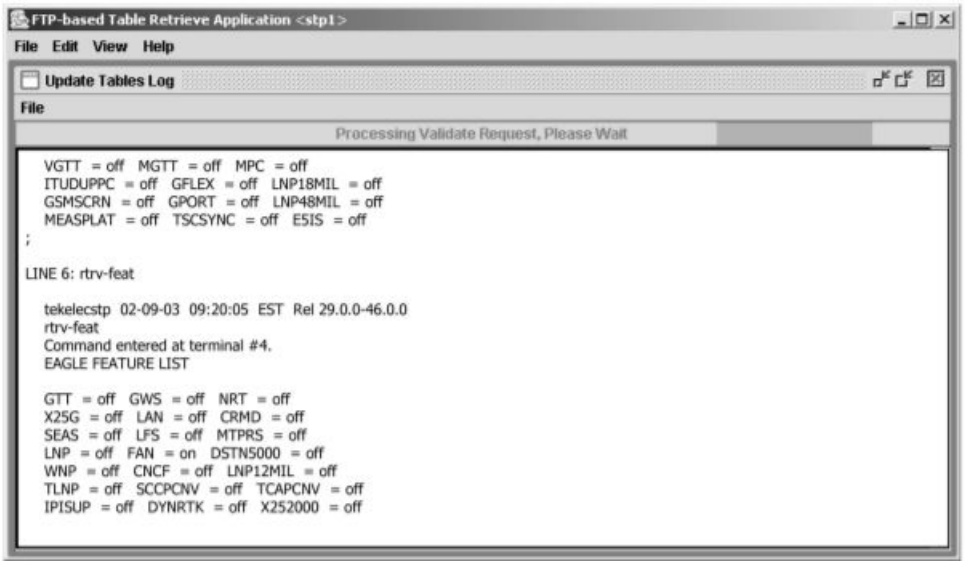



4. Click the **Validate** button.

   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.

   When processing is finished, the **Update Validation Complete** window opens. Click **OK** to continue.

**Figure 2-22 Update Tables Log Window - Processing Retrieve Request**




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

   It contains the events and error messages generated during the validation. .

# 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.

The following table shows the description of the buttons in the **Update Validation Complete** window.

**Table 2-7 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 section. |
| Commit | Sends the commands in the command file to the STP. A **Command Complete** window is opened and the Update Tables Log is updated.<br>If the Update Tables validation is 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. There is no **Commit** button in the **Update Validation Complete**window and hence it prevents the sending of invalid commands.

To fix the errors in the command file, click the **Edit** button and go to the "Editing a Command File" section.

## 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. 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.” Click **OK** to continue. The Update Tables Log contains the commit processing events.

## Stopping 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. 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 opens.

- When the editing is complete, perform one of the following steps.
  1. Select **File > Save** from the **Command File Editor** window.

     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.
  2. Select **File > Save and Commit** from the **Command File Editor** window.

     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. The command file is sent to the selected STP. The Update Tables Log contains the commit processing events.
  3. Select **File > Quit** from the **Command File Editor** window.

     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 opens 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.

# 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 **FTRA** window.

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

   The Update Tables Log display clears.

# 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.
2. Select **View >Update Tables Log** in the **FTRA** window.

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

   The **Save** window opens.
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. The user can use Microsoft Word to open the file even if it is 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.” Click **OK** to continue.

## Printing the Update Tables Log

> **Note**
>
> Perform either step 1 or steps 2 and 3.

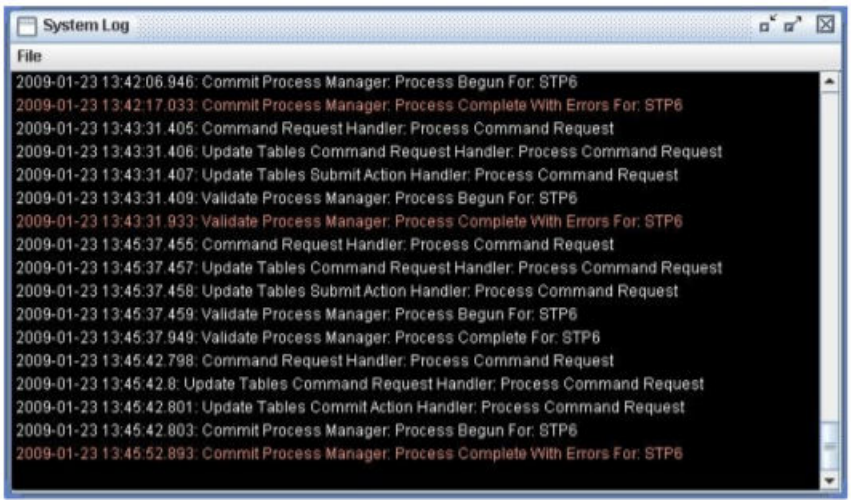
1. Select **File > Print** from the **Update Tables Log** window.
2. Select **View >Update Tables Log** in the **FTRA** window.
3. Select **File > Print** from the **Update Tables Log** window.

   The **Print** window opens.

# 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.

**Figure 2-23 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 **FTRA** window.

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

## Printing the System Log

1. Select **View >System Log** in the **FTRA** window.

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

   The **Print** window opens.

## Saving the System Log to a File

1. Select **View >System Log** in the **FTRA** window.

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

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

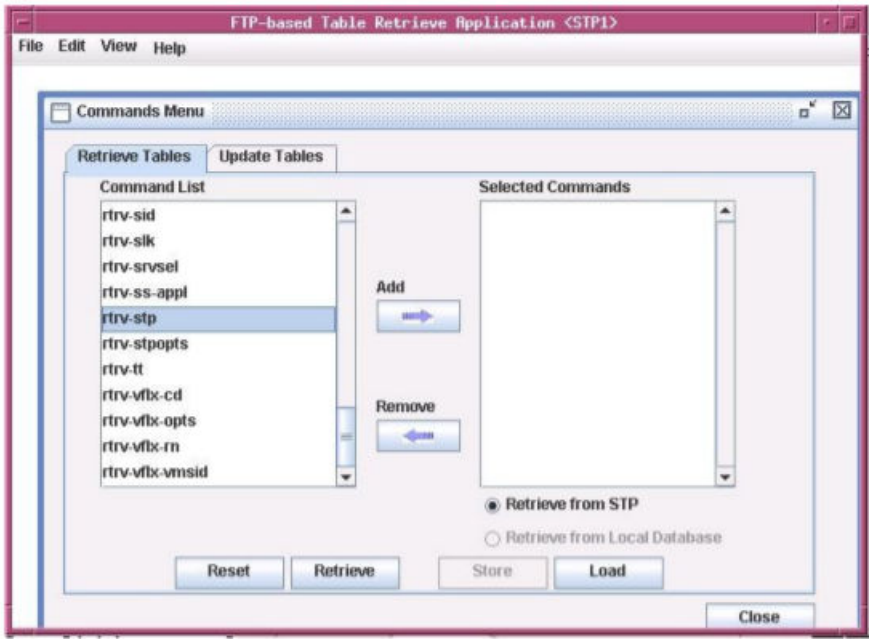
   > **Note**
   >
   > The .doc file type is recommended. The user can use Microsoft Word to open the file even if it is saved as a .txt file.
4. To save the System Log to a file, click the **Save** button.

   A saved file confirmation opens with “Data saved to file”. Click **OK** to continue.

# RTRV-STP Command

The rtrv-stp command provides a consolidated report of STP configuration on a system-wide basis.

**Figure 2-24 Retrieve Tables window with rtrv-stp command selected for retrieval**




# RTRV-STP Command Retrieval Session

Below represented is the FTRA retrieval session when `rtrv-stp` command is supported on EAGLE. If the command is not supported on EAGLE, an error will be displayed and the retrieval session will be terminated.

**Figure 2-25 Successful Retrieval Session for rtrv-stp command**

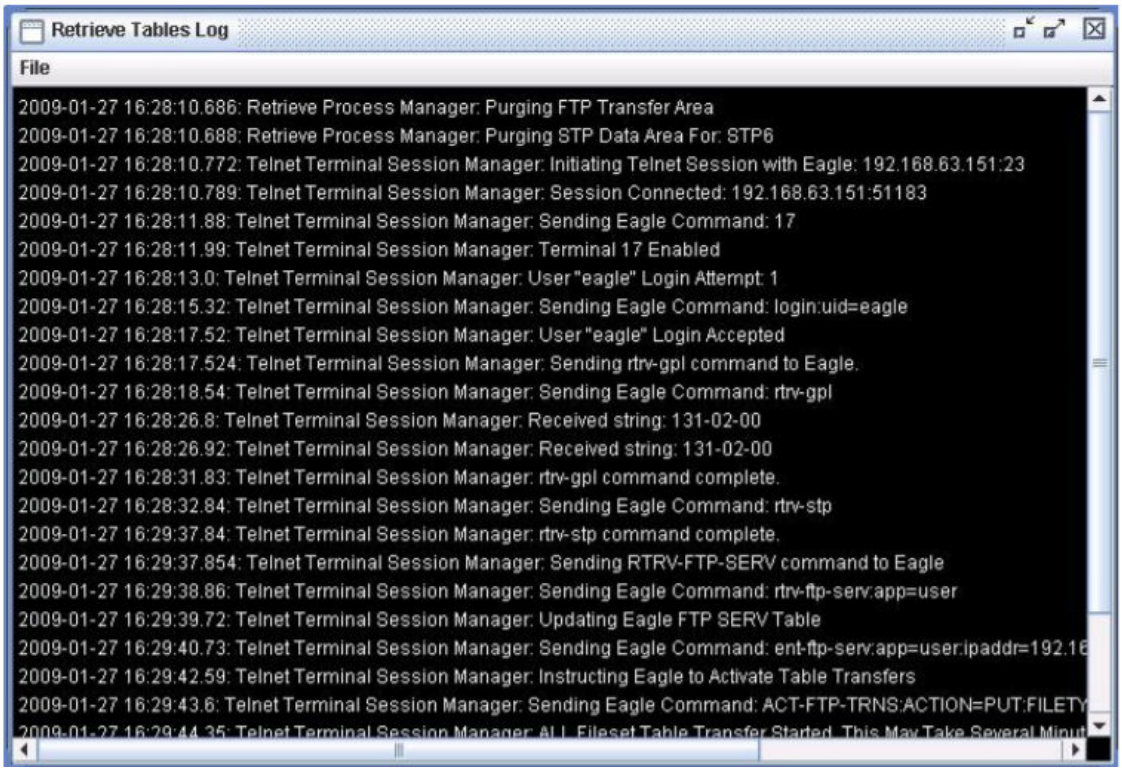
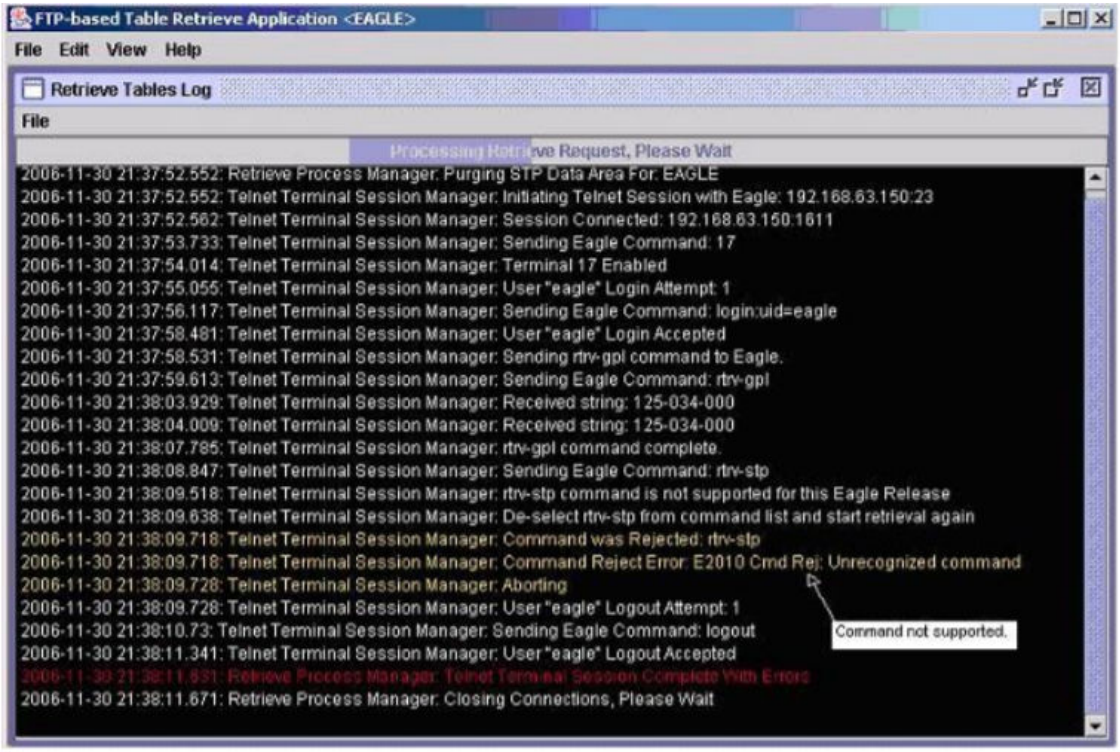



**Figure 2-26 Rtrv-stp Command unsupported on EAGLE release**



# 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 **FTRA** window.

# FTRA release 4.5

FTRA 4.5 is compatible with EAGLE 45.0 and all future EAGLE releases.

# SSH/SFTP Error Codes

Table 2-8 and Table 2-9 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. Each error code contains a brief description of the error and the suggested recovery action.

This section also contains procedures, following Table 2-8 and Table 2-9, for testing connectivity and network problems, and to verify that the setup for making secure connections is correct.

If secure connections to the **EAGLE** cannot be made, verify that the EAGLE OA&M IP Security Enhancements feature is enabled and activated by entering the `rtrv-ctrl-feat` command and verify the SSH and SECURITY parameters are ON by entering the `rtrv-secu-dflt` and `rtrv-ftp-serv` commands, respectively, at the EAGLE before performing any of the actions in Table 2-8 and Table 2-9.

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 *Database Administration - System Management User's Guide* and enable and activate the EAGLE OA&M IP Security Enhancements feature.

If the SSH or SECURITY parameters are not ON, these parameters can be turned ON by entering `chg-secu-dflt:ssh=on` and `chg-ftp-serv`, respectively.

If any of the errors shown in Table 2-8 or Table 2-9 are encountered after the recovery procedure is verified, contact *Customer Care center*.

**Table 2-8 FTP/SFTP/SSH Error Codes**

| SFTP SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| User Errors | | |
| 592 | File open failed. | Invalid file name in the download list, or out of resources. Report this issue to Customer Care Center immediately. |
| 593 | The file name is already specified. | Report this issue to Customer Care Center immediately. (Internal **SFTP** implementation error). |
| 594 | Invalid Path | Verify that the path is valid in the **FTP Server Configuration Menu** window. |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| 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 (See Connectivity Test – I and Connectivity Test – II). 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 is valid and an account exists for the username and password on the **SSHD** server host. |
| **SFTP** Errors | | |
| **SFTP** Client Errors | | |
| 597 | **SFTP** client packet send failure | Perform these tests:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 598 | The **SFTP** connection is closed. | |
| 599 | **SFTP** packet read failure | |
| 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. If the error persists, report the issue to Customer Care Center. |
| 601 | **SFTP** client invalid ID failure | Notify Customer Care Center. |
| 608 | **SFTP** received an 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. If the error persists, report the issue to Customer Care Center. |
| 609 | **SFTP** handle mismatch error. This error is displayed when there is a failure to receive an expected handle upon successful **READ**/**WRITE**/<br>**CREAT**/**TRUNC**/**EXCL** of a file using **SSH_FXP_OPEN** on remote server. | |
| 610 | Unexpected **SSH2_FXP_ATTRS**. | |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| 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. |
| 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 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. |
| 614 | The **SFTP** client receives SSH_FXP_DATA as a response to any file operations from the server. This error implies that the client received an unexpected SSH_FXP_NAME from the server. | |
| 615 | The **SFTP** client received more data than expected. | |
| 616 | The **SFTP** client failed to read the data from the file descriptor of the file specified for transfer. | Report this issue to Customer Care Center immediately. |
| **SSH** Client Errors | | |
| 617 | Excessive identity files. OpenSSH implementation contains the maximum of 100 identity files or the client configuration file is corrupted. | Report this issue to Customer Care Center immediately. |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| SFTP SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 624 | The debug levels allowed for SSH protocol in openSSH is 0-9. The client configuration file contains an error or is corrupted. | |
| 625 | Failure to read the client configuration file. | Report this issue to Customer Care Center 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 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. | |
| 631 | **SSH** user authentication failure. Please verify that only the password authentication is set to “yes” in the SSH server configuration file. See **SSHD** server configuration provided by vendor of the product. The FTRA and the EAGLE is compatible with **openSSH 3.0.2p1**. | Report the issue to Customer Care Center 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 Customer Care Center. |
| 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 640 | A bad message was received during the SSH authentication. | |
| 641 | Missing authentication context, encountered during the SSH user authorization. | Report this issue to Customer Care Center immediately. |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| SFTP SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 645 | A bad option was specified in the SSH client on the EAGLE. | |
| 646 | An unsupported escape character was used in the SSH client on the EAGLE. | |
| 647 | An unsupported cipher type was used in the SSH client on the EAGLE. | Report this issue to Customer Care Center immediately. |
| 648 | An unsupported **MAC** type was used in the SSH client on the **EAGLE**. | Verify that the **SFTP**/**SSHD** version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 649 | A bad port was used in the SSH client on the EAGLE. | Report this issue to Customer Care Center immediately. |
| 656 | Bad forwarding was used in the SSH client on the EAGLE. | |
| 657 | Bad forwarding ports were specified in the SSH client on the EAGLE. | |
| 658 | A bad dynamic port was specified in the SSH client on the EAGLE. | |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| SFTP SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 659 | The host was not specified in the SSH client on the EAGLE. | Verify that the **SFTP**/**SSHD** version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 660 | An invalid option or argument was specified in the SSH client on the EAGLE. | Report this issue to Customer Care Center immediately. |
| 661 | The hostname was not specified in the SSH client on the EAGLE. | |
| 663 | The **SSH** client was unable to load the cipher type on the EAGLE. | |
| 664 | SFTP SSH SET NON BLOCKING CALL FAILURE | |
| 665 | Compression is already enabled in the SSH client on the EAGLE. | |
| 666 | Unknown cipher number on the SSH client on the EAGLE. | |
| 667 | The SSH client key length is invalid. | |
| 668 | No key is available on the SSH client on the EAGLE. | Report this issue to Customer Care Center immediately. |
| 669 | The secure connection was closed by the remote server, see 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 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 Customer Care Center. This is not a software problem but there is a security threat. The keys/authentication may have to be updated immediately. |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| SFTP SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 674 | The **SSH**/**SFTP** client on the EAGLE 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 675 | Corrupted check bytes were detected on the **SSH**/**SFTP** client on the EAGLE. | |
| 676 | Corrupted **MAC** on input was detected by the **SSH**/**SFTP** client on the EAGLE. | Verify that the `sshtools.xml` file provided with **FTRA** software has the field as shown:<br><!-- The Message Authentication Code configuration, add or override default mac implementations --><br><MacConfiguration><br><DefaultAlgorithm>hmac-md5</DefaultAlgorithm><br></MacConfiguration> |
| 677 | Corrupted pad on input was detected by the SSH/**SFTP** client on the EAGLE. | Report this issue to Customer Care Center immediately. |
| 678 | **SSH**/**SFTP** tried to close a connection that is already closed. | |
| 679 | The **SSH**/**SFTP** client on the EAGLE 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 680 | **SSH**/**SFTP** tried to set the packet size twice. | Report this issue to Customer Care Center immediately. |
| 681 | A bad packet size was detected by the **SSH**/**SFTP** client on the EAGLE. | |
| **SSH**/**SFTP** Connection/Setup Errors | | |

**Table 2-8 (Cont.) FTP/SFTP/SSH Error Codes**

| SFTP SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 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:<br>• FTP Server Verification<br>• SFTP /SSHD Server Verification<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 683 | The **SSH** connection was refused by the remote server. | |
| 684 | The **SSHD** server is unreachable. | |
| 685 | The network has reset. | |
| 686 | The **SSH**/**SFTP** connection has been aborted. | |
| 687 | The **SFTP**/**SSH** connection has been reset by the peer. | |
| 688 | Failed to allocate network buffers. | |
| 689 | The **SSH**/**SFTP** socket is already connected. | |
| 690 | The **SSH**/**SFTP** socket is not connected. | |
| 691 | The network channel is down. | |
| 692 | The **SSHD**/**SFTP** server connection host is down. | |
| 694 | **SFTP** client channel read failure. | |
| 695 | **SFTP** client channel write failure. | |
| 696 | **SFTP** client channel open failure. | |

**Table 2-9 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 using the `rtrv-ftp-serv` command, and re-try the connection. |
| 41 | Protocol wrong type for socket | Report this issue to Customer Care Center. |
| 42 | The protocol is not available. | |
| 43 | The protocol is not supported. | |
| 44 | The socket type is not supported. | |
| 45 | The operation is not supported on the socket. | |
| 46 | The protocol family is not supported. | |
| 47 | The address family is not supported. | |

**Table 2-9 (Cont.) Generic Network Error Codes**

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 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:<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 52 | The network dropped the connection on reset. | |
| 53 | Software caused the connection to abort. | Report this issue to Customer Care Center. |
| 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:<br>• Connectivity Test – I<br>• Connectivity Test – II<br>• Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 55 | No buffer space available. | Report this issue to Customer Care Center. |
| 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**.<br>• Connectivity Test – I<br>• Connectivity Test – II |
| 61 | The connection was refused. | Verify that there is a FTP server is running on the remote station by performing the FTP Server Verification test. |
| 62 | The network is down. | Verify that the connection tests pass and network outage numbers are within the allowed limits as shown in these sections:<br>• Connectivity Test – I<br>• Connectivity Test – II |
| 65 | There is no route to the host. | |
| 67 | The host is down. | |

**Table 2-9 (Cont.) Generic Network Error Codes**

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 30 | Read-only file system | • Network Outage Trouble Shooting<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Customer Care Center. |
| 32 | Broken pipe | Report the issue to Customer Care Center. |
| 35 | Unsupported value | |

# Troubleshooting Procedures

## FTP Server Verification

**Component:** The **FTP** server **IP** address shown in the **FTP Server Configuration Menu** window.

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

**Test:** On the Linux 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.

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.

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

**Test:** On the Linux platform, execute the `ps -ef|grep sshd` command. See Linux **MAN** pages for help with `ps` command.

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

On the Windows platform, use 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 and the FTP/ **SFTP** server shown in the **FTP Server Configuration Menu** window.

On an EAGLE terminal, enter the `pass:loc=xxxx:cmd="ping yy.yy.yy.yy"` command, where `xxxx` is location of the service module associated with the **IP** address entered in the **STP Connection Configuration Menu** window, and `yy.yy.yy.yy` is the **IP** address of the FTP/**SFTP** server shown in the **FTP Server Configuration Menu** window.

**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 and FTP/**SFTP** server shown in the **FTP Server Configuration Menu** window.

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 shown in the **STP Connection Configuration Menu** window.

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 supported network statistics.

At the EAGLE, enter the `pass:loc=xxxx:cmd="netstat -p tcp"` command at the EAGLE terminal, where `xxxx` is location of the service module associated with the **IP** address entered in the **STP Connection Configuration Menu** window, 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 such as:

- 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 2-10, fix the network problems and retry the connection.

**Table 2-10 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, see *SSH, the Secure Shell: The Definitive Guide*, First Edition, Barrett and Silverman, O'Reilly, February 2001.

# 3
# Glossary

**B**

- BAT
  Batch Server

  Message distribution application that can send the same short message to multiple recipients.

**C**

- CSV
  Comma-separated values

  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 daemon 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 uses this feature to determine to which service database to send the query message when a Message Signaling Unit (MSU) enters the system.

**F**

- 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.

  Feature Test Plan
- FTRA
  FTP-based Table Retrieve Application

  An application that runs in a PC outside of the EAGLE and communicates with the EAGLE 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 uses to determine which service database to send the query message when an MSU enters the EAGLE 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**

- IETF
  Internet Engineering Task Force

  The Internet Engineering Task Force is an open international community of network designers, professional users, and manufacturers who promote the development and operations of the Internet.

- IP
  Intelligent Peripheral

  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 either a number in dotted decimal notation which looks something like (IPv4), or a 128-bit hexadecimal string such as (IPv6).

**M**

- MAC
  Media Access Control Address

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

- MAN
  Manual

**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) 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).

**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
  Ready to Test

  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 IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.
- STP
  Signal Transfer Point

  The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.

  Spanning Tree Protocol

**T**

- TCP
  Transfer-Cluster-Prohibited

  Transfer Control Protocol

  Transmission Control Protocol

  A connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner.
- TCP/IP
  Transmission Control Protocol/Internet Protocol