

**SSH Transmission Guide**

October 2011

**Table of Contents**

[1 Overview 3](#_Toc307937554)

[1.1 General Requirements 3](#_Toc307937555)

[1.2 Setup Process 4](#_Toc307937556)

[2 Technical Overview 5](#_Toc307937557)

[2.1 Authentication 5](#_Toc307937558)

[2.1.1 Inbound Authentication 5](#_Toc307937559)

[2.1.2 Outbound Authentication 5](#_Toc307937560)

[2.2 File Transfer 6](#_Toc307937561)

[2.2.1 Input Files 6](#_Toc307937562)

[2.2.1.1 File Transfer Options 7](#_Toc307937563)

[2.2.1.2 Input File Naming Conventions 7](#_Toc307937564)

[2.2.1.3 Confirm Files (Input File Receipt Confirmation) 8](#_Toc307937565)

[2.2.1.4 SITEEXIT Command 8](#_Toc307937566)

[2.2.2 Output Files 9](#_Toc307937567)

[2.2.3 PUT & GET Commands 9](#_Toc307937568)

[2.2.3.1 PUT Command 9](#_Toc307937569)

[2.2.3.2 GET Command 9](#_Toc307937570)

[2.2.4 Supported SSH Commands 10](#_Toc307937571)

[2.2.5 Unsupported SSH Commands 10](#_Toc307937572)

[2.2.6 Unsupported SSH Features 10](#_Toc307937573)

[2.3 URLs and IP Addresses 10](#_Toc307937574)

[2.4 Userids and Passwords 11](#_Toc307937575)

[2.4.1 Password Guidelines 11](#_Toc307937576)

[3 Appendix A – Confirms 12](#_Toc307937577)

[3.1 Example 1 – ‘Accepted’ Confirm file 12](#_Toc307937578)

[3.2 Example 2 – ‘Rejected’ Confirm file 12](#_Toc307937579)

[4 Appendix B - Confirm Reject Messages 13](#_Toc307937580)

[5 Technical Assistance 15](#_Toc307937581)

# Overview

Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The two major versions of the protocol are referred to as SSH1 and SSH2. SSH1 is not considered as secure as SSH2 and thus only SSH2 is supported by DTCC.

DTCC offers inbound and outbound SSH file transfer to customers via a dedicated SMART circuit, BT Radianz, SFTI, and over the Internet.

The SMART network is a private DTCC network. BT Radianz and SFTI are both vender networks that allow managed connectivity into DTCC.

Userid/password and public key authentication are used for both inbound and outbound SSH connectivity.

SSH provides security for a file during transmission only. This protection is different from file-level encryption (such as PGP), which protects the file before, during, and after transmission, until the file is decrypted.

Please review your company’s policy regarding the use of SSH for the transmission of files containing sensitive information.

## General Requirements

Firms are required to have technical staff that is familiar with SSH, firewall setups, network issues, and general network/systems connectivity matters. In order to support SSH, the firm and its technical staff will need to address the following topics, among other issues:

* **SSH Software and Operating Systems**
* Procure the appropriate SSH software, which is dependent on the firm’s operating systems. The SSH software must support SSH2.
* **SSH Server/Port specification**
* Firms must provide the IP address and port associated with their SSH server(s). Unless otherwise specified, well-known port 22 is used for SSH.
* **Public Key Fingerprint**
* Exchange the SSH server’s public key fingerprint for initial connectivity verification.
* **Naming Conventions**
* The appropriate file naming conventions must be followed. Technical staff must be able to create and name files accordingly
* **File Transfer commands**
* Transfer of files is initiated through a GUI or a number of technical commands. Technical staff must be able to use the GUI-based software and/or technical commands.

All other requirements are discussed in the Technical Overview section of this document.

## Setup Process

The general steps for setting up connectivity are:

1. DTCC will provide either a Network Information Exchange form or a firewall form to begin the connectivity setup process. The Network Information Exchange forms are specific to each managed network and the firewall forms are used for Internet connectivity. The specific Network Information Exchange forms are the SMART Router Exchange form, the BT Radianz Network Information form, and the SFTI Network Information form.
2. The customer should complete the appropriate form and return it to DTCC. If the customer has forms that should be used - those forms should be submitted to DTCC for completion.
3. Form processing includes:
	1. Configuring DTCC routers and/or firewalls with the specified IP addresses and ports.
	2. Configuring data delivery application(s) with IP addresses and ports, as necessary.
	3. For connectivity inbound to DTCC, DTCC will:
		1. Create a userid and initial temporary passwords.
		2. Create and assign the appropriate directories.
		3. Assign data passwords – as necessary.
		4. Enable the appropriate functions and security rights necessary for file access.
	4. For connectivity outbound from DTCC, the customer should:
		1. Assign a userid and password.
		2. Assign and permission the appropriate directories.
4. The customer should ensure that they are using compatible SSH2 software.
5. The customer should make sure to:
	1. Discuss any platform-specific requirements. For example, a Linux platform that has line termination requirements (e.g. line feed versus carriage return line feed).
	2. Advise of multi-platform transfers. For example, a file is created on a Windows system then transferred to a UNIX platform for final transfer to DTCC.
	3. Discuss any issue that may affect transfer.
6. DTCC will review the file layouts, naming conventions and command information with the customer.
7. Testing will be conducted to confirm connectivity and data delivery. The testing should include any public key / fingerprint testing.

The following sections provide a technical overview to assist with implementing SSH.

# Technical Overview

## Authentication

SSH Secure Shell provides mutual authentication - the client authenticates the server and the server authenticates the client. The capability exists to assure the identity of each party.

DTCC supports two types of SSH authentication:

1. Userid and password.
2. Public key fingerprint verification.

For connectivity inbound to DTCC – both userid/password and public key authentication are used for each connection.

Using a public key for authentication is more secure than just using a complex password. DTCC does not store the public key itself. Instead, the fingerprint to the public key is used for authentication and is stored for future use. Not all SSH client programs support the public key authentication method. Consult your SSH program documentation for details.

DTCC requires all keys to be SSH2 keys (RSA or DSA) and 1024 bits or higher. Other types of keys are not supported.

When connecting to DTCC for the first time, your SSH client will either perform the host key/fingerprint verification automatically or prompt for manual verification. Best practices indicate that initial SSH connections should be manually verified.

When DTCC connects to your server for the first time, the public key/fingerprint verification is done manually for Internet connectivity only.

Key/fingerprint verification will need to be done again if using a different server or if SSH is reinstalled on the same server.

### Inbound Authentication

For inbound connectivity to DTCC, DTCC will provide either the fingerprint to the SSH server’s public key or, if requested, the public key itself. The first login to the server should be set to prompt whether to accept the DTCC SSH host key. Again, it is suggested that the public key/fingerprint be manually verified the first time the systems connect. In addition, it is suggested that the public key/fingerprint be manually re-verified if the server changes or SSH is reloaded. After the first connection, the local copy of the server's public key/fingerprint will be used in server authentication.

### Outbound Authentication

For outbound Internet connectivity from DTCC, DTCC should be given a copy of the fingerprint to your SSH server’s public key.

The fingerprint will then be verified at the initial connection and at any time when the server’s IP address changes, or the SSH software is reloaded. After the first connection, the local copy of the server's public key/fingerprint will be used in server authentication.

For connectivity over any of the dedicated networks (SMART, SFTI, and BT Radianz) DTCC will automatically accept and store the fingerprint provided at connectivity.

## File Transfer

An SSH client program is necessary to perform SSH transmissions. DTCC does not provide this client program; however, many SSH client programs are available. The simplest version, a command-line SSH program, is available on most Unix/Linux operating systems.

Many of the GUI-based FTP programs for Windows can also be used for SSH. Among them, WS FTP Professional and CUTE FTP Professional are the most popular.

In-house programs or scripts may also be used - using any of the programming languages that support SSH.

It is essential that users understand the interaction between the ***put*** and ***get*** commands within this process. Firms must initiate a PUT and GET command when sending in data or trying to retrieve data.

Files are sent in to DTCC using a PUT command or its equivalent - depending on the software used. DTCC does not pick up files from the customer’s server.

Confirm files and output files can either be retrieved using a GET command for a file in a specified directory (Pull); or, they can be transmitted from DTCC to a designated directory on the customer’s server (Push).

Files for pickup from the DTCC server are retained for seven (7) days.

For connectivity inbound into DTCC, DTCC will provide the appropriate input, output, and confirm directories. For outbound connectivity the customer should similar directories.

### Input Files

All input files are transmitted to DTCC. DTCC does not retrieve files from the customer’s server. Each application has a unique number called a SYSID (system identifier) assigned to it. Input that is transmitted to DTCC is associated to its appropriate application by the SYSID.

The Expected Master file contains a record for every SYSID and Broker submitting data. It also contains various control information, approximate number of records expected, and acceptable ranges.

Firms thru their Relationship Managers make requests to submit data to a specific SYSID. Once that request has been received and processed, an originator and sub-originator number are assigned and are to be used in the header record by the firm.

Input files can only be sent to your assigned input directory. Input files have a specific naming convention that must be followed.

The following important file transfer topics are discussed in the sections that follow:

* Files transfer options
* Input file naming conventions
* Confirm files (input file receipt acknowledgement)
* Site commands

#### File Transfer Options

When sending a file to DTCC the two (2) most common file transfer options are the *transfer mode* and *file/record size* characteristics. DTCC will provide the customer with any file and/or record size characteristics for each input SYSID.

File transfer options are set using an ***ls*** request. Its usage is in the form: ***ls /+<name=value>***. Where <name=value> is the requested option.

Example 1: to initiate a text mode transfer the command would be: ***ls / +mode=text.***

Example 2: to initiate a transfer using file/record size characteristics received from DTCC: ***ls /+lrecl=80***

File transfer options can be cleared using the form: ***ls /+NO<name>***.

To specify multiple file transfer options – separate the <name=value> pairs with commas.

Example 3: ***ls /+mode=text,lrecl=80*** (combined from examples 1 and 2 above).

An error is returned if one or more of the options were incorrectly specified, however, any remaining correctly specified options are set as requested.

#### Input File Naming Conventions

Input files transmitted should contain a header record and possibly a trailer record. The header and trailer records will have the following formats found at this link:

<http://www.dtcc.com/products/documentation/cs/formats_masterfiles.php>

Upon completion of the input file transmission, the system dynamically allocates a 44 character file name by appending a date/time stamp to make the file name unique.

Sample filenames:

Production DTSFTP.C1234.S01125

 Internet Production Upload DTS3.UP.C1234.S01125

 Internet Production Download DTS3.DOWN ….

Test DTSUTF.C1234.S01125

 Internet Test Upload DTS4.UP.C1234.S01125

 Internet Test Download DTS3.DOWN ….

#### Confirm Files (Input File Receipt Confirmation)

Once the input file is received the transmission header and trailer records are compared to a master file for validation of specific fields. The results of that comparison are placed in a file called a ***confirm file.*** The results indicate whether the file has been accepted or rejected. If the file is rejected, the data is not passed to the application for processing and the appropriate error is placed in the confirm file. For example:

* The system is expecting a certain date in the header. If that date is incorrect the data will be rejected.
* The system detects a duplicate transmission based on the information received in the header.

Please see Appendix A for examples of the confirm file. Appendix B contains a list of reject codes.

***Confirm files only refer to the status of the file transfer and are not an indication of any processing done on the data that was sent.***

Based on the customer’s output requirements gathered by the connectivity group, the confirm file will either be transmitted back to the sender or placed in a designated confirm directory for pickup.

When DTCC is to transmit the confirm file back to the sender, a file name should be provided in which to write the confirm data.

The use of the SITEEXIT command allows for more control over how confirm files are processed.

#### SITEEXIT Command

Default processing returns a confirmation file to the customer using a programmatic lookup of predefined return parameters. The customer may customize the confirm process by using the **SITEEXIT** command.

***Please discuss the use of the SITEEXIT command with DTCC so that default confirm processing can be turned off.***

Use of the **SITEEXIT** command is a way to set certain server confirmation file return options. In order to provide a method of passing additional data needed to return these confirmations to the client, several in-house extensions have been developed. These additional parameters are marked by the positional parameter **FTPCNTL** as the first argument to the **SITEEXIT** command. This is followed by any or all of the keywords below, in any order, separated by blanks. Each value persists until changed by a subsequent **SITEEXIT FTPCNTL** command. If any of the following 4 return parameters is specified, all are used. Re-specifying a parameter with a null value resets it as if it were never specified.

ls /+siteexit=”ftpcntl **ra**=123.456.789.035 **ru**=serveruserid **rp**=serverpasswd **rd**=serverfilename

**RA=***return IP address* IP address of the customer’s DTCC-registered server to receive the confirmation

 Maximum length: 32 characters

 Default: **\*NORA\***

**RU=***return user* Userid for login to the above server

 Maximum length: 16 characters

 Default: **\*NORU\***

**RP=***return password* Password for the above userid login

 Maximum length: 16 characters

 Default: **\*NORP\***

**RD=***return data file name* Name of the confirmation file to be created at the customer’s site

 Maximum length: 64 characters

 Default: **\*NORD\***

### Output Files

Output files are files that are created as a result of application processing. Generally, all output files are subscribed to by the receiver. DTCC will either place the file in a specified directory for pickup; or, transmit the file to a designated server/directory.

CDTS is an internally developed system that distributes output to participants. The system is also used to monitor the status of output and facilitates the re-transmission of data to participants.

Each output file will have a header associated with it unless the customer has requested no headers. The header can be found at the following link:

<http://www.dtcc.com/products/documentation/cs/nscc_formats/2468700000000_autoroute_header_8digit.pdf>

There are many output options available to the customer. Please ensure that you discuss any file output requirements during the connectivity or the data delivery process.

### PUT & GET Commands

The following commands are used for the actual file transfer process.

Transaction files may be uploaded using the PUT command. Output files may downloaded using a GET command.

#### PUT Command

The **PUT** command submits a file to DTCC.

The following sequence will PUT a fixed block text file at 300 bytes per record:

 Change to DTCC-assigned directory ***cd //dtsutf.c1234***

 List contents of directory, if desired ***ls //dtsutf.c1234***

 Set transfer mode & file characteristics ***ls /+recfm=fb,mode=text,lrecl=300***

PUT input SYSID (file) to directory ***put c:\myfile //dtsutf.c1234.s12345***

#### GET Command

The **GET** command is used to retrieve output and/or confirm files.

Change to DTCC-assigned directory **cd //artdialu.d3346**

List contents of directory **ls //artdialu.d3346**

Set transfer mode & file characteristics ***ls /+recfm=fb,mode=text,lrecl=300***

PUT input SYSID (file) to directory **get //artdialu.d3346.p0298.p0211.d120311.c01 c:/myfile**

When a file is retrieved, a date and cycle number may be appended to the name of the file. For example, “D120311.C01” is appended for the date of 12/03/2011 and cycle 01.

### Supported SSH Commands

**Command Definition**

* PUT put a file to a directory
* GET retrieve a file from a directory
* CD change to an predetermined directory
* LS list directory

### Unsupported SSH Commands

**Command Definition**

* MKDIR make directory
* RMDIR remove directory
* CHMOD change file mode
* CHOWN change file owner
* APPEND put (upload) a file, append to an existing file
* DELETE delete a file
* RENAME rename a file

### Unsupported SSH Features

DTCC only supports the SFTP subsystem of the SSH protocol suite. All other SSH features are disabled.

Unsupported features include, but are not limited to, the following:

**Command Definition**

* SSH1 The entire SSH1 protocol suite is not supported
* Rhost authentication login based on host names
* Kerberos authentication
* Remote Shell Login
* SCP Secure file copy
* TCP and X11 Forward

## URLs and IP Addresses

The DTCC destination IP/URLs and port information that the firm will need include:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System** | **Port** | **SMART** | **BT Radianz** | **SFTI** | **Internet** |
| SSH Prod | 22 | 167.188.68.101 | 167.188.168.101 | 167.188.134.101 |  |
| SSH Test | 22 | 167.188.69.93 | 167.188.169.93 | 167.188.137.93 |  |
| SSH Internet - Prod | 22 |  |  |  | 207.45.41.162 fdmovers.dtcc.com |
| SSH Internet – Test | 22 |  |  |  | 207.45.41.159 fdmoverspse.dtcc.com |

Please note that Internet access has different IP addresses and URLs than non-Internet connectivity.

## Userids and Passwords

The DTCC assigned userid is used during the sign-on procedure. The associated initial password must be changed the first time the system. The initial password will expire if it’s not used within 30 days.

Passwords will expire every 90 days unless changed. Users have the option of changing the password at any time before this 90 day cycle.

### Password Guidelines

The following password guidelines apply to DTCC-issued passwords:

* There must be at least six and not more than eight characters, with no spaces.
* The first four characters must be different alpha characters (non-repeating).
* There must be at least two non-repeating numbers.

# Appendix A – Confirms

## Example 1 – ‘Accepted’ Confirm file

The confirm file received from DTCC will be in the following format:

DTS053C0 RUN DATE 10/01/11 DATATRAK SYSTEM PAGE 001

 RUN TIME 12:53:32

 INPUT PROGRAM TRANSMISSION STATUS REPORT

 STATUS - INPUT RECEIVED BY DTCC'S DATATRAK SYSTEM

 DETAIL RECORDS RECEIVED 22

 HEADER RECORD RECEIVED

 HDR.Saaaaa.E00.Cbbbb.Scccc10072011Example Confirm file AT 04:23:02 \*

 **ACCEPTED**

## Example 2 – ‘Rejected’ Confirm file

DTS053C0 RUN DATE 10/01/11 DATATRAK SYSTEM PAGE 001

 RUN TIME 13:35:08

 INPUT PROGRAM TRANSMISSION STATUS REPORT

 STATUS - INPUT RECEIVED BY DTCC'S DATATRAK SYSTEM

 DETAIL RECORDS RECEIVED 0

 HEADER RECORD RECEIVED

 HDR.Saaaaa.E00.Cbbbb.Scccc10102011 N002

 **REJECTED**

 **NO MATCH ON EXPECTED MASTER FOR HEADER**

# Appendix B - Confirm Reject Messages

|  |
| --- |
| The following explains the reject messages that may appear in the confirmation file. |
| **REJECT MESSAGES** | **EXPLANATION** |
| 8 digits header date but indicator is NO | The file was set-up for a 6-digit header date and the file contained an 8-digit header date. |
| Block Size of Input Does Not Agree With Pre-Edit File | A file was submitted with an incorrect block size. |
| Broker No. in Detail Record Invalid | One or more FIELDS in the detail records is invalid (for example: non-numeric). The file may be accepted, but these records will not process successfully. |
| Broker No. in Detail Record Not on Expected Master | **Service Bureaus only**. You have submitted for a broker that is not on our expected master file. |
| Detail input record failed pre-edit check | A file was submitted that does not meet the DataTrak pre-edit verification criteria. |
| End Exp Different Than Header | The End Record (DataTrak Trailer Record) has different information than the Header Record. |
| End No End Found | No End Record was found. |
| End Not Exp Different From Header | An End Record was found, but not expected, and it is different from the Header Record. |
| End Not Last Record in Batch | A file was submitted where the end record was not the last record in the file. |
| End Not on Expected Master | DataTrak has found, but is not expecting, an End Record in your file. |
| End record count submitted by broker mismatch | DataTrak has detected a possible record count out of balance with the file. |
| Header Fields Incorrect | An error has been found with the record layout of your DataTrak header record. |
| Header record on active input file - Cannot assume record length of 80 | A file was submitted with a record length that does not match with our pre-edit file |
| Input Date Does Not Match Today's Date | A file was submitted with an incorrect date in the DataTrak header record. |
| Input has no records | The firm was not set-up on the DataTrak masterfile to submit a file for this SYSID with zero records. |
| Input Record Failed Pre-Edit or Literal Check | The structural validation of the file by DataTrak has found format errors in your data. |
| Missing Header Record | All incoming files require a DataTrak header record. This header record acts as control for the entire process. It identifies the data being submitted |
| No match on expected masterfile for header | The firm is not set-up on the DataTrak masterfile to submit a file under this SYSID. |
| No SYSID Match on Pre-Edit | The System Identifier (SYSID) was not recognized by DATATRAK. |
| **WARNING/ REJECT MESSAGES** | **EXPLANATION** |
| Pre-edit process date not numeric change file and re-submit | A file was submitted with a processing date on the DataTrak header that was non numeric. |
| Prior Submission | The firm is set-up to send in one file a day. DataTrak has already received a transmission from your firm for this SYSID today, but it was rejected. |
| Prior Submission and Dupe Input | The firm has already submitted (and DataTrak has accepted) the same number of data records under this SYSID today. |
| Prior Submission and Possible Dupe Input | The firm is set-up to send in one file a day. A file was already submitted for this SYSID today. The first file sent was accepted for processing. The number of records in the second file does not match the first. |
| Record Length from JCL Does Not Agree with Pre-Edit File | A file was submitted with an incorrect record length. |
| REJ Input Needed | The Input file lacks input data records. |
| Reject - batch number too high | A file was submitted with batch indicator # greater than the number expected. |
| Reject - batch number too low | A file was submitted with batch indicator # less than your previous file. |
| Reject - batch received after lbi | A file was submitted after a last batch indictor was received in a previous file. |
| Reject - Broker count mismatch | A file was submitted with an end record that does not equal the total number of records submitted |
| Reject - Last batch sequence error | The file contained a character in the Last Batch Indicator field in your DataTrak Header Record (column 60) which was neither an "N" nor "Y". |
| Reject- batch not numeric | A file was submitted with a non-numeric multi-batch indicator. |
| Rej-Fix Exp; Var\* Missing | DataTrak expected a fixed-format input file, but the input file sent was actually in variable format, and the Header Record did not contain "\*" in column 65 as required for variable files. |
| Rej-Fixed Exp; Var Actual | DataTrak expected a fixed-format input file, but the input file sent was actually in variable format. |
| Rej-Var Exp; Var \* Missing | DataTrak expected a variable-format input file, but the Header Record did not contain "\*" in column 65, as required for variable files. |
| Rej-Var Exp; Fixed Actual | DataTrak expected a variable-format input file, but the input file sent was actually in fixed format. |

# Technical Assistance

|  |  |  |
| --- | --- | --- |
| **Support Team** | **Phone** | **Used for…** |
| Business and Technical Support | 888-382-2721 option 5,4 | Initial connectivity and data delivery |
| Enterprise Service Center (ESC) | 888-382-2721 option 5,1 | Daily Production file transmission support |
| Customer Support Center (CSC) | 888-382-2721 option 1,3212-855-8099 option 1,3 | Userid/password issues, General help desk questions |