Canada Savings Bonds Program

FTP Server
User Guide

Version 2.5

September 1, 2015

FTPS Server User Guide – Revision History

Use the following table to track the revision history for this document. Please ensure that the date, phase and contact information are provided so that questions regarding the content may be directed to the appropriate individual.

Revision Date	Phase	Reason	Ver.
May 9, 2007		Draft	1.0
May 24, 2007		Second Draft	1.1
September 11, 2007		Final	1.2
October 22, 2007		Added contact information, modified file name and document title. Added a Preface to summarize details to be provided at implementation.	1.3
January 31, 2008		Replacement of temporary snapshots	1.4
February 19, 2008		Added a note on configuration of organization's firewall.	1.5
March 18, 2008		Expanded the accepted data file naming standard (section 5.1.3) to support an alphanumeric sequence number of any length.	1.6
March 24, 2008		Changed the recommended file transfer mode.	1.7
April 15, 2008		Added a File Confirmation step for Processing Agents in Section 3.3 . Removed references to FundServ.	1.8
May 21, 2008		Added support for explicit mode.	1.9
July 6, 2009		Updated 5.1.3 Data File Naming to separate the explanation for the sequence numbering for payroll contribution files and purchase files as requirements are not the same. And to update links to documentation on CSB website.	2.0
May 11, 2010		Changed RPAC-PFT email address from EDS to csb.gc.ca, changed campaign period from 6 to 2 months and changed EDS to HP.	2.1
April 19, 2013		Changed Processing Agents contact information on preface page.	2.2

May 12, 2014		Changed contact information on preface page. Remove the wording: The format of the data contents has not changed with the migration to FTPS from page 17.	2.3
August 5, 2014		Review	2.4
August 28, 2015		Review	2.5

TABLE OF CONTENTS

TRADEMARKS

GLOSSARY OF ACRONYMS

API	Application Programmer's Interface
ASCII	American Standard Code for Information Interchange
BOC	Bank of Canada
CA	Computer Associates
CD	Compact Disk
CPB	Canada Premium Bond
CPU	Central Processing Unit
CSB	Canada Savings Bond
DB	Database
HP	Hewlett Packard
EMC	EMC Corporation
FTP	File Transfer Protocol
FTPS	FTP over SSL
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
I/O	Input / Output
MFC	Microsoft Foundation Class library
N/A	Not Applicable
OS	Operating System
RDMS	Retail Debt Management System
RDO	Retail Debt Operation
SDK	Software Development Kit
SPOC	Secure Posting Of Contribution and other files
TLS	Transport Layer Security

PREFACE

This document describes the implementation of the Bank of Canada's secure FTPS solution.

CONTACT INFORMATION

Organizations transmitting **payroll contribution files**

- Please call Payroll Savings Program Customer Service at 1 877 899-3599 Monday to Friday, 8 am to 6 pm, Eastern Time.

Processing Agents transmitting Canada Savings Bond **purchase files**

- Please call 1 800 575-5151 Monday to Friday, 8 am to 8 pm, Eastern Time.

1. INTRODUCTION

1.1. Purpose

This document is a guide that can be used by organizations using the FTPS server to upload data files (such as purchase and payroll contribution files). It is intended for a fairly technical audience that is already familiar with FTP and is already aware of the files to be uploaded (see references in section 1.5 'Referenced Documents').

1.2. Scope of this Document

This document provides the technical information required to use the FTPS system. It is not intended to document the business processes related to the FTPS system. It is intended to complement, not replace, the file specifications referenced in section 1.5 'Referenced Documents'.

1.3. Background

The FTPS system supports two types of data file uploads:

- Processing Agent organizations transmit files containing details of bond purchases made by the general public. These purchase files are received during the Canada Savings Bond sales campaign.
- Employer organizations transmit files containing employee contribution details for non-certificated purchases taking place through payroll deduction. Payroll contribution files are transmitted on a regular basis, such as weekly or every two weeks, to coincide with employer payroll cycles.
- In both cases above, the data is classified Protected B[1] and as such special measures are needed to ensure the data is transmitted and handled securely.

1.4. Organization of This Document

Section 1 Introduction. This section describes the purpose, scope and organization of this document. This section also identifies all documents referenced within this document.

[1] "Protected B" (particularly sensitive) is a Government of Canada designation that applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest and often include information, which if released, would reasonably compromise individual privacy e.g., loss of reputation or competitive advantage.

Section 2 Overview. This section provides an overview of the network architecture and the security features of the FTPS system.

Section 3 Using a FTPS Client GUI. This section provides instructions to users wishing to use the FTPS system through a GUI-based client software.

Section 4 Using a FTPS Client API. This section provides instructions to users wishing to use the FTPS system through a custom-built client software.

Section 5 Upload File Specifications. This section provides or references the specifications of the files that may be uploaded through the FTPS system.

1.5. Referenced Documents

The following documents are referenced within, or have been used in the preparation of this deliverable.

Technical Specifications for Proprietary Payroll System Users

http://www.csb.gc.ca/wp-content/uploads/2009/02/s3conv-technicalspecifications.pdf

Retail Debt Management System (RDMS) Purchase File Specifications

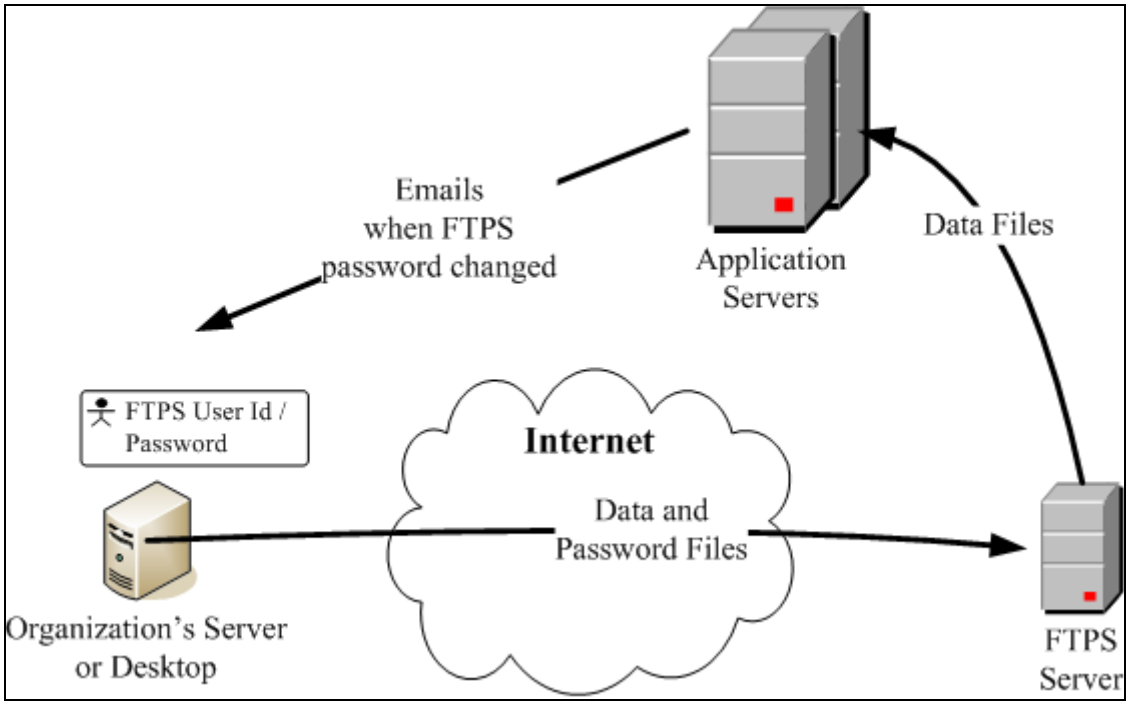
http://csb.gc.ca/fis/selling-and-processing-s42/?language=en

2. OVERVIEW

This section provides an overview of the network architecture and the security features of the FTPS system.

2.1. Network Architecture

The following diagram shows the network architecture of the FTPS system. An organization uses the public Internet to connect to the FTPS server and upload data and password files.



Organizations that use a firewall that restricts outgoing connections must configure their firewalls to allow outgoing connections to IP address 204.104.133.46 (csb-oec.bpmca.com) on ports 990 and 23001 to 23100 if using "implicit" mode, or ports 21021 and 23001 to 23100 if using "explicit" mode.

2.2. Steps for Using FTPS

The following are the basic steps that are followed to use the FTPS system. More details on these steps are provided in the following sections of this document:

1. Establish a connection to the Internet.

2. Connect to the FTPS server. In this step, the user has two options (for either option, data encryption must be enabled):

a. Implicit mode with passive connection type. This option must use port 990.

b. Explicit mode with passive connection type. This option must use port 21021.

3. Login to the FTPS server using the user id assigned to the organization and by entering the organization's secret password.

4. If prompted, accept the FTPS server's certificate.

5. Set the transfer mode to ASCII or binary. On the first attempt to use the FTPS server with a test file, users should use ASCII; if this mode is not successful (which may happen if the file contains special characters) then binary should be used.

6. Repeat the following step as many times as required:

    a. Upload a data file or a password file (the password file is used to change the organization's secret password).

7. Close the FTPS connection.

2.3. Security

The data files uploaded through the FTPS system are not encrypted before being transmitted but are protected by the following measures:

- Files are transmitted using FTP with TLS, which ensures that the files are encrypted while in transit.
- An organization is allowed and encouraged to change their password frequently. At a minimum, it is recommended that your password be changed quarterly (every 3 months).
- Once an organization changes its password, that password is known only to the organization. Our Customer Service Representatives cannot view your password.
- By enforcing stringent criteria for its passwords, the FTPS server ensures that only strong passwords are used (see section 5.2.1 'Password File Contents' for a description of the criteria).
- Users of the FTPS server have upload capability but no download, delete, list, or rename capability.
- The FTPS system verifies the data in the data files against the user id of the sending organization. A data file is accepted only if it contains data that the organization is permitted to submit (see sections 5.1.1 'Payroll Contribution Data File Contents' and 5.1.2 'Purchase Data File Contents' for more details).

3. USING A FTPS CLIENT GUI

This section provides instructions to users wishing to use the FTPS system through a GUI-based client software.

3.1. Suggested FTPS Client GUIs

Organizations may use any FTPS client GUI software since the FTPS solution is standards based and not reliant on a specific vendor.

Note: These suggested products may be used, but have not been tested by the Bank of Canada.

- edtFTPj/PRO (http://www.enterprisedt.com/products/edtftpjssl/overview.html). This is Java-based GUI usable on any platform that supports Java 1.5.x or above.
- WS_FTP Professional (http://www.ipswitchft.com/ws-ftp-client).
- This product can be used on Windows platforms.jMethods JFTP (http://www.jmethods.com). This is Java-based GUI usable on any platform that supports Java 1.4.2 or above.
- FTP Voyager (http://www.serv-u.com/ftpvoyager This product can be used on Windows platforms.
- FileZilla https://filezilla-project.org/

3.2. Steps to Upload a File

The following are the standard steps expected to be used to upload a file to the FTPS server. The screenshots provided in this section are an example of the use of a FTP client GUI.

Note:

- If your organization uses a proxy server, set the proxy server's parameters in FTP client GUI.
- Organizations that use a firewall that restricts outgoing connections must configure their firewalls to allow outgoing connections to IP address 204.104.133.46 (csb-oec.bpmca.com) on ports 990 and 23001 to 23100 if using "implicit" mode, or ports 21021 and 23001 to 23100 if using "explicit" mode.

1. Start the client GUI, and connect using the following information:

- Host name: csb-oec.bpmca.com or 204.104.133.46.
- User Name: your organization's user id (which is "ftp" followed by your Organization Id number).
- Password: enter your FTP secure password (initial password received via email or the new password that you set).
- Security Mode: two options should be available, and both are valid:
"Implicit" option: Select "Implicit TLS" (port should change to 990)
"Explicit" option: Select "Explicit TLS" (port should change to 21 but you must change it to 21021)

- Data Encryption: Must be enabled.
- Connection Type: Must be "passive".

2. When you attempt to connect, you will probably be asked to accept the certificate. Please accept.

3. Set the transfer mode (should be ASCII).

4. Upload your production file.

Note: The file will not appear in the file listing even though it was successfully uploaded. The content of the server folder is blocked due to security requirements.

5. Disconnect from the FTPS server.

Note: File confirmation (for Processing Agents transmitting Canada Savings Bond purchase files only). Processing Agents must provide advanced notice prior to submitting a purchase file. This can be done by sending an e-mail with the file information to rpac-pft@csb.gc.ca. When the file is received and processed, a reply will be sent to the submitting organization. This confirmation should be received within 24 hours of processing. If not, please e-mail rpac-pft@csb.gc.ca for follow-up.

4. USING A FTPS CLIENT API

This section provides instructions to users wishing to use the FTPS system through custom-built client software.

4.1. Suggested FTPS Client API

Organizations may also use any FTPS client API software since the FTPS solution is standards based and not reliant on a specific vendor.

Note: These suggested products may be used, but have not been tested by the Bank of Canada.

- edtFTPj/PRO (http://www.enterprisedt.com/products/edtftpjssl/overview.html).
- WS_FTP Professional SDK (http://www.ipswitchft.com/ws-ftp-client).
- Secure FTP Factory (http://www.jscape.com/products/components/java/secure-ftp-factory/).
- jMethods Secure FTP API for Java (http://www.jmethods.com/secure-ftp-api-for-java).

4.2. Data Files

4.2.1. Payroll Contribution Data File Contents

For specifications of the contents of the payroll contribution data files, please see Technical Specification Guide http://www.csb.gc.ca/wp-content/uploads/2009/02/s3conv-technicalspecifications.pdf

The format of the data contents has not changed with the migration to FTPS.

The FTPS server performs the following validations on the data file before accepting it:

- The transmitter's Organization Id that appears in the transmission header record (record type 10) and in the transmission trailer record (record type 90) must correspond to the FTPS user id that is uploading the file.
- The transmitter's Organization Id that appears in the transmission header record (record type 10) and in the transmission trailer record (record type 90) must correspond to the Organization Id that appears in the file name (see section 4.2.3 'Data File Naming').

- The transmitter's Organization Id must be permitted to submit records on behalf of each Organization Id that appears within a batch header record (record type 20), a batch detail record (record types 30, 40, or 50), and a batch trailer record (record type 80).

4.2.2. CSB Purchase Data File Contents

For specifications of the contents of the purchase data files, please see the "Retail Debt Management System (RDMS) Purchase File Specifications Logical Record Standards and the RDMS Purchase File Specifications Data Element Dictionary" located on the CSB Website at the following address: http://csb.gc.ca/fis/selling-and-processing-s42/?language=en . The FTPS server performs the following validation on the data file before accepting it:

- The user id that uploaded the file must be defined in the FTPS server as a user of type "purchase agent"; otherwise, the file is not processed.

- The Organization Id that appears in the header record (record type A) and in the trailer record (record type Z) must be the same as the Organization Id that appears in the file name (see section 5.1.3 'Data File Naming'); otherwise, the file is not processed.

4.2.3. Data File Naming

A data file name (for payroll contribution data files and purchase data files) must be as follows (the data file naming convention has not changed with the migration to FTPS):

`xxxxxnnn.##T` *(not case sensitive) for testing*

`xxxxxnnn.##P` *(not case sensitive) for production*

Where:

xxxxx	The Organization Id – this is Organization Id that appears in the data file header.
nnn	A sequence number of your choice. **Payroll contribution data files**: The sequence number must use alphanumeric characters only (A to Z, a to z, and 0 to 9) and can be of any length greater or equal to 1. This number can be used to meet the naming requirements of your organization, such as different payrolls, different paydays, etc. Note that if several payroll contribution files are sent on the same day, it is required that this number be unique for each file within that day.

	Purchase data files: The sequence number must use alphanumeric characters only (A to Z, a to z, and 0 to 9) and must be 3 characters. Sequence Numbers should be unique within a campaign period. It is advisable to increment with each transmission.
"##T" / "##P"	Use as is (not case sensitive). A file having an extension of "##P" will be processed normally. A file having an extension of "##T" will be processed as a test file.

Examples of valid **payroll contribution** data file names:

```
999991.##T

9999999999.##P

99999001.##T

99999999.##P
```

Examples of valid **purchase** data file names:

```
99999001.##T

99999999.##P

99999678.##T

00001999.##P

99999001.##T

99999999.##P
```

Examples of invalid file names:

`99999.##P`	(Sequence number is missing)
`99999999.P`	("##" is missing from the extension)
`99999001.###T`	(Too many "#" in the extension)
`99999  1.##T`	(Spaces not allowed)
`99999999.#P`	(Not enough "#" in the extension)
`99999001.TXT`	("TXT" is not an acceptable extension here)
`99999001##T`	(Period is missing)
`34599999.##P`	(Organization Id must be before sequence number)

Notes:

- A data file must strictly follow this naming convention to be considered valid and to be processed successfully.

- The original file stored in your environment is not required to have the same name as the file uploaded to the FTPS server. Our requirement for the file name format must contain the first 5 characters as your org id, and a sequential number to identify your file ending with the proper extension (example: ##p or ##t). For ease of reference the file uploaded should have the same name as the file you have stored on your system.

- We strongly recommend that you keep a copy of the file in your environment until you receive a confirmation of transmission receipt, and batch confirmation from the Bank of Canada.

4.3. Password Files

4.3.1. Password File Contents

We recommend that you change your password on a regular basis. The FTPS system allows you to modify your password by uploading a password file. The password file is expected to contain a single password (case sensitive). The password contained in the file will be your new password.

The FTPS server performs the following validations on the password before accepting it:

- The password must be ASCII character encoded text.

- The password must be at least 12 characters long but no more than 40 characters long.

- The password must contain at least one lower-case alphabetic character, one upper-case alphabetic character, and two numeric characters.

- The password must contain only a combination of the following characters: ‘a’ to ‘z’, ‘A’ to ‘Z’, and ‘0’ to ‘9’.

- The first eight characters of the password must contain at least one numeric character and two alphabetic characters.

- The password cannot be a circular shift of the user id (note that such a password would be invalid anyway because it would be only nine characters long and therefore too short).

- The new password must differ from the previous password and cannot be a reverse or circular shift of the previous password. For this comparison, uppercase letters and lowercase letters are considered to be equal.

- The new password must have at least three characters that are different from the old password. For this comparison, uppercase letters and lowercase letters are considered to be equal.

Examples of valid passwords:

```
Yc9rmnKr056

Fwh7RP86j5ycvt7x5XkuifLcyuxMz3
```

Examples of invalid passwords:

`ABCxyz123`	(less than 12 characters long)
`1933to1995ElizabethVictoriaMontgomeryWasBewitched`	(too long)
`ElizabethVictoriaMontgomery`	(no numeric characters)
`1933to1995elizabethmontgomery`	(no upper-case characters)
`1933TO1995EMONTGOMERY`	(no lower-case characters)
`ElizabethMontgomery1933to1995`	(no numeric characters in first 8 characters)
`33-95ElizabethMontgomery`	(special character '-' is not accepted)
`33 95 Elizabeth Montgomery`	(space is not accepted)

4.3.2. Password File Naming

A password file name must be "password_xxxxx.txt" (not case sensitive) where xxxxx equals the Organization Id of the FTPS User id that is uploading the file. If a password file uses any other name, it will not be processed as a password file.

Examples of valid password file names:

```
Password_99999.txt

PASSWORD_99999.TXT

password_99999.txt

Password_99999.TXT

PassWord_99999.TXT
```

Examples of invalid file names:

`PASSWORD_99999`	(extension is missing)
`PASSWORD_99999.DOC`	(extension must be "TXT")
`Pass word_99999.txt`	(space is not accepted)
`Password_99999-txt`	(dash is not accepted in place of period)
`OpenSesame_99999.txt`	("OpenSesame" must be changed to "password")
`PaSsWoRd.TxT`	(org id is missing)

Notes:

- A password file must strictly follow this naming convention to be considered valid and to be processed.
- The password change takes effect within a few minutes after a password file is uploaded. You will receive an email after the password change is attempted by the FTPS server; the email will state whether the change was successful or not.