BRITISH COLUMBIA

Ministry of Health

Secure File Transfer Protocol

User Guide

Date Created:	November 10, 2009
Date Updated:	November 12, 2013
Next Update:	
Version:	1.6

Approvals

Signature   Date

_____   _____

Director, DA&IM

Signature   Date

_____   _____

Manager, HDAS

Revision History

Date	Author	Version	Change Reference
Nov.2. 2009	Mike Botrakoff	1.0	Initial draft
Nov.12, 2009	GCorbett	1.1	Updated
Feb. 18, 2010	GStodola	1.1	Updated
Mar.4, 2010	DAS Analysts	1.2	Updated
Mar.25, 2010	MTownson/SOrr/MBotrakoff	1.3	Updated
May 6, 2010	Robyn Wood	1.4	Updated
Dec 2, 2011	Joe Jaffey	1.5	Updated
Feb 26, 2013	Bruce Stuart	1.6	Updated

Table of Contents

1 Overview

1.1 Purpose of this Document

This document has been written to support clients using this secure file transfer tool.

After reading this document, users will be able to use SFTP to:

- Submit and/or receive files securely to/from the Ministry and external user (person to person transfer); and
- If required, exchange files using automated computer-to-computer transfers.

1.2 Terms of Reference

SFTP or Secure File Transfer Protocol is a secure file transfer tool between a SFTP server and user, using a SFTP client or SFTP software. The file is encrypted during the transfer, but not while it is sitting on the server. Access is facilitated by utilizing a public/private key pair exchange between client and server and user ID and password. This system supports manual (person-to-person) transfers and automated (machine-to-machine) transfers. If automated transfers are required, the external party must also have an SFTP server and the servers involved in the transfer exchange public keys. In both situations, the Ministry of Health (MoH) SFTP Service Consultant must contact the external IT contact to complete the setup.

Personally Identifiable Data refers to information that would allow the identification of an individual by direct means, such as a PHN or SIN, or by a combination of information that would allow the deduction of the identity of an individual, such as gender, birth date and postal code.

Information Sharing Agreement (ISA) is a generic term referring to a document that describes and authorizes the sharing of data between two parties.

Data Access Agreement (DAA)/Schedule 20 refers to the documents that describe the framework for data access or data exchange between the Ministry and the Applicant and the conditions of their access.

1.3 A Summary of the Application Process

To initiate the process for obtaining SFTP, the Ministry business area contact fills out the Secure File Transfer request form located at https://gww.health.gov.bc.ca/forms/mailform_H7101.html

- ➢ The request is forwarded to their Director for approval
- ➢ Their Director approves it and forwards the form and their approval to the Data Access Services (DAS) mailto:Hlth.HnetConnection@gov.bc.ca

NOTE: *Without the Director's approval the DAS Connections Analyst cannot proceed with the request.*

If personally identifiable data is involved, a copy of the **Information Sharing Agreement** authorizing the sharing of this data must be attached to the request. Without this copy (if required), the DAS Connections Analyst cannot proceed with the request.

The external Information Systems (IS) contact information **must** be provided. At this point, the Ministry business area contact will be notified by the DAS Connections analyst that they must obtain the appropriate software (SFTP client).

NOTE: *Without an IS contact, the DAS Connections Analyst cannot proceed with the request.*

If external users are sending Personally Identifiable Data to the Ministry of Health, they **must** encrypt and **must** use the Ministry of Health Standard products: WinZip or PGP.

A Data Access Agreement (DAA) and Schedule 20 are required by the external contact. These documents address the responsibilities associated with using this service. **Exceptions** to this requirement are:

- ➢ Health Authority users (these services are covered under the overarching Data Access Agreement (DAA) with the health authority)
- ➢ Transfers where the file is 'pulled' from the external parties SFTP server to the MoH SFTP server by a Ministry employee or contractor engaged by the Ministry. In this scenario, the external party does not have access to the MoH SFTP server, therefore an agreement is not necessary.

NOTE: *Without a DAA and Schedule 20 (if required), the DAS Connections Analyst cannot proceed with the request.*

Once these steps in the process have been completed, the DAS Connections Analyst will forward the request to the MoH SFTP Service Consultant to proceed with the setup. The consultant will then contact the external IT contact and the individuals named on the request and complete the setup.

Only those individuals named on this request are given access to the 'mailbox' or folder. This service can only be used for the purpose identified in the box labeled 'Description of the data being transferred' on the request form (#7101).

2   Roles

2.1   Description of Roles

2.1.1   Data Access Services (DAS) Connections Analyst

The DAS Connections Analyst is the MoH person(s) who receives the request for the SFTP service and confirms that all requirements for this service are met. They forward the request to the MoH SFTP Service Consultant to setup the SFTP access for this client.

2.1.2   MoH SFTP Service Consultant

The MoH SFTP Service Consultant is the MoH person(s) responsible for the SFTP server. They will contact both the MoH Business Area User and the External IT contact to obtain the necessary information for the setup. Both MoH users and external users will be provided with User ID and passwords that will allow them access to the server. Upon their initial contact with the SFTP server, the server will install a non-expiring key.

2.1.3   External IT Contact

The External IT contact is the person(s) on the external client side who will possess the necessary IT skills to assist the MoH SFTP Service Consultant in setting up the SFTP server for secure file transfer. This person identified must be able to assist in the gathering of network information and coordinate software installations. For this reason, it is **mandatory** that the MoH SFTP Service Consultant communicate with the External IT contact to help facilitate this setup.

2.1.4   Ministry Business Area User

Ministry Business Area User is a person(s) who will have access to the SFTP folder or 'mailbox and be sending or receiving data on behalf of the Ministry. They are responsible for submitting the request for SFTP, the provision of necessary agreements, defining their internal work flows and testing and implementing the service.

2.1.5   External Users

The External User is the person(s) who will have access to the folder or 'mailbox' and be sending or receiving the data on behalf of the external client. They may be required to sign a Data Access Agreement and Schedule 20 for the use of the service.

3   Technical Security

- SFTP uses the SSH protocol to send data over a secure channel or tunnel. Access is facilitated by dual factor authentication, utilizing a public/private key pair exchange and/or ID and password.

- With manual transfers, the External IT contact provides the MoH SFTP Service Consultant the information needed to set up the External User on the SFTP server. The first time the External User connects with the server, they are prompted to receive a non-expiring 'cached key' from the ministry SFTP server.

- With an automated transfer, public keys are exchanged between the two SFTP servers to enable a secure transfer.

- Encryption is 256 bit. Note that the files are encrypted during transfer only.

- Encryption of the file before it is sent to the SFTP server is **mandatory** and is the responsibility of the client transferring the data. The encryption password will need to be provided to the file receiver so it can be de-encrypted once it is received.

Please see Corporate Information Security and Audit's security bulletin for current MoH encryption standards (before the file is encrypted) and secure file transfer options.

4 Service Support

If you require assistance with SFTP, contact your SFTP/IT person. If you do not have an IT person or you are an IT person seeking support on behalf of a user in your organization:

- Call the MoH Help Desk (250-952-1234) or TOLL FREE (1-888-764-2323)
- Send an email directly to HLTH.HnetConnection@gov.bc.ca.

Please have the following information ready to provide the MoH Help Desk, or include these details in your email:

- Inform them you are using SFTP;
- Define the problem, including the specifics of any error messages displayed; and
- Ask that your call be assigned to DAS Connections Analyst.

By completing these steps you will ensure that the information required is captured and that your problem is assigned to the appropriate group for resolution.

5   Adding or Deleting Users to the Service

Changes to Service - Once the SFTP setup is established, it is up to the Ministry Business Area User(s) and External User Access Administrator(s) to inform the DAS Connections Analyst of any changes to access, including deletions as well as additions.

MOH User Adds and/or Deletions - The Ministry Business Area User will communicate desired additions or deletions to their Director who will provide authorization for these access changes to the DAS Connections Analyst hlth.hnetconnection@gov.bc.ca .
The analyst in turn will inform the MoH SFTP Service Consultant.

External User Adds and/or Deletions - External Users will communicate user additions or deletions to their Access Administrator(AA). The AA will then notify Ministry of Health DAS Connections Group hlth.hnetconnection@gov.bc.ca If they do not know who their AA is, they will need to phone the Ministry helpdesk for this information at 1-888-764-2323

Note: The AA will provide the users name, email address, phone number, organization number and the name of the SFTP service they would like the user to have access to.

6   Using SFTP

6.1   Prerequisites for Access to SFTP

Prerequisites for SFTP transfer depend on whether or not the transfer will be manual (person to person) or automated (machine to machine). In some situations, file transfers are partially manual and partially automated so the user will have to fulfill the requirement for both.

In this section we discuss several software options. The selection, installation and support of the software are the responsibility of the end user. We are providing this information only to assist you in this process and not to recommend any particular product.

6.1.1   Manual transfer

For a manual transfer, the user will need an SFTP client (the term 'client' refers to the software) to connect to the SFTP server. MoH users should request WS_FTP Professional, via an RFS request, the government standard product, to be installed on their PC. Instructions on how to obtain and use WS_FTP Professional are provided in Section 6.4.

For External Users not having a designated SFTP client, information has been provided, for example, on two free products. The External User must ensure that their organization allows the use of these (or other) free products:

   a. Unmanaged computer: For demonstration purposes we have provided instructions on how to obtain, install and use an Open Source SFTP client called Filezilla in Section 6.2.

   b. Managed computer: For demonstration purposes, instructions are provided on how to obtain, install and use a utility called PSFTP Putty in Section 6.3.

Once your request for SFTP is processed, you will be contacted by the MoH SFTP Service Consultant and given a User ID and password. For External Users, your IT contact will have been contacted by this Service Consultant to obtain the necessary setup information and coordinate the exchange of public keys, if required. The first time a user connects with the server using an SFTP client, they receive a non-expiring key which enables file transfer from that point on.

6.1.2   Automated Transfer

If an automated transfer is required, the two servers involved in the automated transfer must both be capable of SFTP. The MoH SFTP Service Consultant will contact the External IT Contact and arrange the exchange of public keys.

Automated transfers are typically set up server to server as they are designed to be available 24x7. Workstations are designed to be available only during work hours. If any part of this transfer is manual, you will also need an SFTP client to place files on the SFTP server.

6.2   Installing and Using Filezilla

These instructions assume that you have been given access to the SFTP server and that you have been provided a User ID and password.

First you must download and install Filezilla, which takes about 15 minutes. You will not need to reboot after the install. The download is located at:

http://filezilla-project.org/download.php

Select the latest version of Filezilla from the above link.

Then follow these instructions:
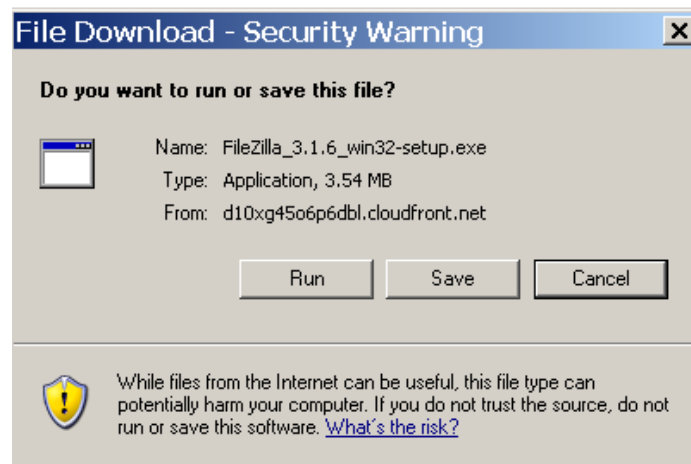
 ➢ Click 'Run'. The following popup will appear.
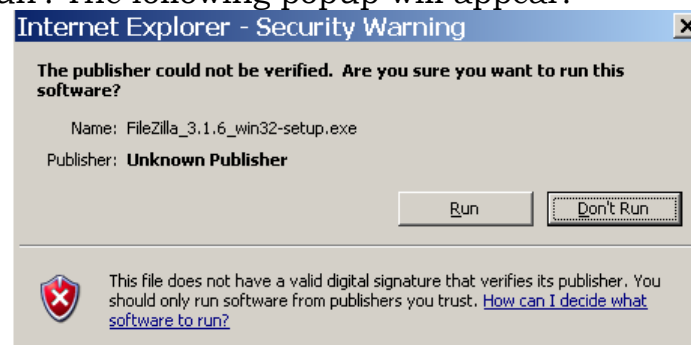
 ➢ Click 'Run'.
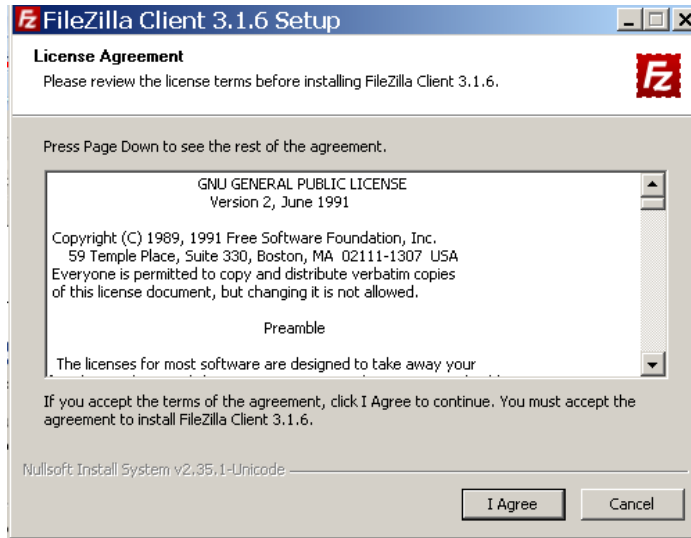
➤ Select 'I Agree'.
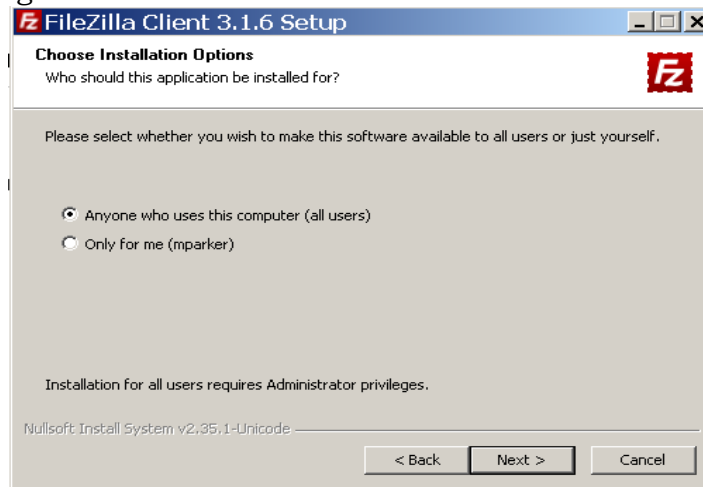
➤ Click 'Next'.
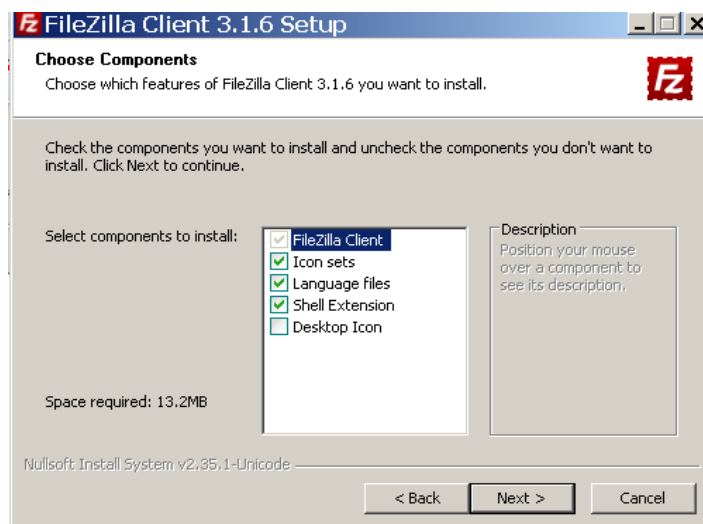
Leave the default selected components: 'Filezilla Client', 'Icon sets', 'Language files', 'Shell Extension'.

> ➢ Tick 'Desktop Icon', if this is your preference, then 'Next'.
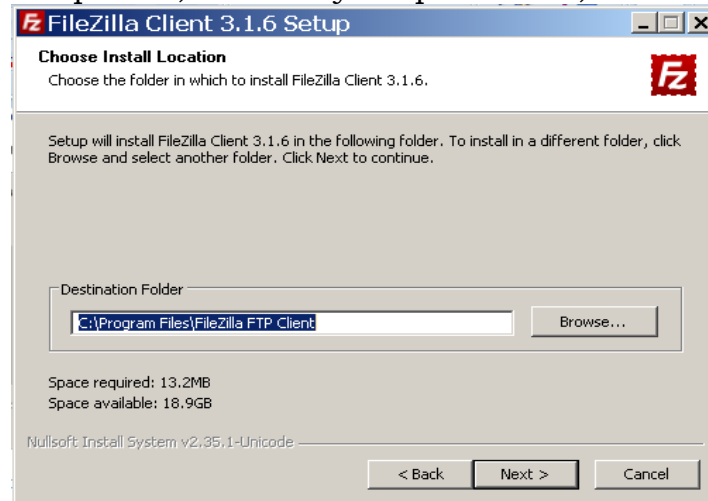
> ➢ Keep the default 'Destination Folder', click 'Next'.
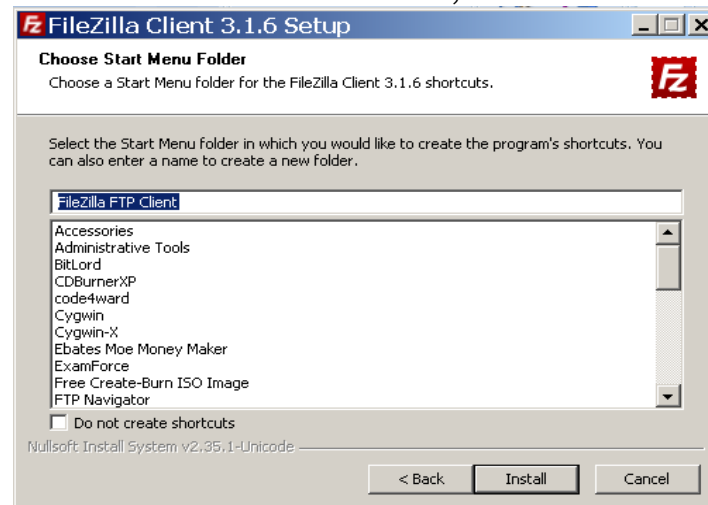
> ➢ Click 'Install'.
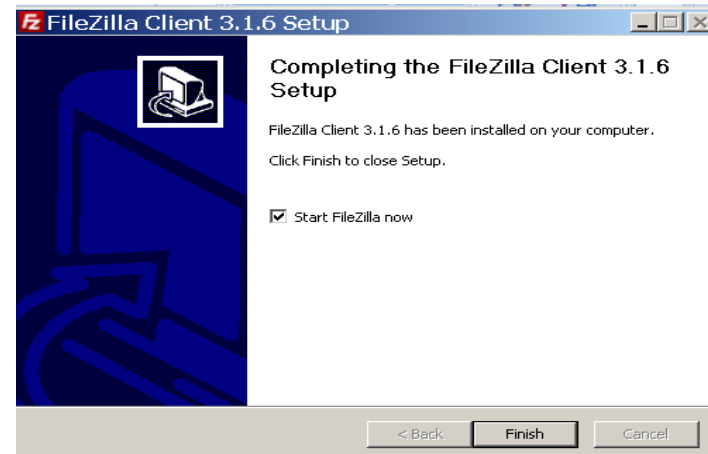
➤ Click 'Finish'.
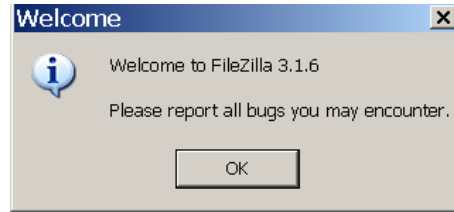
➤ Click 'OK' and Filezilla opens.
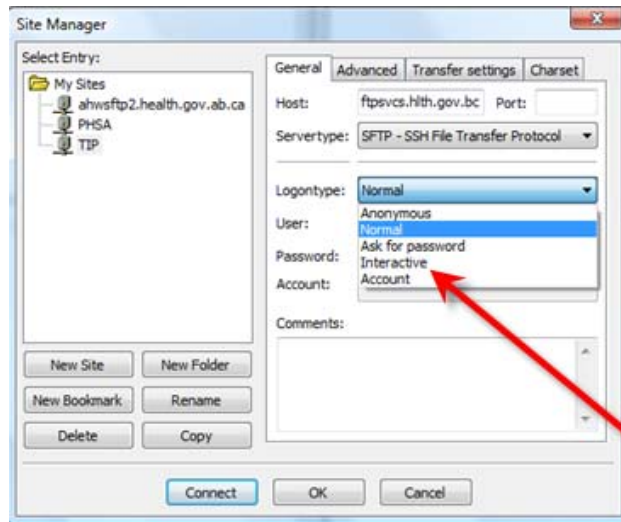
➤ The first time you connect to the site using Filezilla you will need to reset your password. To do this you will first have to specify the 'Interactive' Logontype within Site Manager for that site. The Site Manager is found in the upper left hand corner, under the File menu.

➤ When you have done this exit the Site Manager and return to the main screen.
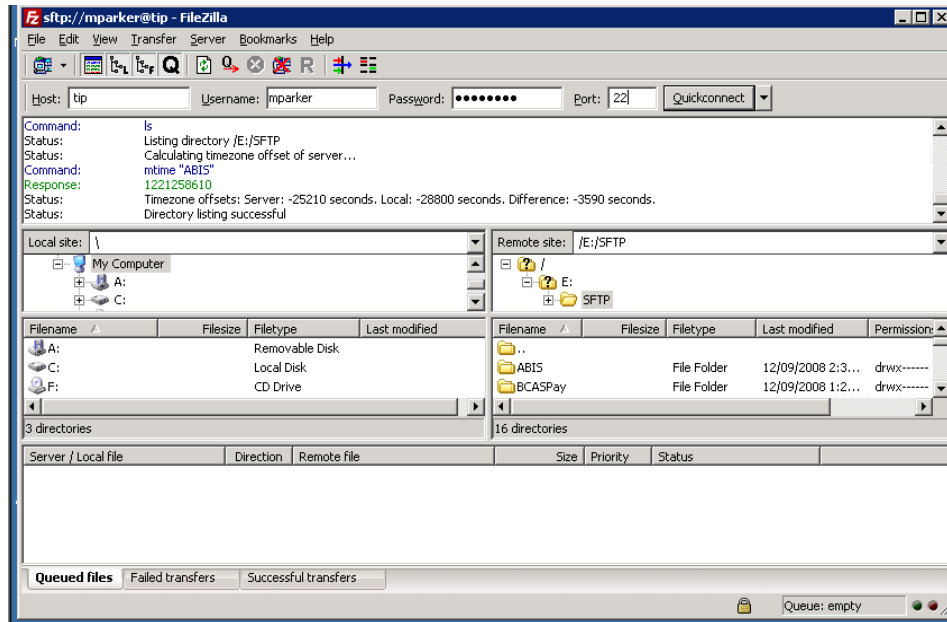
> In the 'Host' field, enter the IP address (or servername) that you were given for the SFTP server.
> In the 'Username' field, enter the User ID you were provided to the SFTP server.
> In the 'Password' field, enter the password for that User ID.
> In the 'Port' field, enter '22', which is the port for SFTP.
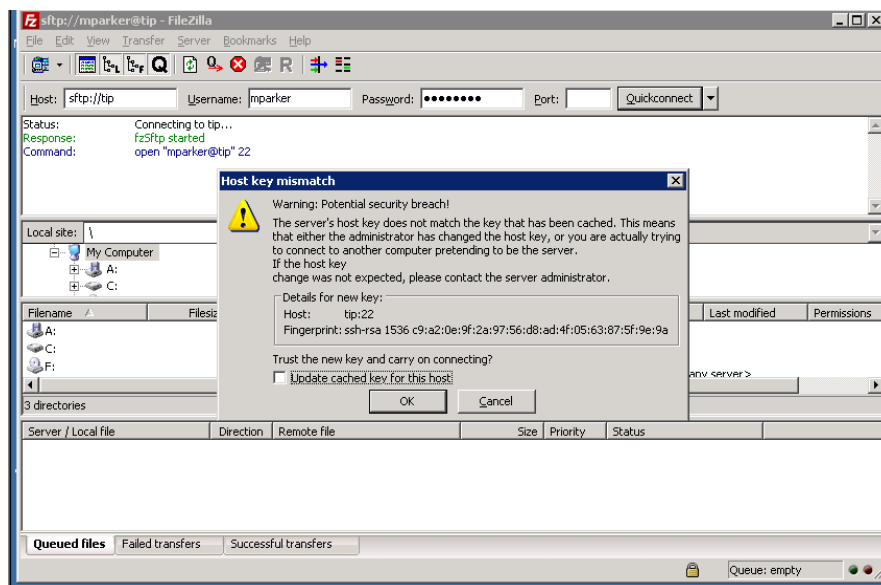
> A popup box appears 'Host Key Mismatch'.
> Tick the checkbox 'Update your cached key for this host'. Then click 'OK'.

This question will only be asked the first time you connect to the server.

➤ After you have logged in and changed your password, change the Logontype back to 'Normal' in Site Manager for this site.

6.2.1   Using Filezilla
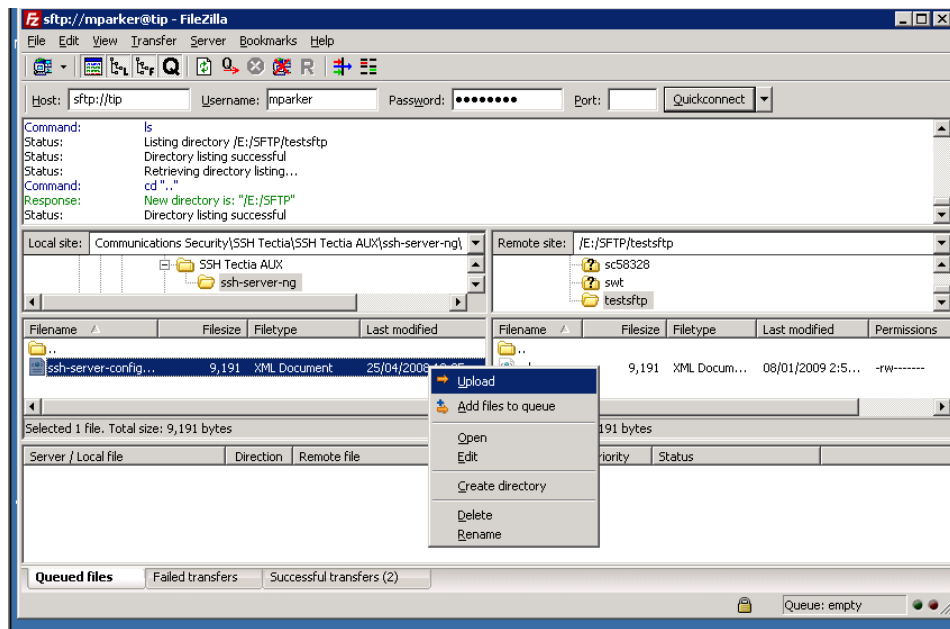
➢ In the left pane you can navigate to a folder on your local computer.

➢ In the right pane, you can navigate to a folder on the SFTP server.
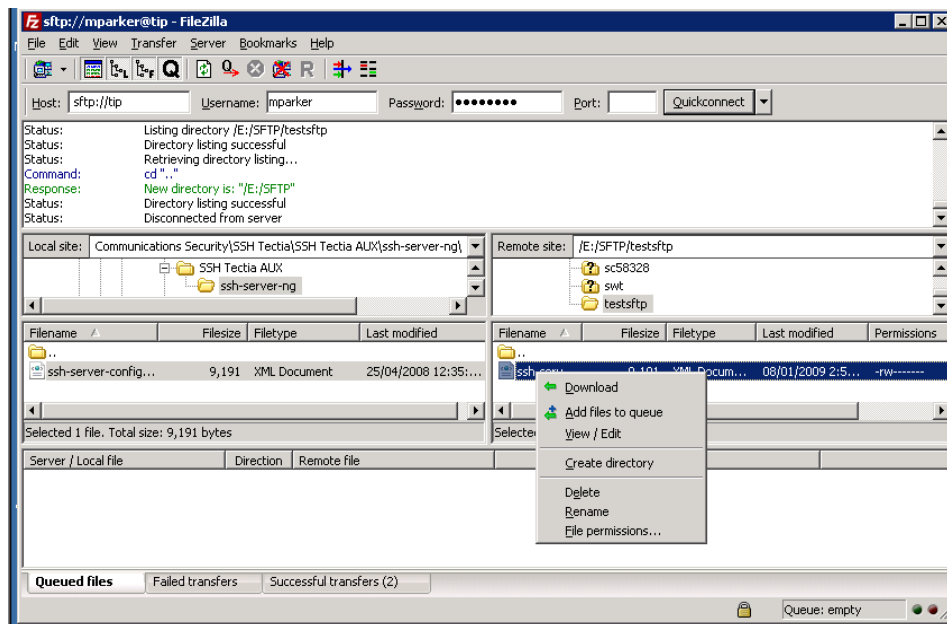
➢ Right click on the file that you want to upload to the server and select 'Upload' from the dropdown menu.

➢ Once you have transferred the file over to the server, you can right click on it.

➢ You now have full access to the file and are free to rename it, delete it, etc...
➢ You can create directories on the server by right clicking on the folder you have access to and selecting 'Create Directory'. Enter the name of the newly created directory.
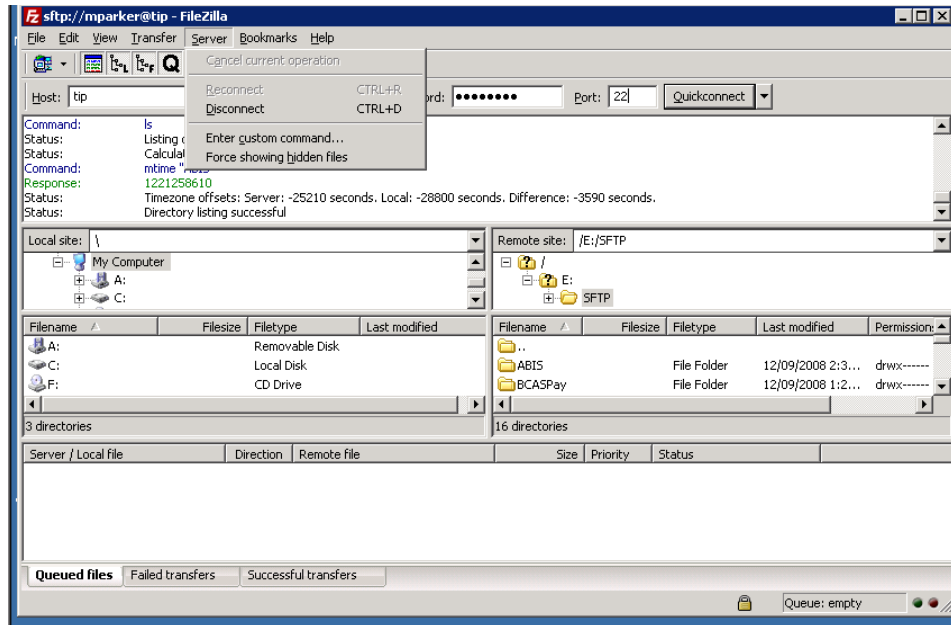
➢ When you are finished sending the files to the server, select 'Server' from the file menu and then 'Disconnect' from the dropdown list.
➢ You are now disconnected from the server.
➢ As part of the install, this Filezilla icon will appear on your desktop. You can select it when you need to access the server via SFTP.

6.3   Installing and Using PSFTP Putty Utility

External Users with managed PC's can use a free utility called PSFTP Putty. To download, go to this site:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Then follow these instructions:

> Click on the '<u>psftp.exe link</u>'. The following screen appears:
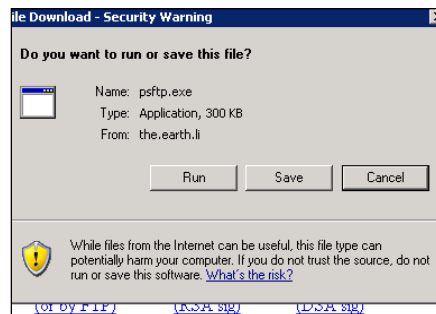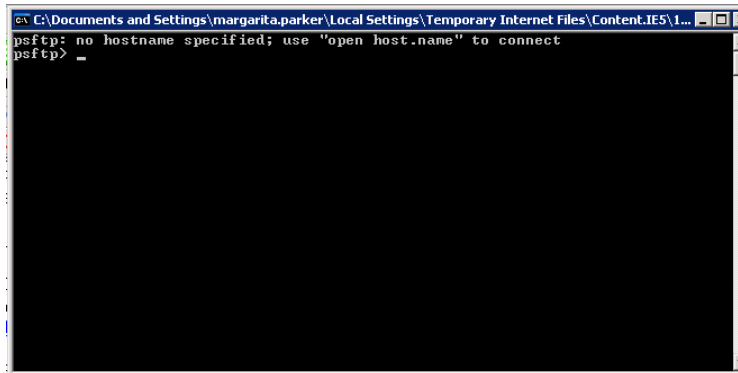
> Click on 'Save' to obtain a copy of this utility for future use. If you do not save the file to your PC before you run it, you will need to download it from the Web each time you run the utility.
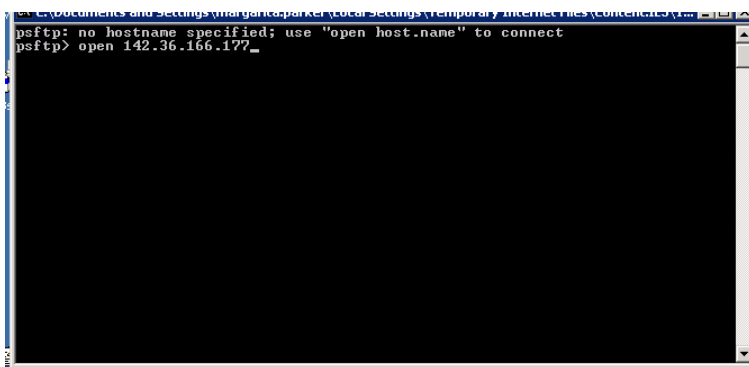
> Click 'Run'.

The following screen appears:
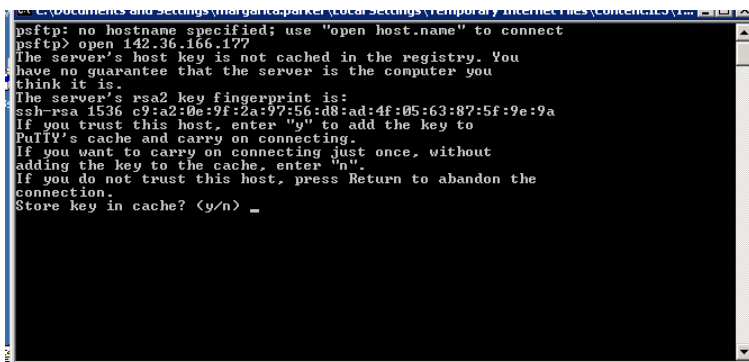
> ➤ Type: Open the servername (or the IP address that was given to you).

> ➤ When asked to store key in cache, type 'Y'. This question will be asked only the first time you connect to the server.

> ➤ When asked for your Logon ID, type the User ID that you were provided to connect to the server.

> ➤ When asked for your password, type the password for that User ID. The characters in your User ID and password are case sensitive.

6.3.1   Using PSFTP Putty

Once you are connected, you will need some commands to help you navigate and manage files:

➢ 'CD' (change directories) allows you to navigate to a different folder. Note: you only have access to the folders that you require.

➢ 'LCD' changes the location that you are at on the local machine (not the server) e.g. lcd <directory> (c:\temp for example.)

➢ 'Put' allows you to put files on the server. e.g 'Put <filename>'.

➢ 'Get' gets files from the server and copies them to the local machine. e.g. 'Get <filename>'.

➢ 'Mkdir' creates a directory e.g. mkdir <directory name>'.

➢ 'Help' will get a list of commands that you can use.

6.4 Installing and Using WS_FTP Professional

If you are a Ministry of Health user, you will be using WS_FTP Professional. If this is not already installed on your PC, please go to this URL to request it be installed:

https://gww.health.gov.bc.ca/forms/mailform_H7007.html

6.4.1 Connection Wizard

When you first use WS_FTP Professional, there is a Connection Wizard that will step you through the initial setup. The MoH SFTP Service consultant will provide you with the information you need to provide the Wizard once the consultant receives your request. You will be prompted to enter the following information as described in the following screenshots:

➢ **Connection Name**: this can be whatever you want – the name of the data you are sending or the SFTP server (TIP)
➢ **Server Address**: ftpsvcs.hlth.gov.bc.ca
➢ **Username**: (this will be provided by the MoH SFTP Service consultant)
➢ **Password**: (this will be provided by the MoH SFTP Service consultant)
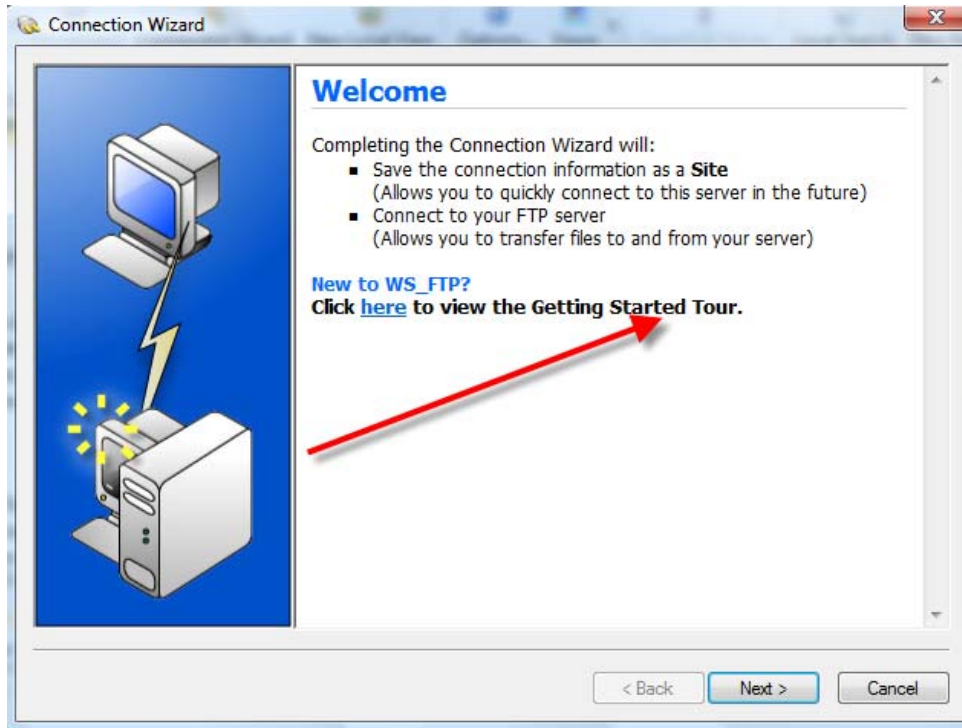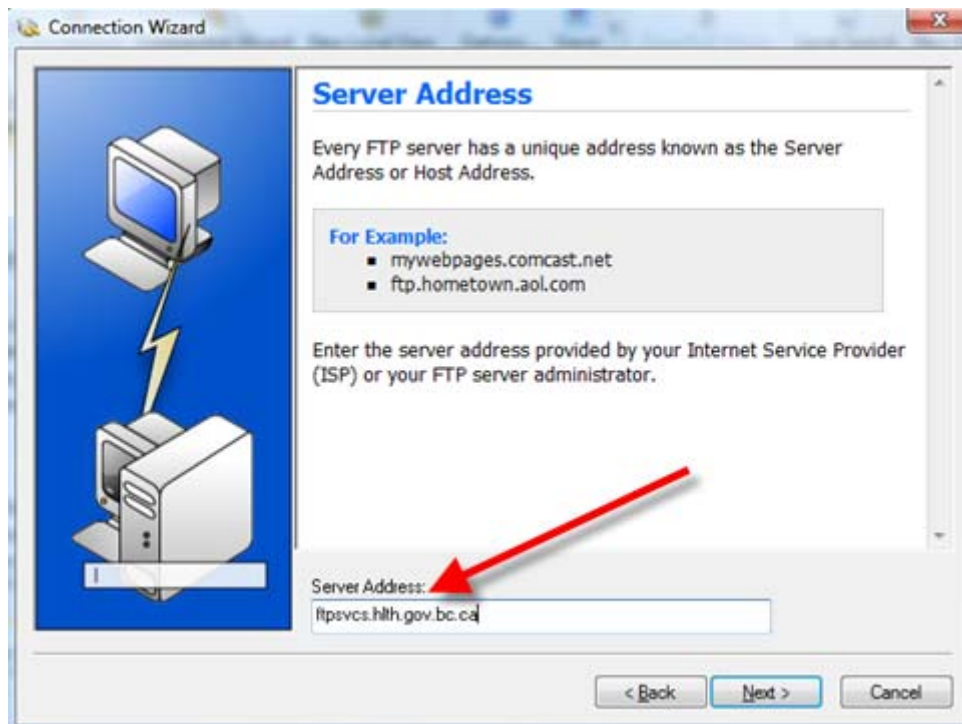
- ➢ There is a tutorial to help you get acquainted with WS_FTP Professional.
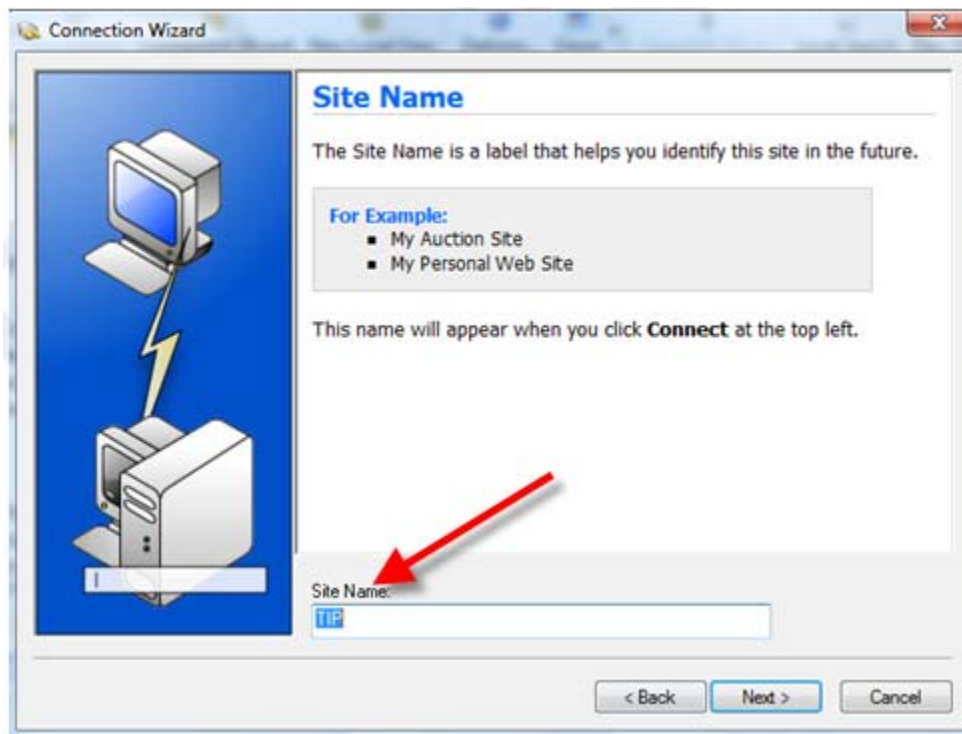
- ➢ Enter in a site name. This could be the name of the server or the purpose for which you will be using SFTP.
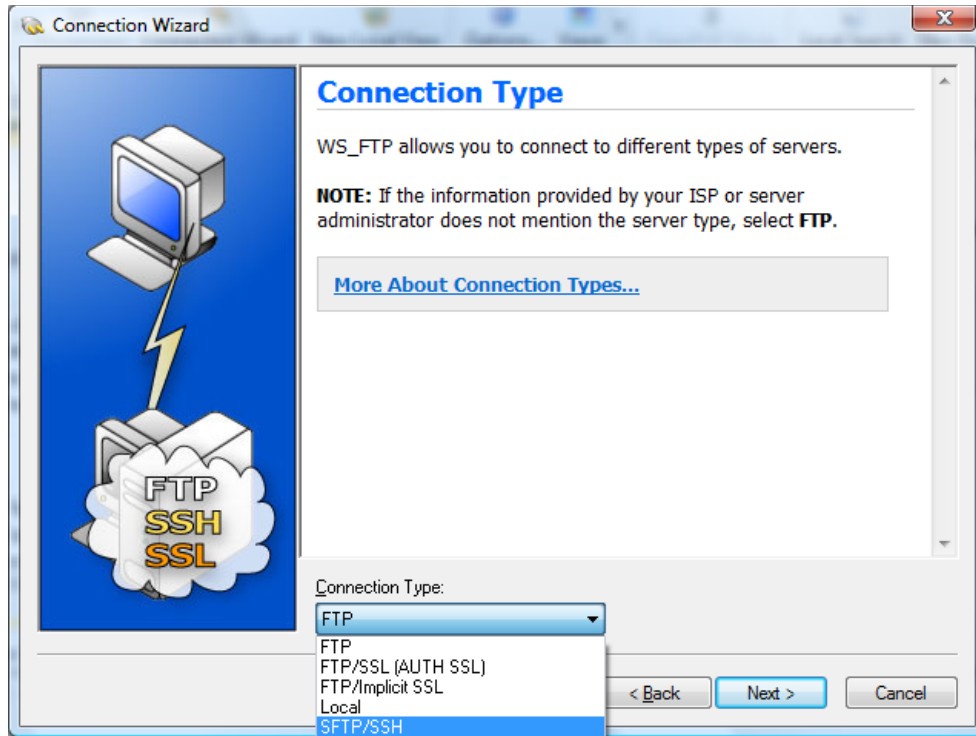
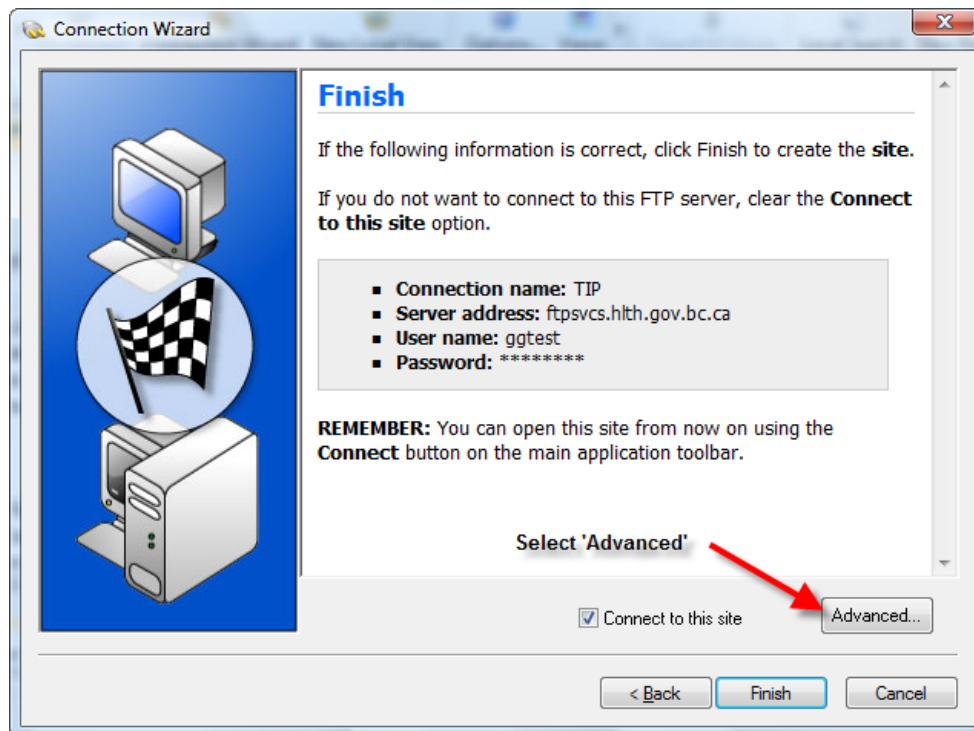➢ Select Connection Type 'SFTP/SSH'.

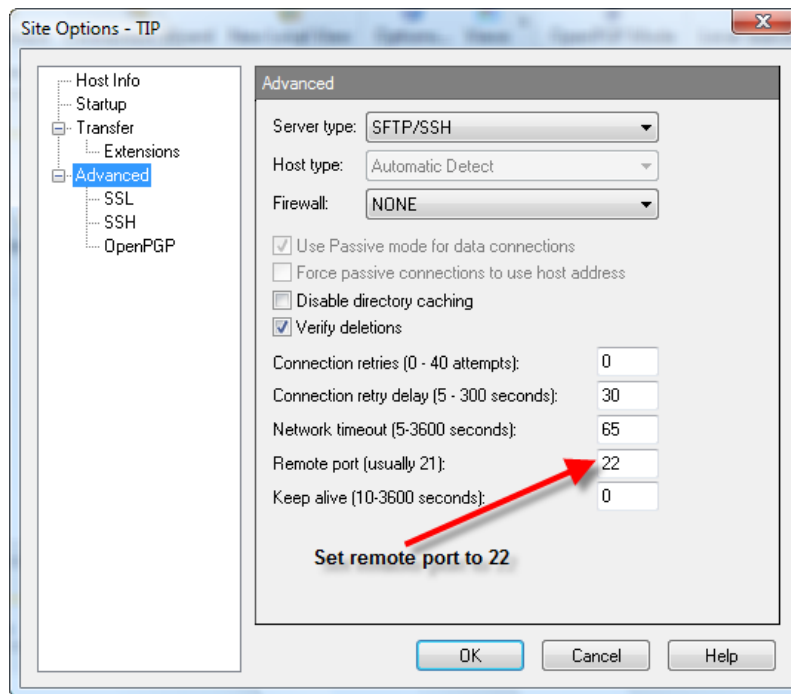➢ Enter 'ftpsvcs.hlth.gov.bc.ca' in the Server Address field.

> ➢ Enter the User ID and Password you were provided into the User Name and Password field. Click 'Next'.

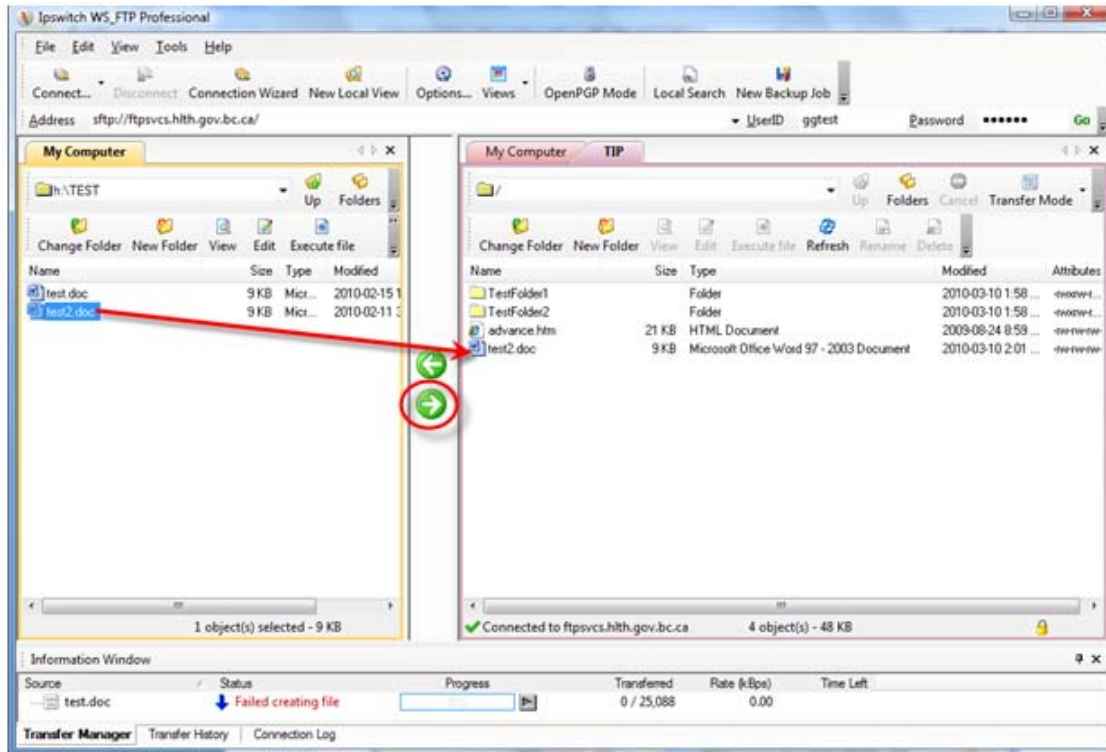> ➢ Untick the 'Connect to this site' box. Next click the 'Advanced' button shown above.

> ➤ On this screen enter '22' into the Remote Port field.

6.4.2 Using WS_FTP Professional

Once you have completed the wizard, the application will present the following screen:

> ➤ Choose 'Trust this key'. This question is only asked the first time you connect to the server.

> ➢ To transfer files to the SFTP server, select a file from your C: drive or LAN drives on the left hand side, then select the right pointing arrow in the centre of the window. The file will be transferred to the SFTP server. Ensure you are in the correct folder on the server. You can also drag the file over.

> ➢ To transfer the file from the SFTP server to your drives, just select the file on the right hand side, and then select the left pointing arrow in the centre of the window and the file will be transferred to your selected drive. You can also drag the file over.
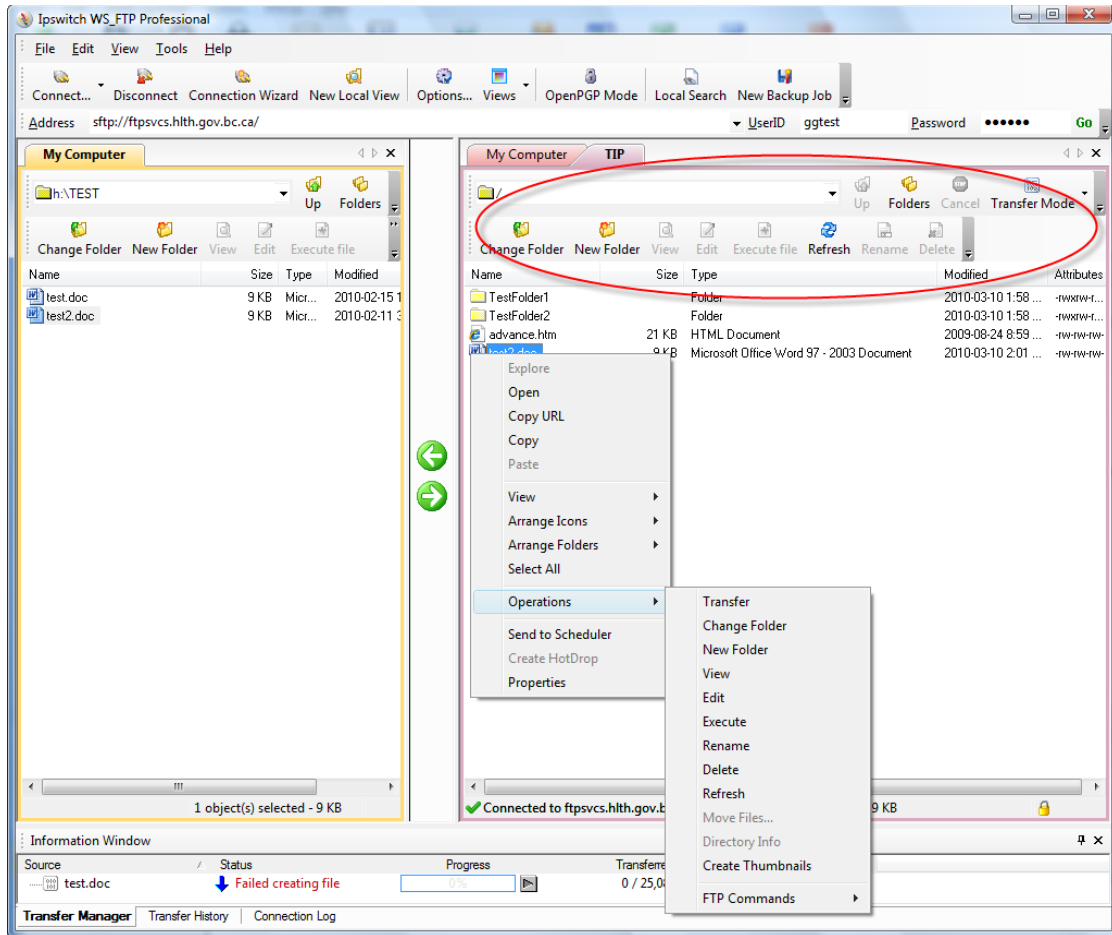
> ➢ There are several operations you can perform on this file by clicking on your right mouse button. A drop down menu will appear listing these operations. These same options are also available on the toolbar at the top.
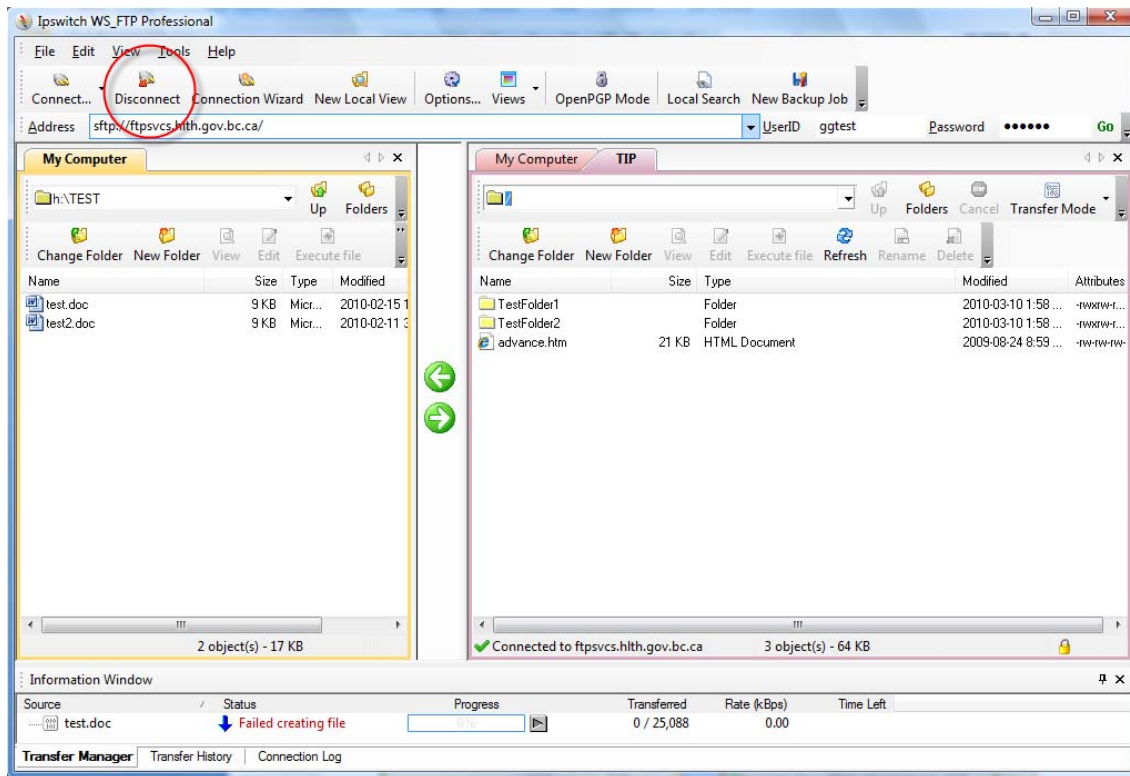
➢ When you are finished, remember to click the 'Disconnect' button on the top left menu bar to log off.