Ministry of Health

Secure File Transfer Protocol

User Guide

Date Created:	November 10, 2009
Date Updated:	May 13, 2019
Next Update:	
Version:	2.3

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
April 14, 2014	Bruce Stuart	1.7	Updated
October 11, 2017	Mike Botrakoff	2.0	Updated
December 13, 2018	Mike Botrakoff	2.1	Updated
January 8, 2019	Mike Botrakoff	2.2	Updated MOH s/w info
May 13, 2019	Mike Botrakoff	2.3	Updated WinSCP info

Table of Contents

1 Overview

1.1 Purpose of this Document

This document has been written to support clients using the Secure File Transfer Protocol to transfer files.

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

- Submit and/or receive files securely to/from the Ministry of Health and external user (person to person transfer)
- Exchange files using automated computer-to-computer transfers.

1.2 Terms of Reference

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.

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

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.

SFTP or Secure File Transfer Protocol is a method of transferring data between an SFTP server and another party, using an SFTP client or SFTP software. The data is encrypted during the transfer, but not while it is sitting on the server (see sections **1.3 A Summary of the Application Process** and **3 Technical Security** below to view information regarding encryption methods). Access is facilitated between a client and the server by a user ID and password or SSH key. 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 a server capable of SFTP transfers. In both situations, the Ministry of Health (MoH) Service Consultant must contact the external IT contact to complete the setup.

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/our-tools/forms/information-management/hlth-7101-secure-file-transfer-request

- The request is forwarded to their Director for approval
- Once approved, the Director forwards the form and their approval to the Systems Services network team - netreqst@gov.bc.ca

NOTE: *Without the Director's approval the Systems Services Consultant cannot proceed with the request.*

If personally identifiable data is involved, an **Information Sharing Agreement** authorizing the sharing of this data must be in place.

The external Information Systems (IT) contact information **must** be provided.

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 (using AES=256 encryption with password)** or **PGP** (contact netreqst@gov.bc.ca for more details).

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 Systems Services Consultant cannot proceed with the request.*

Once these steps in the process have been completed, the Systems Services 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 folder(s) on the SFTP server. 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) and to which the DAA applies.

2 Roles

2.1 Description of Roles

2.1.1 MoH Service Consultant

The MoH Service Consultant is the Ministry 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 IDs and passwords that will allow them access to the server. Upon their initial contact with the SFTP server, the user will be prompted to accept and install the SFTP server's public key.

2.1.2 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 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 Service Consultant communicate with the External IT contact to help facilitate this setup.

2.1.3 Ministry Business Area User

The Ministry Business Area User is a person(s) who will have access to the SFTP folder(s) and will 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 the internal work flows and testing and implementing the service.

2.1.4 External Users

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

3 Technical Security

SFTP stands for "Secure File Transfer Protocol". The Secure File Transfer Protocol ensures that data is securely transferred using a private and safe data stream. It is the standard data transmission protocol for use with the SSH protocol.

SFTP uses the same port as SSH (22) – once the SSH connection has been established, the SFTP protocol can be used. The SFTP protocol runs on a secure channel - no clear text passwords or file data are transferred.

Before establishing a connection, the SFTP server sends an encrypted fingerprint of its public host keys to ensure that the SFTP connection will be exchanging data with the correct server. When a connection is first established, this key is not yet known to the client program and must therefore be confirmed by the user before data is exchanged for the first time. Different servers issue fingerprints only once. They are generated by a server's private key.

The SFTP server uses AES-256 as its encryption cipher when establishing connections with other computer clients and servers.

All data that contains personally identifiable information must be encrypted to the standards as stated in the Corporate Information Security and Audit's security bulletin (before the file is transferred and during secure file transfer options).

In addition to users encrypting their data using WinZip (AES-256 with version 11 or better) with passwords, the SFTP server can use OpenPGP technology to safeguard data at rest if required. OpenPGP uses a public key and a private key to encrypt data and maintain security. For more information, please contact netreqst@gov.bc.ca

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 netreqst@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
- Ask that your call be assigned to Systems Services

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 MoH Service Consultant of any changes to access, including deletions as well as additions.

MOH User Additions 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 MoH Service Consultant – netreqst@gov.bc.ca

External User Additions and/or Deletions - External Users will communicate user additions or deletions to their Access Administrator (AA). The AA will then notify MoH Service Consultant – netreqst@gov.bc.ca. If they do not know who their AA is, they will need to phone the Ministry helpdesk for this information at #250-952-1234 (Toll-free 1-888-764-2323)

Note: *The AA will provide the users name, email address, phone number, organization number and the name/number 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.

This section discusses several software options. The selection, installation and support of the software are the responsibility of the end user. Information is provided only to assist 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 install **WinSCP**. Instructions on how to obtain and use WinSCP are provided in Section 6.2

Another SFTP client to consider is **Ipswitch WS_FTP Pro**. Please note: WS_FTP Pro requires a client license. Instructions on how to obtain and use WS_FTP Pro are provided in Section 6.3

Once the request for SFTP is processed, users will be contacted by the MoH Service Consultant and given a User ID and password. The first time a user connects with the server using an SFTP client, they receive an encrypted fingerprint of the SFTP server public 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 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 WinSCP

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

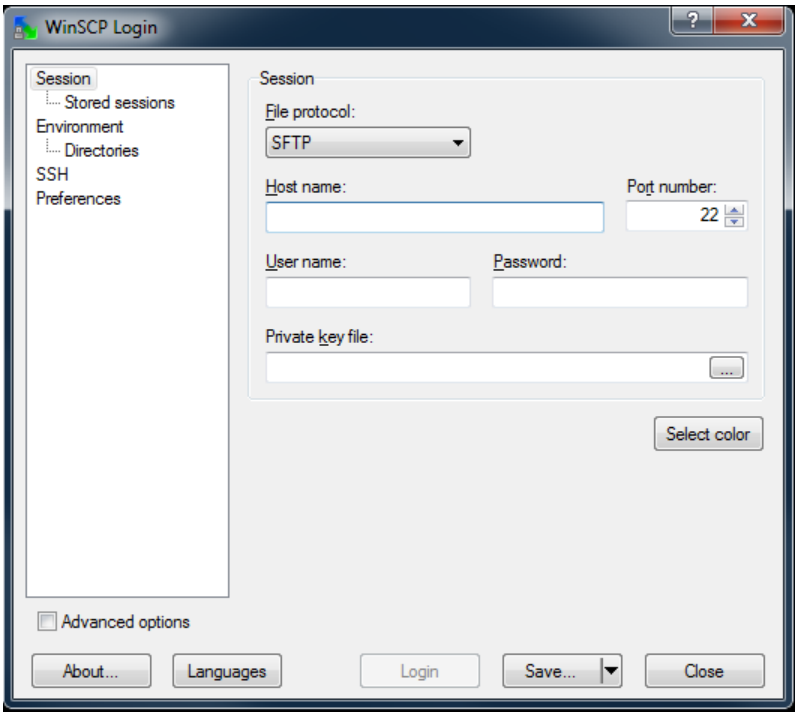
For non-Government users:

WinSCP is located here.

For MoH users:

From the Start Button/Orb on your desktop, navigate to Microsoft System Center and then Software Center. Search for WinSCP and then click Install.

Once you start WinSCP, you will be presented with the following screen:

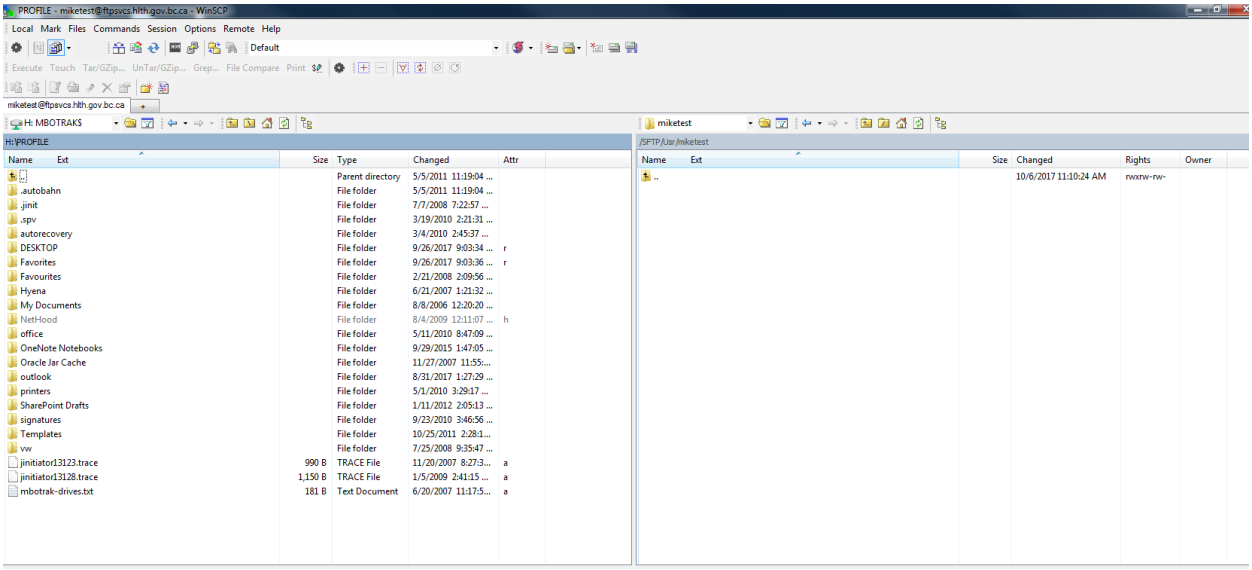


For this screen enter:

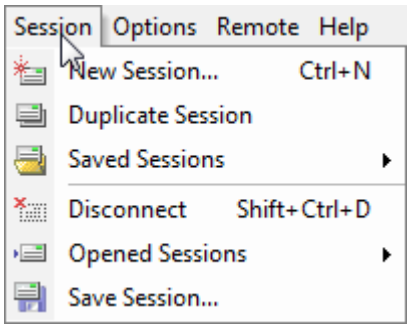
File Protocol = SFTP
Host name = ftpsvcs.hlth.gov.bc.ca
User name = as supplied
Password = as supplied by netreqst@gov.bc.ca

6.2.1 Using WinSCP

- 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.



- You can drag and drop between screens.
- When you are finished sending the files to the server, select 'Session' from the file menu and then 'Disconnect' from the dropdown list.



6.3 Installing and Using WS_FTP Pro

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

For non-Government users:
WS_FTP Pro is located here.

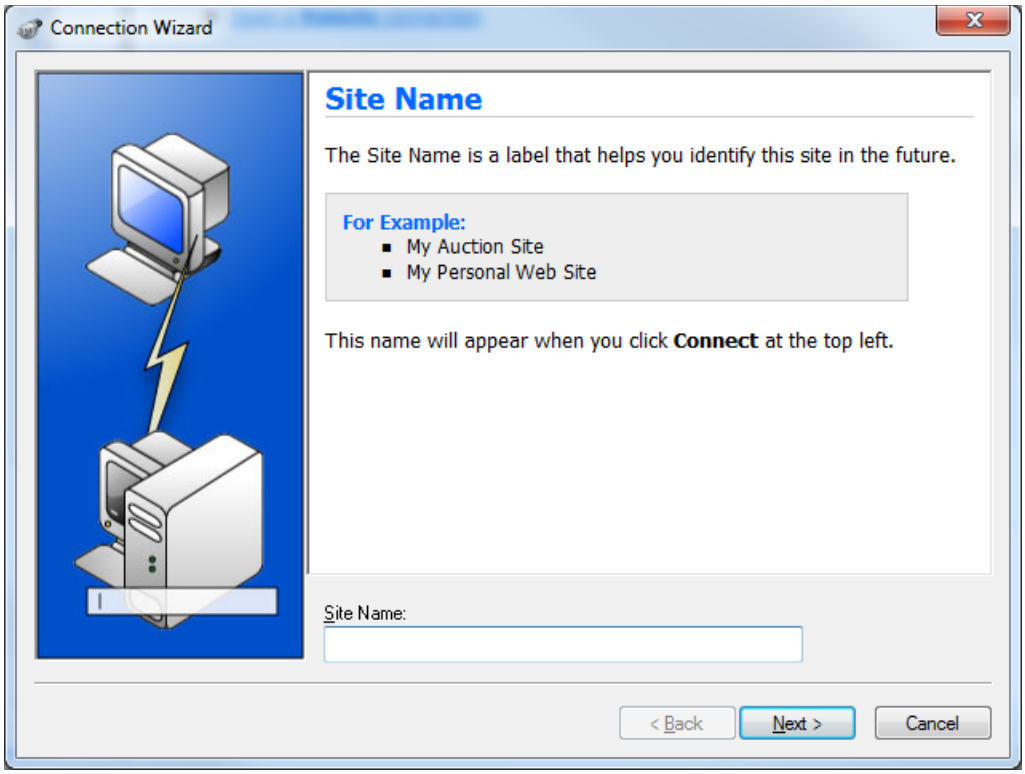
For MoH users:

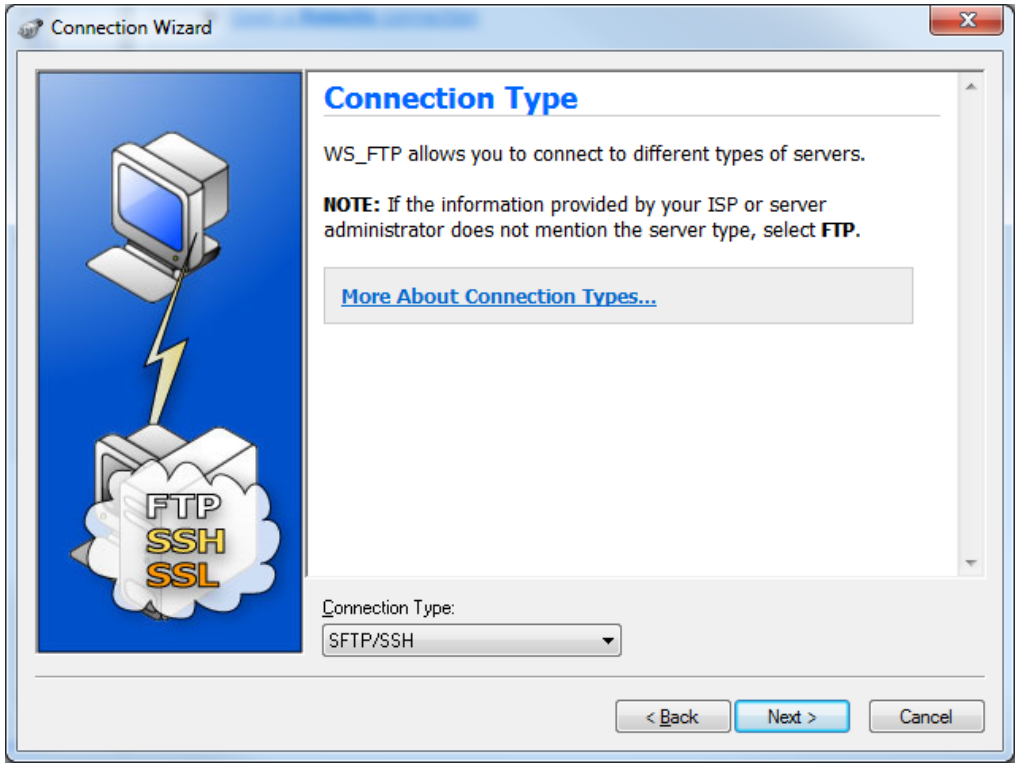
Please complete an RFS Form for this software to be installed on your computer. It may take a few days to be installed. Note that this software is licensed and requires Expense Authority approval.

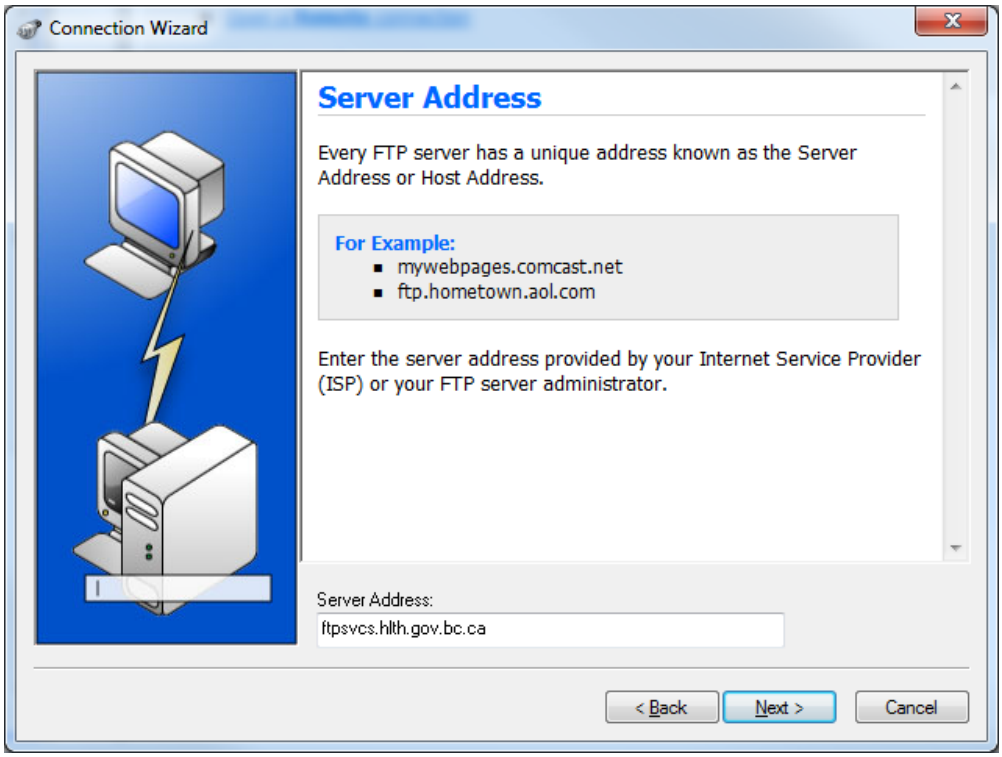
6.3.1 Connection Wizard

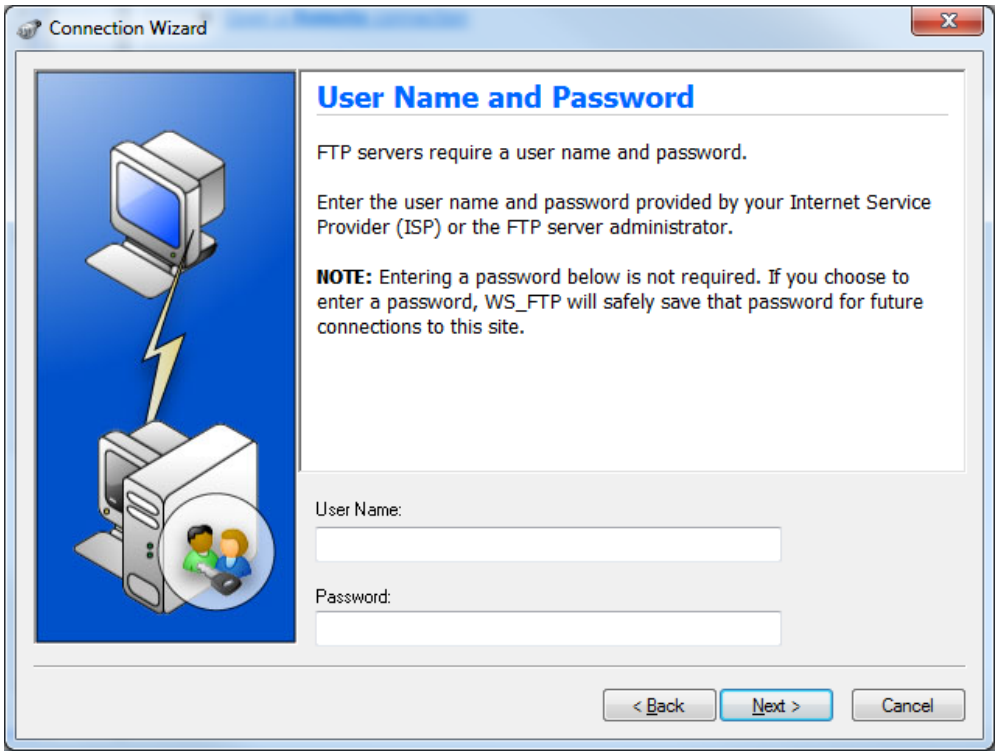
After WS_FTP Pro is installed, there is a Connection Wizard that will step you through the initial setup. Users will be prompted to enter the following information as described in the following screenshots:

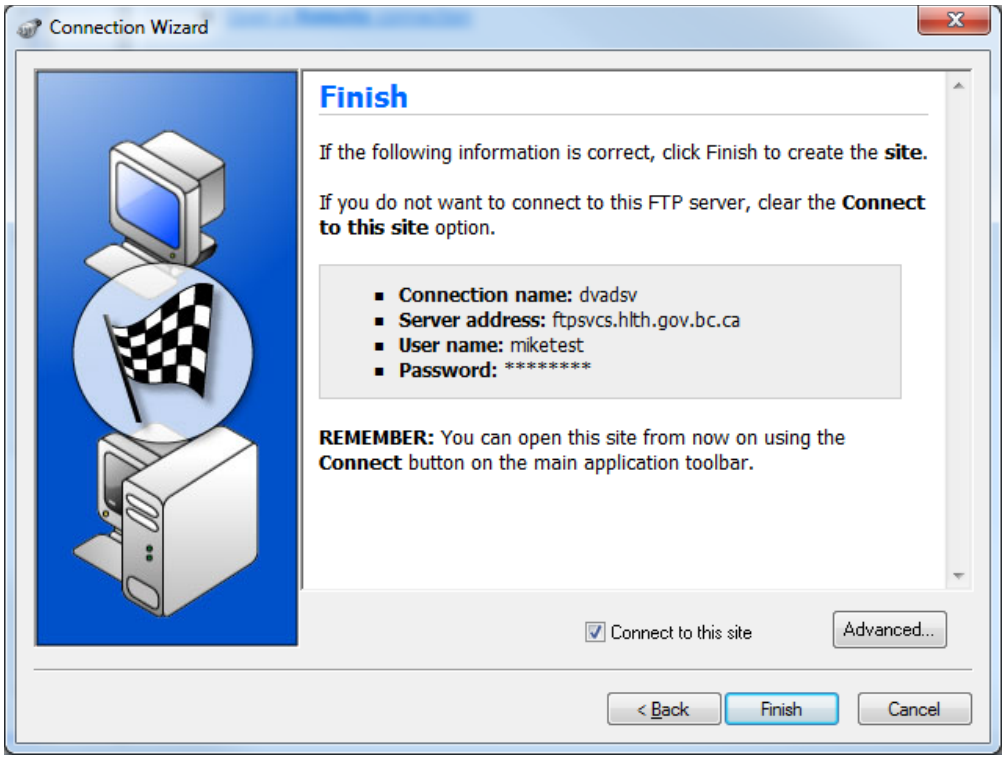
- **Site Name**: This can be whatever you want – a suggestion would be to name it **MOH SFTP Server**
- **Connection Type:** Select SFTP/SSH
- **Server Address**: ftpsvcs.hlth.gov.bc.ca
- **Username**: Provided by the MoH Service consultant
- **Password**: Contact netreqst@gov.bc.ca for this


Connection Wizard
Site Name
The Site Name is a label that helps you identify this site in the future.
For Example:
My Auction Site
My Personal Web Site
This name will appear when you click Connect at the top left.
Site Name:
< Back
Next >
Cancel


Connection Wizard
Connection Type
WS_FTP allows you to connect to different types of servers.
NOTE: If the information provided by your ISP or server administrator does not mention the server type, select FTP.
More About Connection Types...
FTP
SSH
SSL
Connection Type:
SFTP/SSH
< Back
Next >
Cancel


Connection Wizard
Server Address
Every FTP server has a unique address known as the Server Address or Host Address.
For Example:
mywebpages.comcast.net
ftp.hometown.aol.com
Enter the server address provided by your Internet Service Provider (ISP) or your FTP server administrator.
Server Address:
ftpsvcs.hlth.gov.bc.ca
< Back
Next >
Cancel

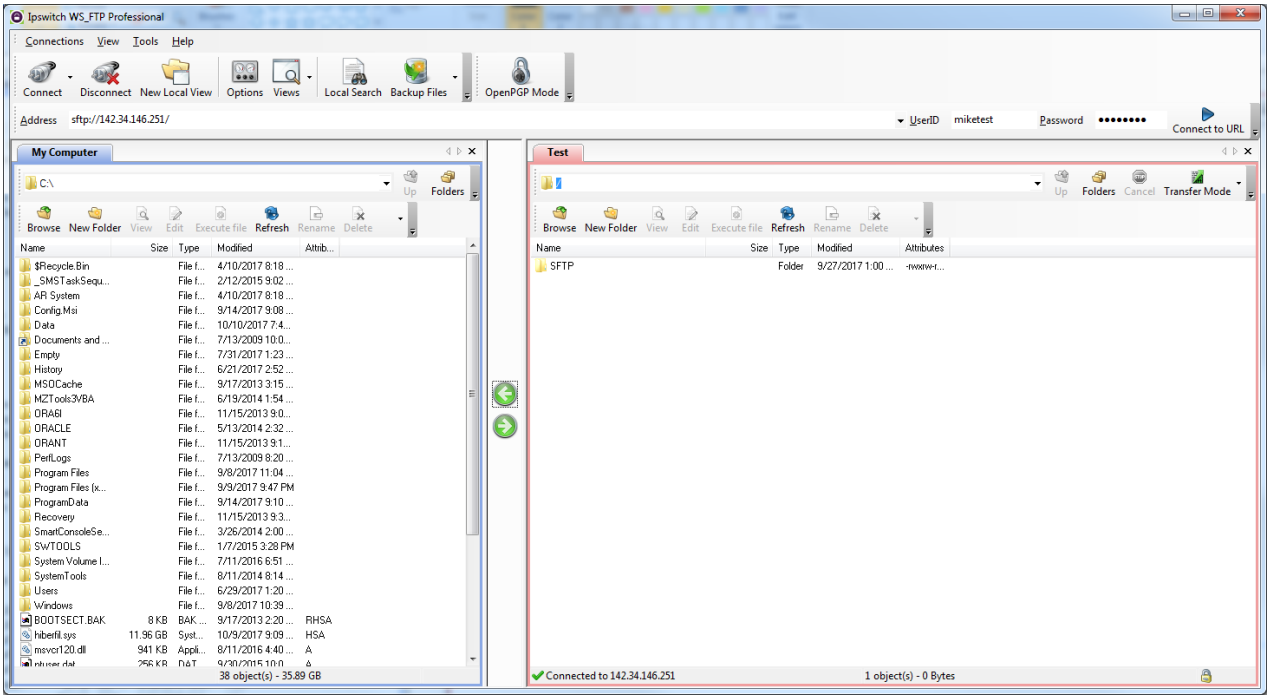

Connection Wizard
User Name and Password
FTP servers require a user name and password.
Enter the user name and password provided by your Internet Service Provider (ISP) or the FTP server administrator.
NOTE: Entering a password below is not required. If you choose to enter a password, WS_FTP will safely save that password for future connections to this site.
User Name:
Password:
< Back
Next >
Cancel


Connection Wizard
Finish
If the following information is correct, click Finish to create the site.
If you do not want to connect to this FTP server, clear the Connect to this site option.
Connection name: dvadsv
Server address: ftpsvcs.hlth.gov.bc.ca
User name: miketest
Password: ********
REMEMBER: You can open this site from now on using the Connect button on the main application toolbar.
Connect to this site
Advanced...
< Back
Finish
Cancel

6.3.2 Using WS_FTP Pro

The first time you connect to the MOH SFTP server, the application will present the following screen:

- Choose 'Trust this key' and then OK.



- To transfer files to the SFTP server, select a file from 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 – please ensure you are in the correct folder on the server. You can also drag and drop the file between panes.

- 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 location. You can also drag and drop the file between panes.

- When you are finished, click the 'Disconnect' button on the top left menu bar to log off.