SCP/SFTP info for Non-Enterprise Applications dropping files on DTP/DTT

NOTE: References to DTT are for test connections. Substitute DTP for production.

To Setup An Account

We will need to know the IP address of the workstation/server that the transfers will be initiated from because connections are filtered by IP address.
If you have a departmental userid that you want to use, please let us know that also. Otherwise, an account on DTT will be set up for you.
You will have access to an upload folder at /HOME/KFS/gl/collector/.
You will be able to upload files to the upload-folder.
You will not be able to delete, download or overwrite files in the upload-folder.

If you want to transfer the file manually, you will need to have an SCP/SFTP client installed. For IU departments SFTP software can be downloaded from IUWARE including WinSCP, AnyClient (Windows), Fetch (Mac) and Cyberduck (Mac). You can find more info in the KB article titled "At IU, what SSH/SFTP clients are supported and where can I get them?".

To Automate the Transfer of the Files

1. You can connect with an SFTP-type interface using sftp2.exe. The KB article titled "What is SFTP, and how do I use it?" has instructions, but note that the executable is "sftp2.exe" instead of "sftp.exe", and it may not be in your command PATH, so you will need to either be in the source directory, or put the correct directory in your command PATH.
2. You can also use "scp2.exe". This is not an interactive session. It is more like a copy command where you designate the source file and destination file and is very useful if you are interested in creating a script that you can run to perform the file transfer. See the KB article "In Unix, how do I use the scp command to securely transfer files between computers?" The info is the same for running this from Windows except that the executable is "scp2.exe" instead of "scp.exe", and as with sftp2.exe, you will need to either be in the source directory, or put the correct directory in your command PATH when you run this.

Using Public Key Authentication Instead of Using a Username/Password

Once the above components are in place, a key-pair must be generated from the SSH client and the public-key uploaded to our SSH Server. Please contact FMS Operations to schedule a time to work with KFS staff to perform the following setup.

General Steps to Configure a Key Pair for Public Key Authentication

1. Use the SSH client's tool for generating and saving a public/private key pair.
2. Make a connection to dtt.iu.edu or dtp.iu.edu, designating the private key for authentication.

o If this is the client's first connection to this server, the client will be prompted to save the host key and they should reply 'yes' or 'ok'.
o On their first connection with the new private key, they will need to authenticate with their password.
o At that point the server, either quietly or after prompting the client to save their public key on the server, will store the public key, derived from their private key, in the correct format, in the correct location; \SSH home\.ssh2\%username%\authorized_keys2.

Manually Configuring The Public Key

If the above auto-upload of the public key does not work properly, the client will need to save a copy of their public key, and make that key available to ESA for configuration.
If they do not already have a copy of a public key file saved, they should be able to use their client's tool for generating key pairs to generate and save a public key that is derived from their saved private key.
To make that public key file available to ESA, they can (1) connect to dtt.iu.edu or dpt.iu.edu using password

authentication and place the contents of their public key file into \SSH home\.ssh2\%username%\authorized_keys2. The contents of the key needs to go into \SSH home\.ssh2\%username%\authorized_keys2.

- That file can hold more than one key if desired.

- The key needs to be in the correct format.

- If the file contents begins with 'ssh-dss' followed by a long string of characters, it is in the proper format and can simply be copied into the authorized_keys2 file (or if it is the only key, the file can simply be renamed).

- If the file contents begins with '---- BEGIN SSH2 PUBLIC KEY ---- Comment:' it will need to be converted.

Things To Keep in Mind

Server Name To Connect To

We recommend using the FQN (fully qualified name) for the alias DTP.IU.EDU when connecting because it is the most reliable. But, whether you use the FQN, or the shorter DTP, it is important to connect using the same syntax each time. Otherwise, you will be prompted to save multiple hostkeys from the SSH Server on DTP (or DTT) because SSH treats "DTP" and "DTP.IU.EDU" as two different hosts when it comes to hostkeys.

The First Time You Connect

You will be presented with the fingerprint of a hostkey and prompted to save the hostkey. Accept the hostkey and continue. From then on, it will not prompt you about the hostkey, as long as you connect using the same server name. Once connected, you are in the /HOME folder. If you are automating the process, the first connect and acceptance of the host key needs to be performed manually since it is an interactive activity.

1. **How Do I Submit a Collector File?**
   The non-enterprise application that creates the Collector file will use Secure Copy (SCP) or Secure File Transfer SFTP with public key authentication or password authenication to drop the file to the IU server 'DTT. iu.edu' (for test) or DTP. IU.EDU (for production) in the directory '/HOME/ KFS/gl/collector.' Once the file has been completely transferred the non-enterprise application will drop a '.done' file which has the same name as the data file to indicate the complete ID Billing file has been transferred. This done file can be empty

2. **How Should My File Be Named?**
   The file name specifications are: gl_idbilltrans_chartorg_yyyymmddhhmmss.data and gl_idbilltrans_chartorg_yyyymmddhhmmss.done. For example, gl_idbilltrans_BADSER_20060105.08.46.00.data and gl_idbilltrans_BADSER_20060105.08.46.00.done. The chart and org should match the second and third fields in the collector file in the header record starting in position 5. A carriage return is required at the end of each line/record in the file.