Secure File Transfer

Overview

In the course of doing business, SheerID may need to send and receive files to and from partners and customers. It is essential that these files are transmitted and stored in a secure manner, as they may contain proprietary, personally-identifiable information or other confidential data. This document outlines SheerID's approved strategies for such file transfers. While the scope of this document is limited to the approved file transfer mechanisms, it is important for both parties to also ensure that sensitive files are handled securely once they have reached their destination, and securely destroyed once their purpose has been realized.

Inbound File Transfer (To SheerID)

The following methods are allowed for transferring a file from an external party to SheerID. With either of these strategies, the SheerID contact will confirm the delivery and integrity of the file transferred immediately upon receipt.

Encrypted Email (PGP)

Sensitive files may be sent via an encrypted email or an encrypted email attachment to an approved SheerID email address using its public PGP key (see Appendix A). There are a variety of software solutions available for encrypting email, including OpenPGP, GPG4Win, Enigmail.

Secure FTP (FTPS)

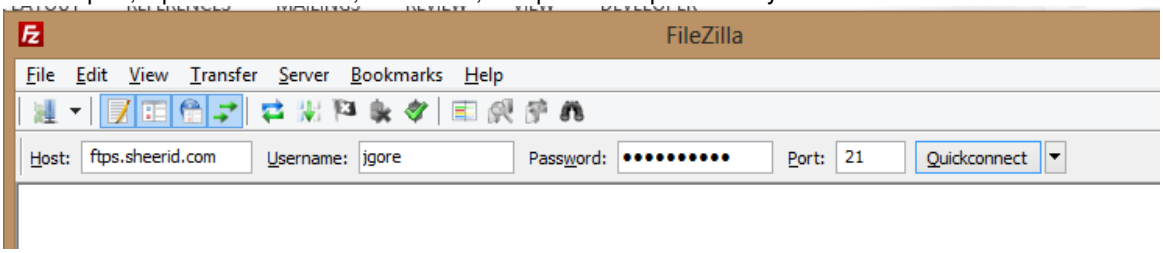
SheerID can provision a secure FTP account for the sender to transmit the file. This server uses FTPS (explicit TLS over FTP, not to be confused with SFTP) to ensure secure password and data transfer. Once the file has been transferred to SheerID, it will be removed from the FTP server.

Server Details

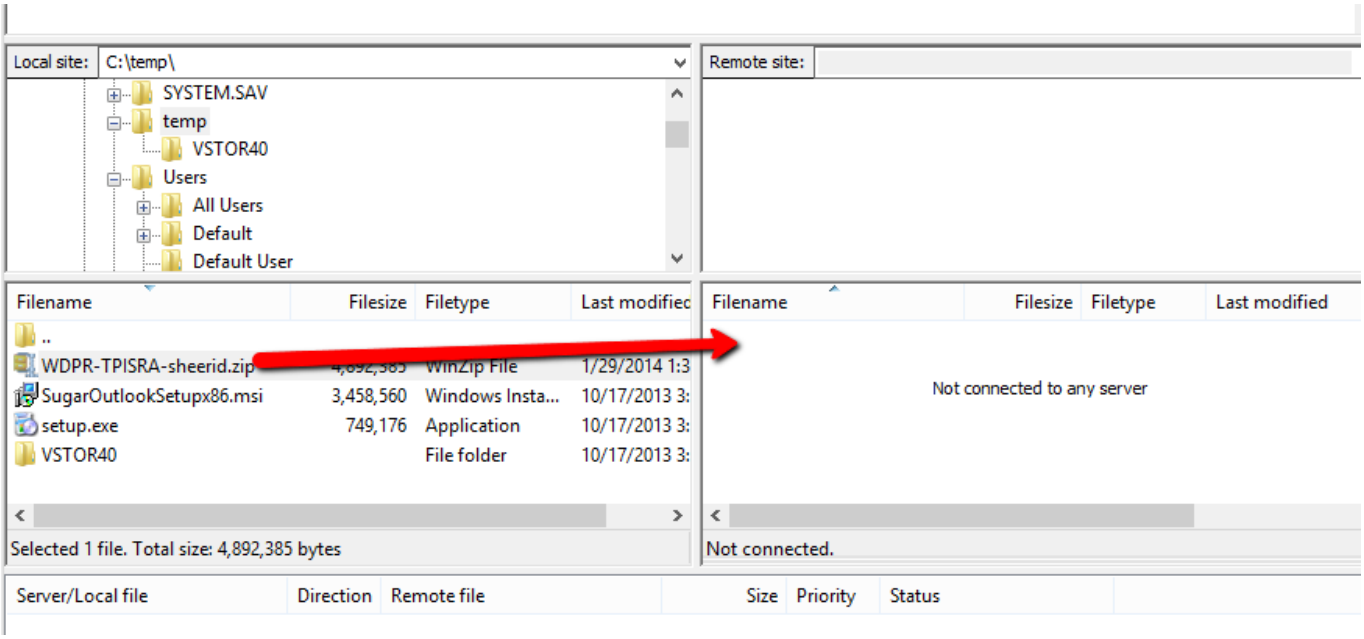
- Host: ftps.sheerid.com
- Port: 21
- Username: [generated upon request]
- Password: [generated upon request, delivered via phone]

FTP Instructions

1. Install an "FTP Client" of your choice, such as FileZilla or CyberDuck for Mac
2. Once Open, input the hostname, username, and password provided by SheerID



3. Drag the file to transfer from your computer /local site (left side of screen) to the desired FTP location / remote site (right side of screen)



4. Inform your contact at SheerID that the file has been transferred. You will be notified when receipt has been confirmed.

More information can be found on the Wikipedia page for FTPS.

Outbound File Transfer (From SheerID)

The following methods may be used to transfer a confidential file from SheerID to an external party. With either of these strategies, the external contact should confirm the delivery and integrity of the file transferred immediately upon receipt.

Encrypted Email (PGP)

If a PGP public key exists for the external contact email address, SheerID may send an encrypted email or encrypted email attachment to that address.

Secure FTP (FTPS)

SheerID may provision an FTPS account for the purpose of transmitting the file. If an FTPS account has already been provisioned for an external party, that account may be used to send files back. The external contact should remove the file(s) from the FTPS account once receipt has been confirmed.

Appendix A: SheerID Email Addresses with PGP Keys

The following key information may also be available on a key server, for example MIT PGP Public Key Server. As a result, these keys may be discoverable from within a mail client.

alex@sheerid.com

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.3

mQENBFJVdm4BCACnFE6XxA8Exradw9/Y66fmiI+NDfdJpgQcFu8BDpBavL4JHV5jf5YjgyoX
lPiqet0q2t5gNfEfLLjpTEWMJhrcYyQT3XC0qbBxqzNmuZuRnL46wyC11qoxFmYNpsDIsDqS
FrM2mquIAMIDWK5VGdDhdxWp3+O1wMKRPa85PREQETcl9oAfsTbTMRAo7HdO0+KWT8UevGS6
tIuKwL4le6jWYmoqDLmfR3hqNBrA8xWDPr+IyT1xXmfOotD9J11yGdEuJrH0vMagLYnMBkjo
JWjZgU87ZPVLlZaJxna8Kq9pJhCLrNNu51Nxmeb2n6GQIjncX6kchkZlrvpqr09eB94XABEB
AAG0HUFsZXggQm9vbmUgPGFsZXhAc2hlZXJpZC5jb20+iQE9BBMBCgAnBQJSVXZuAhsvBQkH
hh+ABQsJCAcDBRUKCQgLBRYCAwEAAh4BAheAAAoJEAFcvQDIj4JgbNEH/2CFKiHiixbiVE3v
sxq35E8UfOPcjkPSomYJOrarORmjsT1uH4lsMKGeE2EV2SMmrjYsiutkhdWgEF1KBxWZCLFi
dFx8mSdDt+IJjnwiCVgRtWhr1pjaSa6CH/KvvMrHrkzl9OzL8eDb18+GuGti4U6D1hzKiSvj
9nU0EXN2KGX830Av+G/v8mnscv/nkN3QCr4X3dy4Mu0JwV5S8rpf+KJ+OIDErOTb5d+YO4sL
WMNXSI0gEn0Y/Ebvz/YDzSCrS4QqViUN+nEPVtf171Hxry7ewCXzYbXVKEqF69FtJmNTxpVs
9OVDGyg72T7lEYBn/5yJ1INMOWxhw7Z/+0OFr9+5AQ0EUlV2bgEIAKA1ofYwas2HV/JgAJAn
2PRnMxyMXnfcPvtfvCSU4O0nN+ArwiYlMTagps6raHkTnkFR9HoZxHHOhU6F/xIkY25rjXkP
LMxlA+P1Y3WYWCgwqbygQ7XHpjDcfzjZjp/LnhVikZ9PUYWnyOY8Bal04jWMeDudWOocEYiw
VXpatzzlGhVz+Cx99bLOxdXunXeGOVtIIZ7/JJX362QnvYqAxZsUExCiB505Rv1aZm6iJgis
xD8zLk3pXjtjCl67ZlCBl9fKRY5yQI3p1+id9SujW9KB62ALqzKk2l7zxbIakiEqhz4VGFEU
g8pnHb0qxm6NuJSzYZa+6tI0w94k4tFU1r0AEQEAAYkCRAQYAQoADwUCUlV2bgIbLgUJB4Yf
gAEpCRABXL0AyI+CYMBdIAQZAQoABgUCUlV2bgAKCRAAyGCRjGA7tASeB/wLdyj+Vy2mWbs2
1Z2P5v0TNHqQwHbg9PiZTFmIqUOHaQd1x5VNTNzMKGfplAiDcEGDyqrDFhbw05+ZSz+gbEEm
6dSvObQaM2cU8fIeIrnSBJUQ9V1InPgaAQrcFALV8xwka//DvJkIfl6N9TwT8tjlJWyUzJC2
/2xHBZUmX5KYx6b5IX0bp8x6yABB3sENhs9lTL1CUEfN3kvIQ4flp3uIBuVdpU7oJW9xszAp
BBo2IKBrYQwd+zniSW+KXXNl0vckDTRYP8Ews1Clbnov6J7iecBgNpVDUTzR1WEXxIUsLgJx
cHE1E0uWdCwk0iPwfSJVFexyuN5D3Ovoy4eOqa0IYiMH/jZzGGRf6b/ybC0aOe3H+w3/zBu4
1mPjdAr6oBjjEsjsFZcZLq0s4vj0t9Y44udargirpDvxXprlc3Q5DPlyIDTqLOsHJ6zT9SuR
mbhTTwvAoImcqcvUxOC0AlziJkjn3hQkUMvDY5pUEtIOxdBiXvuOU0p9qHnge9lUekOQ3H/8
3UFg/lZBrC31/Qvngh5tB//zQYsaihycZkF3h+8b3zbHw8BN/2E93DeRMN73pndWu51i/miW
6BU6+C7C9/gm6Z4ys8dMAN2cS+GS4ml2/q/mJ7pT0xsLOFwb34Jt8ZYChlOpCBZEtNERdwP8
A+1E5YKZt4mZjfJCdvzs5WQbcc4=
=02GV
-----END PGP PUBLIC KEY BLOCK-----