CONNECTIVITY

Secure File Transfer Protocol (SFTP)

Trading partners choosing this option will connect through a firewall to a Windows server on the BlueCross BlueShield of South Carolina network. You can access this server via the Internet. Additional authentication is done through the use of a unique login ID and public key file. When this authentication is complete, the trading partner will upload files (if applicable) into the inbound directory where they will be uploaded for EDI Gateway processing. When you choose this connectivity option, EDI Gateway will request additional information from the trading partner, such as source public IP address and public key.

Our SFTP server accepts SFTP client connections using the SSH2 secure protocol. The client product our Network Operations department recommends using is SecureFX from VanDyke Software, although any SFTP/SSH2 client that supports public key authentication (SSH2 public key, DSA, 2048-bit) should work.

Choosing an SFTP Client

Your SFTP client needs to support:

SSH2 secure protocol
Public Key authentication (this is different than PGP)

Our SFTP server does not support PGP encryption. Please do not create or try to use a PGP key when authenticating with our server. We recommend VanDyke SecureFX as an SFTP client. There are many other SFTP clients including WS_FTP Professional, Putty, and WinSCP. Every client has its own particular configuration and system requirements imposed by its vendor. Vendors will need to be contacted for software support beyond what is articulated in this document.

Installing an SFTP Client

Install the SFTP client on the workstation(s) and/or server(s) that will connect to our SFTP server.

Notify us of your IP address(es) that will connect to our SFTP server by completing the SFTP Customer Connectivity Parameter Survey form and returning via email to EDIG.Support@PalmettoGBAservices.com. The IP address will be the IP address BlueCross BlueShield of South Carolina EDI Gateway will see coming over the internet. You may need to contact your network staff for this information.

Please notify us promptly of IP address changes (new and discontinued use)

Testing Network Connectivity via Telnet

To verify network connectivity from your location through our firewall to the SFTP server, open a command prompt
(START -> RUN -> *type* CMD):

And type
telnet 208.60.144.253 22

A successful connection is indicated by the message **SSH-2.0-VShell_4_0_1_478 VShell.** If you do not receive this message, your connection probably failed.

Configuration of SFTP Client

Session Configuration

Create a new connection / session:

Host name to connect to = **208.60.144.253**
Port to connect to = **22** (SFTP port)
If a Firewall option is listed, choose NONE

Authentication Configuration

1. Unselect ALL references to password authentication.

   Our SFTP server does not support password authentication. If your SFTP client attempts to connect with password authentication you will receive an error and will not successfully connect.

2. Once authenticated, when asked for User ID, enter your 10-character trading partner id:

   For non-production, use the test trading partner id provided.
   For production, use the production trading partner id provided.

3. Configure the client to use **PUBLIC KEY** authentication.
   Use an existing public key and private key pair
   or
   Create a new public key and private key pair

   When creating a new public key use these settings:
   Key Type = DSA
   Key Length = 2048-bit
   Pass Phrase = whatever you choose

   Email the public key file as an attachment to BlueCross BlueShield of South Carolina EDI Gateway (should be a .pub file). The public key file will be uploaded to the SFTP server. You will then be able to connect to our SFTP server. If your public key changes, you must ensure you notify us and provide the new public key file to avoid interruption in connectivity.

FORMS

South Carolina

BlueCross BlueShield of South Carolina is an independent licensee of the Blue Cross and Blue Shield Association

BlueCross BlueShield of South Carolina Gateway
Trading Partner Enrollment Form

Date: _____

Trading Partner Name: _____

_____

File Format: ☐ **Proprietary** ☐ **HL7 – CCDA** ☐ **Other:** Click here to enter text.

Protocol: ☒ **SFTP**

Primary Contact Person Name: _____

Phone: _____ **Fax:** _____

Address: _____

_____

City: _____ **State:** _____ **ZIP:** _____

Email Address: _____

Secondary Contact Person Name: _____

Phone: _____ **Fax:** _____

Address: _____

_____

City: _____ **State:** _____ **ZIP:** _____

Email Address: _____

Other Contact Person Name: _____

Phone: _____ **Fax:** _____

Address: _____

_____

City: _____ **State:** _____ **ZIP:**

Email Address: _____

BlueCross BlueShield of South Carolina Gateway SFTP Customer Connectivity Parameter Survey

This document is for third parties who want to establish Secure File Transfer (SFTP) connectivity to the EDI Gateway. Complete this form and return it to EDI Gateway. All the information you enter on this survey is confidential. If we must return incomplete survey forms or forms containing inaccurate information, it may delay your service implementation.

Customer Business Contact's Name: _____

Phone: _____ **Fax:** _____

Email Address: _____

Customer Technical Contact's Name: _____

Phone: _____ **Fax:** _____

Email Address: _____

Company Name: _____

Phone: _____ **Fax:** _____

Address: _____

_____

City: _____ **State:** _____ **ZIP:** _____

SFTP Information

Blue Cross Blue Shield of South Carolina Public IP:	208.60.144.253 PORT 22
Customer Static Public IP:	
Customer FTP Client Software Used:	

Notes:

1. EDI Gateway:
   - Uses a Cisco VPN Concentrator
   - Only supports IKE encryption scheme
   - Uses Diffie-Hellman Group 2 (2048 bit)
   - Uses IKE lifetime = 24 hours
   - Accepts SFTP using the SSH2 secure protocol. It does not support PGP encryption. SSH2 Public Key ID is required.
2. Client may use an IPSec compliant VPN Gateway.