

File Transfer

User Guide

For Clients and Vendors

Last Revised: November 1 2017

Table of Contents

- File Transfer User Guide for Clients & Vendors 1**
- Section 1: Overview 1**
 - Confidentiality 1
 - Contact Information & Technical Support 1
- Section 2: Selecting Your Protocol 2**
 - Selecting a File Transfer Protocol..... 2
 - Determine the Method of Data Exchange..... 3
 - Protocol Connection Details 4
 - FTPS and HTTPS - TLS and Cipher Support..... 5
 - SSH Cipher Support..... 5
- Section 3: Authentication and File Transfer Details 6**
 - Account Credentials 6
 - Access Control List 6
 - Time Out..... 6
 - Polling 6
 - SSH Key Authentication 6
 - FTPS SSL Certificate Authentication 7
 - FTPS Client Certificate Authentication 7
 - Directory Structure..... 7
- Section 4: File Format Specifications 9**
 - Text Encoding..... 9
 - File Size 9
 - File Naming – For Clients 9
 - File Naming – For Vendors..... 10
 - PGP Keys 10
- Section 5: Troubleshooting 12**
 - Common Mistakes / Errors 12

File Transfer User Guide for Clients & Vendors

Section 1: Overview

This user guide has been prepared for Concur clients and vendors participating in data exchange through various secure file transfer protocols.

This document supersede[s] any other form of data exchange documentation previously provided by Concur.

For any file transfer with Concur consider and prepare the following information:

- Determine the type of secure file transfer protocol
- Determine the method of data exchange
- PGP and SSH key exchanges
- Process and standards in file naming convention
- Common errors and mistakes

Confidentiality

This document contains sensitive information that may be of value to persons wishing to compromise the security of client data. Although multiple protection methods are employed throughout Concur facilities and systems, clients and vendors are instructed to keep this document confidential and to limit distribution to required personnel only.

Contact Information & Technical Support

The following contact information is for clients & vendors who have a client specific issue.

Region	Contact Information
Americas Monday – Friday 5 AM – 4 PM PT	Expense & Invoice Support +1 877 901 4960 - USA & Canada Expense, Invoice & Travel Support Toll Free: 018000835525 - Mexico Travel Support +1 877 812 5060 - USA & Canada

Region	Contact Information
Asia Pacific Australia Monday – Friday 9 AM – 6 PM AEST/AEDT	<p>Expense, Invoice & Travel Support +61 (02) 9113 7319 - All APA</p> <p>Expense, Invoice & Travel Support +800 2555 6311</p> <p>Australia, China, Hong Kong, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan & Thailand</p> <p>001803442494 - Indonesia</p> <p>120 11520 - Vietnam</p>
Europe Monday – Friday 9 AM – 6PM GMT+1	<p>Expense, Invoice & Travel Support +800 2221 8787</p> <p>Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovak Republic, Spain, Sweden, United Kingdom</p> <p>+44 1753 50 1777 - Mainland Europe</p> <p>01753 50 1777 - United Kingdom</p>

Section 2: Selecting Your Protocol

Selecting a File Transfer Protocol

Concur's preferred and recommended protocol is SFTP (Secure Shell File Transfer).

Do not include the FTP protocol in client file transfer decisions. The FTP protocol will be disabled May 15th, 2018 and any connection attempts via FTP will fail. Note that the FTPS (FTP-SSL) protocol will still be available.

File Transfer Protocol	Considerations
SFTP (Secure Shell File Transfer Protocol)	<p>Concur's preferred protocol.</p> <p>Transmits credentials and data over an encrypted channel.</p> <p>All communication is over a single TCP port, simplifying firewall configuration.</p> <p>Well-suited to automated processing, transferring multiple files.</p>
FTPS (File Transfer Protocol Secure)	<p>Transmits credentials and data over an encrypted channel.</p> <p>Communication is over separate control and data TCP ports, data ports being dynamic. Encryption makes this more difficult to properly allow through firewalls; the full range of dynamic ports must be open.</p> <p>Well-suited to automated processing, transferring multiple files.</p>

File Transfer Protocol	Considerations
HTTPS (Hypertext Transfer Protocol Secure)	<p>Transmits credentials and data over an encrypted channel.</p> <p>All communication is over a single TCP port, simplifying firewall configuration.</p> <p>Manual use only, not suitable for automated processing.</p>

Determine the Method of Data Exchange

You need to determine your preferred method for sending files to Concur and the software used to carry out the exchange of files. You will want to take into account the types of software that our managed file transfer gateway supports.

Concur uses Axway's SecureTransport as our gateway for managing file transfers. In selecting your file transfer software ensure the tool selected is supported by SecureTransport.

The following list is currently supported:

Software Type	Supported Software Versions
SSH Clients	<ul style="list-style-type: none"> • Axway Secure Client 5.8, 6.0, 6.1, 6.2, 6.3 • cURL 7.45 • FileZilla Client 3.14.1 • PSCP 0.60 • PSFTP 0.60 • Tectia Client 6.1, 6.2 • VanDyke SecureFX 7.3.3 • WinSCP only the latest version • Any client that complies with RFCs 4251–4254
SSH servers for server-initiated transfers	<ul style="list-style-type: none"> • Axway SecureTransport 5.1, 5.2.1, 5.3.0, 5.3.1, 5.3.3 • Axway Gateway 6.16.x • OpenSSH 7.1 • Tectia Server 6.2 • VanDyke VShell 4.0.5
FTP/S servers for server-initiated transfers	<ul style="list-style-type: none"> • Axway Gateway 6.16.x • Axway SecureTransport 5.1, 5.2.1, 5.3.0, 5.3.1, 5.3.3 • GlobalSCAPE EFT Server 7.1.0 • IBM Mainframe FTP(S) • Ipswitch WS_FTP 12.4 • Oracle Solaris 10 FTP Server

Software Type	Supported Software Versions
FTP/S Clients	<ul style="list-style-type: none"> • Axway Secure Client 5.8, 6.0, 6.1, 6.2, 6.3 • cURL 7.45 • CuteFTP Professional 9.0.5 (Windows) • FileZilla Client 3.14.1 • IglooFTP PRO 3.9 • Ipswitch WS_FTP 12.4 • LFTP 4.6 • SmartFTP Client 6.0
Browsers for the SecureTransport web clients	<ul style="list-style-type: none"> • Apple Safari 9 on OS X only • Google Chrome latest version • Microsoft Internet Explorer 11 (Compatibility View is not supported) • Mozilla Firefox latest version Microsoft Edge • Microsoft Edge
HTTP clients	<ul style="list-style-type: none"> • All supported browsers for SecureTransport web interface • ST Web Client • Axway Secure Client 5.8, 6.0, 6.1, 6.2, 6.3 • cURL 7.45
HTTP/S servers for server-initiated transfers	<ul style="list-style-type: none"> • Axway SecureTransport 5.1, 5.2.1, 5.3.0, 5.3.1, 5.3.3

Protocol Connection Details

NOTE: There should only be one (1) connection open at a time with any protocol, but we allow up to three (3) open connections if needed.

Protocol	Port	Additional Information
SFTP	22	
FTPS	21 (control) 65400-65500 (data)	Connect with explicit TLS Use passive mode for data transfer Transfer files in binary mode
HTTPS	443	

FTPS and HTTPS - TLS and Cipher Support

Protocol	TLS Version Support	Cipher Support
FTPS	TLSv1.1, TLSv1.2	TLS_ECDHE _RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_EMPTY_RENEGOTIATION_INFO_SCSV
HTTPS	TLSv.1.1, TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_EMPTY_RENEGOTIATION_INFO_SCSV

SSH Cipher Support

Protocol	Key Exchange Ciphers	Transfer Ciphers
SSH	diffie-hellman-group14-sha1; diffie-hellman-group-exchange-sha1; diffie-hellman-group-exchange-sha256	aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc, aes128-ctr, aes192-ctr, aes256-ctr

Section 3: Authentication and File Transfer Details

Account Credentials

Concur's data exchange is secured with a username/password authentication. Your username is your Concur Entity ID.

- Your username and password will be transmitted separately from this document
- Passwords cannot be retrieved, only reset for security purposes
- Concur will never ask you for your password
- Please do not share the password

Access Control List

For US Commercial Clients Only: Connections must originate from public (Internet routable) IP addresses and the IP address must reside on our access control list (ACL). Provide Concur with the public internet-routable IP address(es) from which you will connect to transfer files. Any access attempts from IP addresses not on Concur's ACL will fail with an invalid credentials error. Concur will store up to ten (10) total IP addresses per client for both production and test systems combined.


For our CGE or EMEA clients the above information does not pertain to those environments.

Time Out

After you complete transferring your files to/from Concur, please disconnect your connection. There is a time out for systems that stay idle for a period of time.

Polling

Do not authenticate repeatedly to Concur, as this can trigger a Denial Of Service (DOS) and adversely impacts file transfer performance. Concur recommends connecting no more often than twice in an hour.

 An account will be disabled if its behavior jeopardizes overall file transfer activity and performance.

SSH Key Authentication

- Upload your SSH public key file to your root directory at Concur.
- Keys may be DSS (1024 bit) or RSA (1024-4096 bit, 2048 recommended) format.

- Open a case on the Client Support portal to request SSH key authentication and provide the filename of the SSH key you have uploaded.

FTPS SSL Certificate Authentication

- TLS (SSL) Protocol (ftps, https)

NOTE: Concur's SSL certificate is signed by the chain "C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance CA-3" "/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA".

- You will, at a minimum, need to trust the root certificate. Most client SSL certificate bundles will include this CA. There is likely no action necessary on your part.

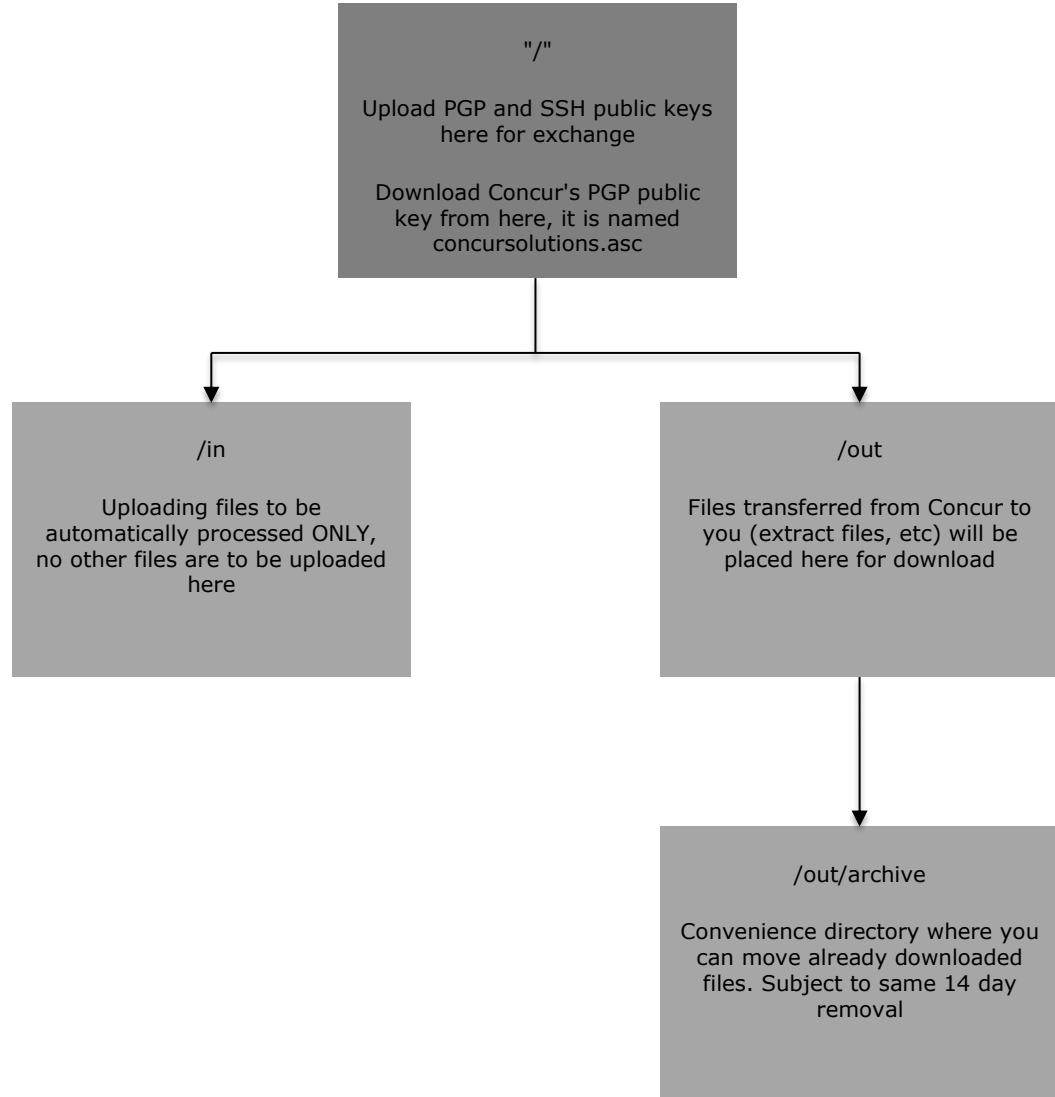
FTPS Client Certificate Authentication

- Upload your SSL certificate to your root directory at Concur.
- We will need the public key of the Certificate Authority signing your SSL certificate (and any intermediates), if not already known to Concur.
 - ◆ A list of acceptable Certificate Authorities is provided as part of the TLS protocol when connecting.
- Open a case on the Client Support portal to request FTPS client certificate authentication and provide the filename of the SSL key you have uploaded.

Directory Structure

Each client and vendor is routed to their own folder, eliminating the ability to traverse into another company's file system.

NOTE: All files are deleted from their ftp directory after 14 days.



For file transfers to Concur, you must upload directly to the correct destination. They should be uploaded into the /in directory with the correct file name. Concur's file handling processes are triggered at the end of a successful upload. Repeated uploads or renaming of files after upload can prevent automated file handling from functioning correctly.

Section 4: File Format Specifications

Text Encoding

Any files uploaded as text must be encoded as ASCII or UTF-8 with a byte order mark (0xef 0xbb 0xbf)

File Size

Uploaded files cannot exceed a size of 1GB uncompressed maximum.

File Naming – For Clients

- File Type
- Entity ID
- Unique visual identifier, this is not evaluated by the system but can be helpful when identifying files, it is not required
- Date and time stamp, preferred format is YYYYMMDDHHMMSS
- Only alphanumeric characters, minus sign (-), underscore (_) and dot (.) should be used in files names

Import File Naming Samples

If there is a file type not listed below and you need further help for naming your files, please contact Client Support.

Import Type	Sample Filename
Attendee Import	attendee_t0001234uv1w_sample_20051206095621.txt.pgp
Employee Import	employee_t0001234uv1w_sample_20051206095621.txt.pgp
List Import	list_t0001234uv1w_test_20051206095621.txt.pgp
Travel Allowance Import	perdiem_t0001234uv1w_test_20051206095621.txt.pgp
Exchange Rate Import	currency_t0001234uv1w_sample_20051206095621.txt.pgp

Extract File Naming Samples

If there is a file type not listed below and you need further help understanding your extract files, please contact Client Support.

Extract Type	Example Filename
AMEX Remittance US	extract_IBCP_t00022598yzv_yyyymmddhhmmss.txt.pgp

Extract Type	Example Filename
AP/GL Extract	extract_CES_SAE_v2_t00022598yzv_yyyymmddhhmmss.txt.pgp
Standard Concur Pay	extract_cp_t00022598yzv_yyyymmddhhmmss.txt.pgp
Standard Travel Request	extract_Travel_Request_Extract_t00022598yzv_yyyymmddhhmmss.txt.pgp

File Naming – For Vendors

Please follow the naming convention that was communicated to you at the time of your initial setup. If you have any issues with the naming of your files please contact: cardfeedsces@concur.com

PGP Keys

All files must be PGP encrypted and we can only support a single key from a client at a time for test and production. Concur currently supports the following OpenPGP-compliant software:

PGP Software	Website
PGP 5.x and above	http://www.pgp.com
GnuPG v1.0.6 and above	http://www.gnupg.org

Any files delivered from Concur to your /out directory will be OpenPGP encrypted. You will need to provide your public PGP key to Concur before those files can be delivered, so that we may encrypt them for you.

Creating your PGP Key

- PGP public key must be formatted as OpenPGP (version 4)
- ASCII-armored keys are supported
- You will need to have a public signing key, and an encryption sub-key (this is the default generated by GnuPG, for example)
- Keys should be either DSS/ElGamal (1024-3072 bit, 2048 recommended) or RSA type 1 (sign and encrypt, 1024-4096 bit, 2048 recommended)
- Set key to never expire

The following is a list of the encryption, hashing, and compression algorithms currently supported by Concur. While we prefer you use the preferences found in Concur's PGP key, you may explicitly use these algorithms when encrypting files to us. You may also set them as preferences in your public key signature for files Concur will encrypt to you.

Type	Supported List
Ciphers	<ul style="list-style-type: none"> • 3DES • CAST5 • BLOWFISH • AES • AES192 • AES256 • TWOFISH • CAMELLIA128 • CAMELLIA192 • CAMELLIA256
Hashes	<ul style="list-style-type: none"> • MD5 • SHA1 • RIPEMD160 • SHA256 • SHA384 • SHA512 • SHA224
Compression	<ul style="list-style-type: none"> • Uncompressed • ZIP • ZLIB • BZIP2

To upload your PGP key

- Transfer your public key in ASCII mode to the root directory of your login
- Open a case on the Client Support portal to request PGP key import, providing the filename of the PGP public keyfile that you have uploaded
- Concur will provide you the key ID and fingerprint of your imported PGP key as a test of successful PGP key ring addition. If you receive the correct key ID from Concur, your PGP key is ready for use

To use Concur's PGP key

Concur's public PGP key must be used for encrypting files sent to Concur and can be permanently found in the root file transfer directory. You may choose to sign the OpenPGP files you send to Concur, but we must already have your PGP key.

Files imported to Concur must be encrypted with Concur's provided public PGP key.

- Download *concur_solutions.asc* from your root directory
- Apply this file as Concur's public PGP key to your system
- Use this key to encrypt all import files destined for Concur

Section 5: Troubleshooting

Common Mistakes / Errors

Common Mistake	Resolution
Login fails because the connection is attempted from an IP not on Concur's Access Control List (ACL)	The IP you are trying to connect from is not on the Access Control List. You have a total of ten (10) slots for IP access and the connection must come from one of those ten IP addresses listed in the access control list. Check your gateway (external/public IP) address first.
Uploading files to a temporary file and then renaming the file	You cannot upload a file to a temporary filename and then change the name. The file you upload must be named correctly at the time of uploading to the /in directory. This could be enabled by default in your client software, please verify your settings.
Invalid public pgp key	We explicitly cannot accept version 3 keys, nor algorithms RSA type 2 (encrypt only) or 3 (sign only)