Shared: File Transfer for Customers and Vendors

User Guide

Last Revised: January 20, 2021

Applies to these SAP Concur solutions:

- ☒ Expense
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Travel
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Invoice
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Request
  - ☒ Professional/Premium edition
  - ☒ Standard edition

Table of Contents

Revision History

Date	Notes / Comments / Changes
January 20, 2021	Added information about the concursolutionsrotate.asc public PGP key. (page 11)
December 14, 2020	Removed TLS_empty_renegotiation_info_scsv from the Cipher Support for FTPS section. (page 4)
November 25, 2020	Updated date when SFTP with SSH key authentication becomes the mandatory protocol for all accounts.
October 23, 2020	Updated several sections with details about creating a new key. Also removed selected text for clarity, added alert to choose strongest cipher supported by SAP Concur and recommendation to use NIST or similar government resource for guidance on ciphers.
April 27, 2020	Renamed the Authorization Request check box to Request on the guide's title page; cover date not updated
April 17, 2020	Updated Sections 2, 3, 4, and 5.
March 14, 2020	Updated to reflect EoS for HTTPS on February 24.
February 14, 2020	Updated to reflect EoS for TLSv1.1 and time change from 8 am to 2 pm for HTTPS changes on Feb 24.
January 29, 2020	Updated to reflect EoS for TLSv1.1 on Feb 10 and HTTPS on Feb 24.
January 15, 2020	Updated the copyright; updated China terminology to Hong Kong, China and Taiwan, China
November 9, 2019	Updated multiple sections with information about deprecated protocols and protocol versions (FTPS, HTTPS, and TLS).
September 21, 2019	Updated *File Transfer DNS endpoints/IPs* section.
July 18, 2019	Added information about SFTP with SSH Key Authentication. Updated the list of supported SSH key exchange ciphers and transfer ciphers.
July 9, 2019	Made several cosmetic fixes to footer, doc properties, etc. No revision date change.
May 22, 2019	Converted fact sheet into formal Guide.

File Transfer for Customers and Vendors

Section 1: Overview

This user guide has been prepared for SAP Concur customers and vendors participating in data exchange through secure file transfer.

This document supersedes any other form of data exchange documentation previously provided by SAP Concur.

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

- SFTP with SSH Key Authentication is required for all new file transfer.
- Beginning April 10, 2021, SFTP with SSH Key Authentication is required for all file transfer accounts.
- 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 customer data. Although multiple protection methods are employed throughout SAP Concur facilities and systems, customers 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 customers & vendors who have a customer-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	**Expense, Invoice & Travel Support** +61 (02) 9113 7319 - All APA **Expense, Invoice & Travel Support** +800 2555 6311 Australia, China, Hong Kong, China, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, China & Thailand 001803442494 - Indonesia 120 11520 - Vietnam
Europe Monday – Friday 9 AM – 6PM GMT+1	**Expense, Invoice & Travel Support** +800 2221 8787 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 +44 1753 50 1777 - Mainland Europe 01753 50 1777 - United Kingdom

Other Resources – National Institute of Standards and Technology (NIST)

Clients may take advantage of the security recommendations available at National Institute of Standards and Technology (NIST) or a similar government agency to guide your choice of the very most secure connection for the strongest security posture.

Section 2: File Transfer Protocol

All new accounts must use SFTP (Secure File Transfer Protocol) with SSH (Secure Shell) Key Authentication. Beginning on April 10, 2021, all existing accounts must use SFTP with SSH Key Authentication and FTPS will not be allowed.

File Transfer Protocol	Considerations
SFTP (Secure File Transfer Protocol)	**The SAP Concur mandatory protocol (with key authentication) for new accounts as of the June 2019 release and for all accounts as of April 10, 2021.** Transmits credentials and data over an encrypted channel. All communication is over a single TCP port, simplifying firewall configuration. Well-suited to automated processing, transferring multiple files.

File Transfer Protocol	Considerations
FTPS (File Transfer Protocol Secure)	**As of April 10, 2021, FTPS is no longer allowed.** Transmits credentials and data over an encrypted channel. 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. Well-suited to automated processing, transferring multiple files.

Protocol Connection Details

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

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

FTPS - TLS and Cipher Support

⚠ SAP Concur recommends choosing the very strongest cipher supported both by SAP Concur and the client site in order to maintain a strong security posture.

Protocol	TLS Version Support	Cipher Support
FTPS **FTP/S is not an option for new accounts and, as of April 10, 2021, all accounts must use SFTP with SSH key authentication.**	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

SSH Cipher Support

⚠ SAP Concur recommends choosing the very strongest cipher supported both by SAP Concur and the client site in order to maintain a strong security posture.

Protocol	Key Exchange Ciphers	Transfer Ciphers
SSH (SFTP)	diffie-hellman-group14-sha1; diffie-hellman-group-exchange-sha256	aes128-ctr, aes192-ctr, aes256-ctr

Section 3: Authentication and File Transfer Details

File Transfer DNS Endpoints/IPs

The following file transfer DNS endpoints are used by SAP Concur:

For US and EMEA accounts created before 3/25/2020:

- US: st.concursolutions.com (12.129.29.5)
- EMEA: st-eu.concursolutions.com (46.243.56.11)

For US and EMEA accounts created after 3/24/2020:

- US: mft-us.concursolutions.com (12.129.29.138)
- EMEA: mft-eu.concursolutions.com (46.243.56.21)

For CGE accounts:

- CGE Stable: st-cge.concursolutions.com (12.129.29.201)
- CGE DR: st-cge-dr.concursolutions.com (199.108.17.109)

NOTE: SAP Concur recommends connecting to the DNS endpoint since IP addresses are subject to change.

Account Credentials

The SAP Concur data exchange is secured using username/password or username/key authentication. For clients, your username is your Concur Entity ID.

- SSH Key Authentication using SFTP is required for new accounts.
- Current passwords cannot be retrieved.
- If you no longer have your password and need to authenticate, open a case on the SAP Concur support portal to request SSH key authentication and attach your SSH public key file to the case.
- SAP Concur will never ask you for your password.
- Do not share your password.

NOTE: New SAP Concur accounts must use SFTP with SSH Key Authentication, and, as of April 10, 2021, existing accounts must use SFTP with SSH Key Authentication.

Access Control List for st.concursolutions.com (12.129.29.5)

Connections must originate from public (Internet routable) IP addresses and the IP address must reside on our access control list (ACL). Provide SAP 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 the SAP Concur ACL will fail with an invalid credentials or connection refused message. Concur will store approximately ten (10) total IP addresses per customer for both production and test systems combined. Reasonably sized IP ranges are allowed if a business case is presented by the customer and approved by SAP Concur.

Time Out

After you transfer your files to/from SAP Concur, disconnect your connection. Connections that are idle for an extended period will time out.

Polling

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

⚠ IMPORTANT: An account will be disabled if its behavior jeopardizes overall file transfer activity and performance. This may include disabling IP addresses which would affect other accounts attempting to connect with the same IPs.

Account Locking

NOTE: This information pertains to the following DNS endpoints:

- st.concursolutions.com (12.129.29.5)
- st-eu.concursolutions.com (46.243.56.11)
- st-cge.concursolutions.com (12.129.29.201)
- st-cge-dr.concursolutions.com (199.108.17.109)

User accounts will be locked after five (5) consecutive failed authentication attempts. The customer will not receive an account locked message, it will appear as if they are entering an incorrect password even after the account is locked. Customers who have locked themselves out of their accounts should contact SAP Concur support to have their account unlocked.

SSH Key Authentication (SFTP)

- Keys must be RSA format (2048-4096 bit, 2048 recommended).
- For new file transfer accounts, provide your SSH public key file to SAP Concur.
- For existing accounts, open a case on the SAP Concur support portal to request SSH key authentication and attach your SSH public key file to the case.

FTPS SSL Certificate Authentication

- TLS (SSL) Protocol (FTPS is not an option for new accounts. As of April 10, 2021, existing FTPS accounts must use SFTP with SSH key authentication.)

  NOTE: The SAP Concur 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 customer SSL certificate bundles will include this CA. There is likely no action necessary on your part.

FTPS Client Certificate Authentication

- FTPS Client Certificate Authentication is not an option for new accounts. As of April 10, 2021, existing FTPS accounts must use SFTP with SSH key authentication.
- Upload your SSL certificate to your root directory at SAP Concur (x.509 pem format)
- We will need the public key of the Certificate Authority signing your SSL certificate (root and intermediates), if not already known to SAP Concur.
- Open a case on the SAP Concur support portal to request FTPS client certificate authentication and provide the filename of the SSL key you have uploaded.

Directory Structure

Each customer and vendor is setup with their own directory structure. They do not have the ability to traverse to other directories.

NOTE: All files are deleted from client/vendor file transfer directories after 14 days.

"/"

- Upload your PGP public key here, your files created by Concur will be encrypted with this key.
- Download the SAP Concur PGP public key, concursolutionsrotate.asc. All files uploaded to SAP Concur for processing must be encrypted with this key.

📖 Refer to *To use the SAP Concur PGP key* in *Section 4* of this document for more information.

"/in"

- Upload ONLY properly named encrypted files you want processed.
- The SAP Concur file handling process is triggered at the end of a successful upload. As such, renaming files and repeated uploads are not allowed and will have unexpected results.

"/out"

- Files created by SAP Concur (extracts, etc.) will be encrypted with your PGP key and placed here for you to download.

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 Customers

- File Type
- Entity ID
- Unique visual identifier

NOTE: The unique visual identifier is not evaluated by the system but can be helpful when identifying files, it is not required.

- Date and time stamp

NOTE: The preferred format is YYYYMMDDHHMMSS

- Only alphanumeric characters, minus sign (-), underscore (_) and dot (.) should be used in file names
- Spaces are not allowed in file 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 SAP Concur 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 SAP Concur support.

Extract Type	Example Filename
AMEX Remittance US	extract_IBCP_t00022598yzv_yyyymmddhhmmss.txt.pgp
AP/GL Extract	extract_CES_SAE_v2_t00022598yzv_yyyymmddhhmmss.txt.pgp

Extract Type	Example Filename
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

NOTE: Spaces are not allowed in file names.

PGP Keys

All files must be PGP encrypted. SAP Concur can only support a single key from a customer at a time for test and production.

Any files delivered from SAP Concur to you / out directory will be OpenPGP encrypted with your PGP key.

Creating your PGP Key

- Use OpenPGP compliant software
- PGP public key must be formatted as OpenPGP (version 4)
- Keys should be RSA (sign and encrypt, 2048 to 4096bit, 2048 recommended). This is the default GnuPG option when generating keys.
- You will need to have a public signing key and an encryption sub-key

Guidelines and Tips When Creating your PGP Key

Customers may rotate keys at any time by following these instructions but must restrict this action to a single supported key as stated above. Be sure to create your new PGP key in *advance* of the expiration of the current key to ensure your file transfers are not interrupted. Additionally, specifying an expiration date supports a best practice policy of regular rotation. However, this is optional and SAP Concur supports customer keys with no specified expiration date.

⚠ SAP Concur strongly recommends rotating keys every 2 years at minimum, or at any time you believe the key might be compromised, to maintain a strong security posture.

The following is a list of the encryption, hashing, and compression algorithms currently supported by SAP Concur. While we prefer you use the preferences found

in the SAP Concur PGP key, you may explicitly use these algorithms when encrypting files for us. You may also set them as preferences in your public key signature for files SAP Concur will encrypt for you.

⚠ SAP Concur recommends choosing the very strongest cipher supported both by SAP Concur and the client site in order to maintain a strong security posture.

Type	Supported List
Ciphers	• 3DES • CAST5 • BLOWFISH • AES • AES192 • AES256 • TWOFISH • CAMELLIA128 • CAMELLIA192 • CAMELLIA256
Hashes	• MD5 • SHA1 • RIPEMD160 • SHA256 • SHA384 • SHA512 • SHA224
Compression	• 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 SAP Concur support portal to request PGP key import, providing the filename of the PGP public keyfile that you have uploaded
- SAP 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 SAP Concur, your PGP key is ready for use

To use the SAP Concur PGP key

Files uploaded to SAP Concur must be encrypted with the SAP Concur public PGP key, concursolutionsrotate.asc:

- concursolutionsrotate.asc
  - Key file is available in the client's root folder
  - RSA 4096-bit signing and encryption subkey
  - Key expires every two years
  - Client is responsible for replacing the key before it expires
    - Next expiry date: September 4, 2022
    - SAP Concur plans to replace the current rotating public PGP key in the client's root folder 90 days before the expiration date

You can choose to sign the OpenPGP files you send to SAP Concur, but SAP Concur must already have your PGP key.

⚠ **IMPORTANT**: The SAP Concur legacy PGP key is still supported for existing clients but will be deprecated in the future. SAP Concur recommends all clients use the more secure rotating public key, concursolutionsrotate.asc.

Section 5: Troubleshooting

Common Mistakes / Errors

The following list provides solutions for the most common errors you may encounter. Be sure to use the resources at NIST or a similar government agency to guide your choice of the very most secure connection for the strongest security posture.

Common Mistake	Resolution
Login fails to our US environment (st.concursolutions.com, 12.129.29.5) because the connection is attempted from an IP address not on the SAP Concur Access Control List (ACL)	The connection must come from one of the addresses listed in the SAP Concur ACL. Check your gateway (external/public IP) address first.
Uploading files to a temporary file and then renaming the file	You cannot upload a file with 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)

Common Mistake	Resolution
Files uploaded to SAP Concur encrypted with the client's PGP key.	Files that you upload to SAP Concur for processing must be encrypted with our SAP Concur PGP key. For information, refer to the *PGP Keys* section of this document.
Attempting to connect to SAP Concur with unsecure SSH protocol algorithms/ciphers.	You will not be allowed to connect if you are attempting to use unsecure algorithms/ciphers that SAP Concur does not allow. We recommend your file transfer software auto selects what is used based on the algorithms/ciphers that we have in common. To have compatible selections, you might have to upgrade your software to the latest version.
Your account is locked after five consecutive failed login attempts. You might receive an incorrect password error when your account is locked.	Contact SAP Concur support to have your account unlocked.