Shared: File Transfer for Customers and Vendors

User Guide

Last Revised: March 1, 2022

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
May 2, 2022	Fixed a bookmark/TOC issue; cover date not updated.
March 1, 2022	Updates throughout.
January 21, 2022	Updated the copyright year; no other changes; cover date not updated
August 27, 2021	Updated information about ciphers and CCPS.
May 13, 2021	Removed an email address reference. No cover date change.
April 21, 2021	Updated to reflect that SFTP with SSH Key Authentication is required for all file transfers.
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 clients and vendors that meet the following criteria:

- Participating in data exchange through secure file transfer
- SAP Concur entity is in one of the DNS Endpoints listed in Section 3 of this guide or an EU2/US2 entity that needs to access Image Delivery Extracts via the US or EMEA endpoints

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.

Security Recommendations

Clients can 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 most secure connection for the strongest security posture.

Section 2: File Transfer Protocol

All accounts must use SFTP (Secure File Transfer Protocol) with SSH (Secure Shell) Key Authentication. Other protocols and SFTP with password authentication are not allowed.

File Transfer Protocol	Port	Considerations
SFTP (Secure File Transfer Protocol)	**22**	**The SAP Concur mandatory protocol (with SSH key authentication)** 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.

Cipher Support

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

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

NOTE: For CCPS, SAP Concur uses FIPS validated ciphers. If you need a list of supported ciphers for CCPS, open a case on the SAP Concur Support Portal.

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)

For CCPS accounts:

- mft-usg.concursolutions.com (52.222.82.120, 160.1.102.62, 15.200.49.20)

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

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.

SFTP with SSH Key Authentication

- SFTP with Username and SSH Key Authentication is required for data exchange with SAP Concur.
- For clients, username is your Concur Entity ID.
- Keys must be RSA format (2048-4096 bit, 2048 recommended).
- Provide your SSH public key file to SAP Concur.
- We allow up to 10 SSH keys per account.

Directory Structure

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

NOTE: All files are deleted from account file transfer directories after 14 days.

"/"

- 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 the *To use the SAP Concur PGP key* section in *Section 4* of this document for more information.

"/in"

- Upload ONLY properly named encrypted files you want processed.

"/out"

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

Legacy File Move Migration

Clients whose entities are currently configured to use the legacy file move process within SAP Concur are being migrated to a more efficient and secure file routing process.

With the legacy process, clients had to wait for the file move schedule to run at a specified time. With the more efficient process, extracts and other outbound files from SAP Concur will be available within the existing overnight processing period shortly after the files are created.

Best Practices

Time Out

After you transfer your files to/from SAP Concur, close 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 per hour.

Miscellaneous

- Do not rename files. Renaming a file will have unpredictable results.
- Do not upload the same file repeatedly.

⚠ **IMPORTANT:** An account will be disabled if these best practices are not adhered to and/or the account's behavior jeopardizes overall file transfer activity and performance.

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 the maximum allowed size of 1GB of uncompressed data.

File Naming – For Clients

- 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 in 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
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 accounts.

Any files delivered from SAP Concur to your /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

You may rotate keys at any time by following these instructions, but you must restrict this action to a single supported key as stated above. Be sure to create your new PGP key in *advance* of your current key's expiration to ensure your file transfers are not interrupted. 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.

⚠ If you require a list of the encryption, hashing, and compression algorithms currently supported by SAP Concur, open a case on the SAP Concur Support Portal. You must use preferences found in the SAP Concur PGP key when you encrypt files to be uploaded to SAP Concur.

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

To provide a new PGP key after initial setup

- **Clients**: Open a case on the SAP Concur support portal to request PGP key import, attaching your PGP public key file to your case.
- **Vendors**: Email your SAP Concur contact, attaching your PGP public key file to the email.

To use the SAP Concur PGP key

Files uploaded to SAP Concur must be encrypted with the SAP Concur public PGP key:

- concursolutionsrotate.asc
  - Key file is available in your root folder
  - RSA 4096-bit signing and encryption subkey
  - Key expires every two years
  - You are 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 your 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 to verify your signature.

⚠ **IMPORTANT**: The SAP Concur legacy PGP key will be supported for existing accounts until October 10, 2022.

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.

Common Mistake	Resolution
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 when you upload it 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)
Files uploaded to SAP Concur encrypted with the account'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.