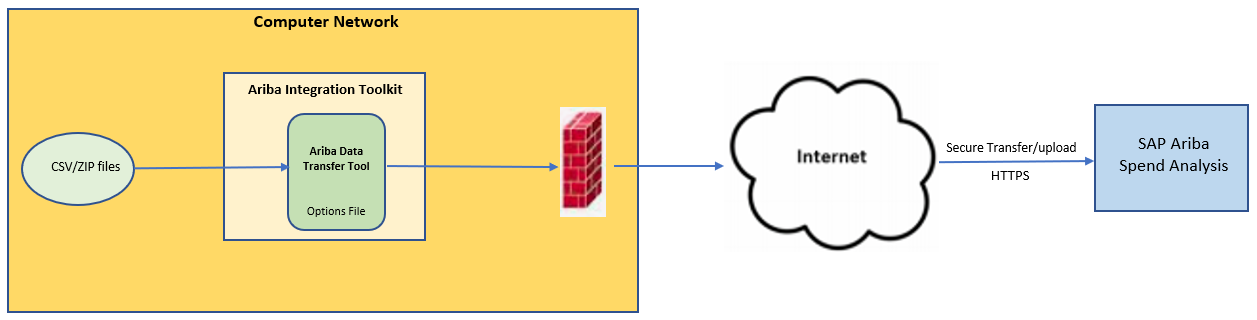
**INSTALLATION and CONFIGURATION of the SAP Ariba Cloud Integration Toolkit (ITK) for Spend Analysis data file uploads:**

The SAP Ariba integration toolkit consists of the SAP Ariba data transfer tool, a command-line utility that facilitates a CSV/ZIP file transfer (upload) in batch mode from a local computer on your network to your SAP Ariba Spend Analysis site. The tool uses a configuration file referred to as the “options” file and uses the parameters specified therein to accomplish the data file transfer. (Note: The parameters you specify in the configuration file can be overridden using options at the command line, however, the configuration file must exist with parameters specified, before you can use the SAP Ariba Integration Toolkit.)



**Installation and Configuration Steps:**

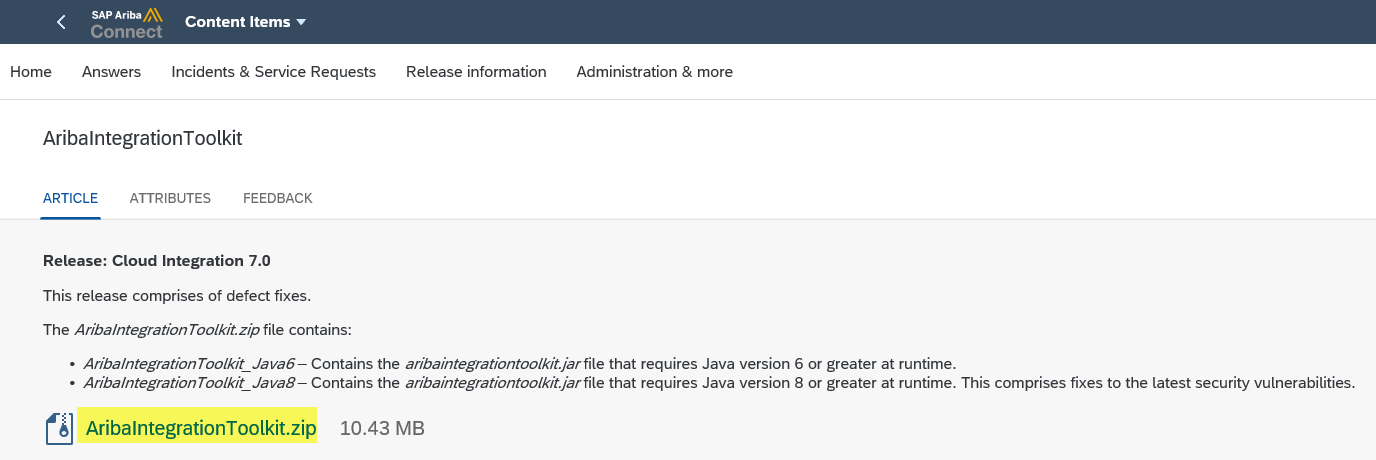
1. Prerequisites/Minimum Hardware/Software/Other requirements:

- The ITK hardware requirements are very basic, however, the machine/system running the ITK must be able to access the Internet and must have access (locally or on a remote machine) to the data file extracts to be uploaded to Spend Analysis (SA).

- The ITK may be installed either on a Windows or a UNIX-based system

- Java JRE 1.6 or higher must be installed on the system where the ITK will be installed (if you choose to download “AribaIntegrationToolkit\_Java8” in step 2 below, you must install JRE 1.8 or higher).  
- You are expected to know how to run scripts on the command line in either UNIX or Microsoft Windows. You must also understand environment variables and know how to edit scripts/batch files.  
Note: The command prompt instructions listed below are based on a Windows/Batch (.bat) file environment. These steps will need to be adjusted as needed for a Unix/.sh environment.)

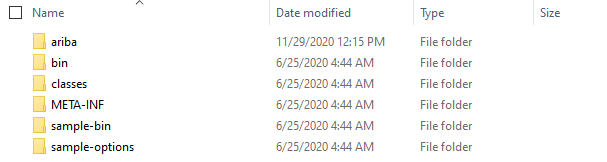
1. A Designated Support Contact (DSC) from the customer side, may download the latest Cloud Integration (Integration Tool Kit – ITK) jar file from <https://connectsupport.ariba.com/sites#item-view&/116093>



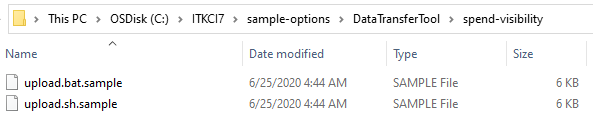
1. Create the ITK installation directory on the PC/system that the ITK is to be installed on. For example create C:\ITKCI7 - this directory name lists the ITK version "Cloud Integration 7.0", as a best practice, just in case you need to upgrade the ITK at some point, you can install a newer version in a separate directory. For example, "C:\ITKCI9"



1. Extract contents of the jar file downloaded in step 1 to this directory - C:\ITKCI7 - The ITK is now installed. Now we will have to configure the SA ITK Upload.bat also known as the "Options" file.

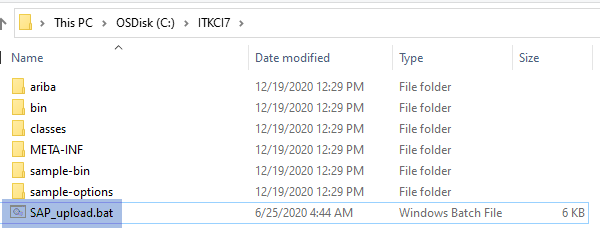


1. Go to "C:\ITKCI7\sample-options\DataTransferTool\spend-visibility"



COPY upload.bat.sample (use “upload.sh.sample” instead, for an UNIX system) and paste in the ROOT of C:\ITKCI7

1. Go to C:\ITKCI7 and rename upload.bat.sample to SourceSystemName\_Upload.bat for example: "SAP\_upload.bat"



1. Edit the options file “SAP\_upload.bat” with a Text Editor (do not use notepad.exe for readability issues)
2. In the options file make the following parameter changes:
3. **JAVA\_HOME**

Set “JAVA\_HOME” to the location of JAVA (jre) on your system, as per step 1. Specify the full path to the Java JRE executable, java.exe, up to, but not including the bin directory. For example: “set JAVA\_HOME=C:\Program Files\Java\<jre version>”

1. **site**

Set "site=mycoolcompany" to your actual Ariba site name for example, "site=actualrealmname". The site name can be obtained within the SA site URL. For example: <https://s1.ariba.com/Sourcing/Main?realm=actualrealmname>

1. **serviceMode**

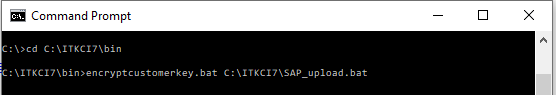
Change “set serviceMode=-1" to "set serviceMode=0" (0 is for OnDemand)

1. **encryptionKeyPath**

(Note: In this step you would select a customer encryption key and use the “encryptcustomerkey” utility to encrypt it. Next, in step e., you would use the “encryptstring” utility (that uses the customer encryption key created in step d.) to encrypt the integration password. The encrypted integration password will differ based on the customer encryption key created in step d.)

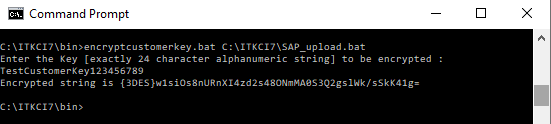
Uncomment "::set encryptionKeyPath=" by removing colons -> "set encryptionKeyPath="

1. Open a Command Prompt and navigate to the ITK installation directory "cd C:\ITKCI7\bin"
2. Within the command prompt under C:\ITKCI7\bin enter the following command for example, "encryptcustomerkey.bat C:\ITKCI7\SAP\_upload.bat" (note: instead of “SAP\_upload.bat” use whatever you have named the .bat options file as, in step 6 above)

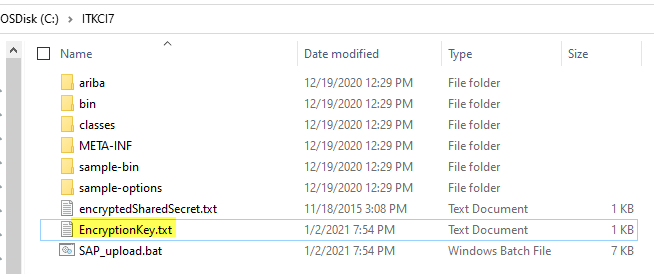


Hit ENTER.

1. You will be asked to enter a 24 character key (Enter whatever you would like but the key MUST be exactly 24 characters long – example: TestCustomerKey123456789) and hit ENTER.



1. Copy the encrypted string that is displayed. COPY THE ENTIRE STRING BUT DO NOT INCLUDE ANY SPACES
2. Create a new text file in the SA ITK Root Directory C:\ITKCI7\EncryptionKey.txt

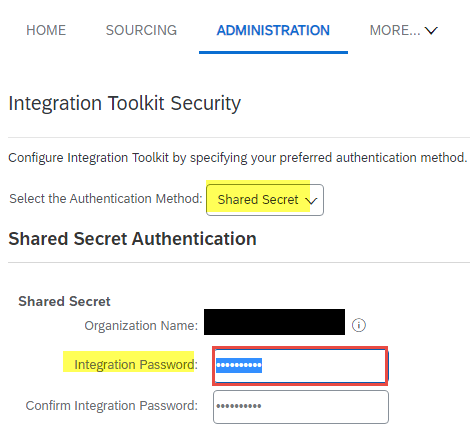


1. Edit the EncryptionKey.txt file in a text editor, paste the encrypted string that was copied from the command prompt, and save the EncryptionKey.txt file. ENSURE ALL WHITE SPACE IS REMOVED BEFORE AND AFTER THE ENCRYPTED STRING
2. Edit the options file, adjust the "set encryptionKeyPath=" parameter to point to the exact location of the EncryptionKey.txt file, and save the options file. For example, "set encryptionKeyPath=C:\ITKCI7\EncryptionKey.txt "
3. **integrationPasswordKeyPath** (if you choose the SharedSecret-based method of authentication) (Note: for Certificate-based authentication, please refer “SAP Ariba cloud solutions integration toolkit guide” page 16)

Uncomment "::set integrationPasswordKeyPath=" by removing colons ->

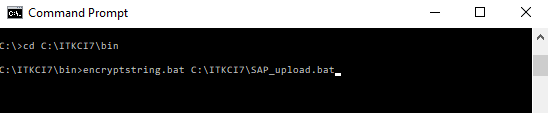
"set integrationPasswordKeyPath="

1. We need to know the Upstream Integration Toolkit Security - Shared Secret (Integration Password). Your Ariba SA Deployment Lead has access to an admin tool called the Service Manager. Have your SA Deployment Lead look up the following: If a shared secret is already defined under Service Manager => Realm Name => Administration => Integration Manager => Integration Toolkit Security, we would need to know the value of the shared secret.

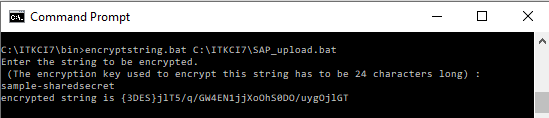


Ariba does not know what the value is and it would most likely be known by your Admins. Changing this value through Service Manager can impact other Ariba modules. If a shared secret is not defined, we need to define it here. Keep in mind if the other Upstream (Sourcing, Contracts, etc.) Ariba Modules want to leverage the ITK they would also need to know this same shared secret (integration password). If the shared secret ever needs to be reset, the SA ITK options file will need to be adjusted with a new encrypted key. Please discuss and get approval from all necessary teams involved with managing an ITK configuration prior to changing the Shared Secret directly on the SAP Ariba site.

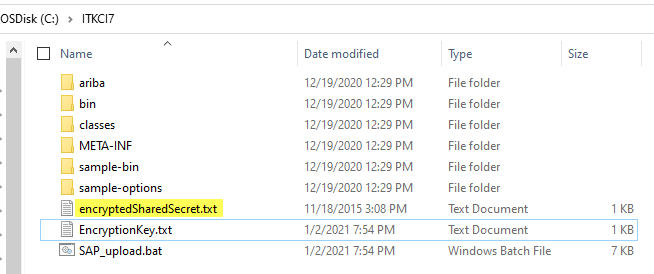
1. Keep in mind: if your Upstream (Sourcing, Contracts, or Spend Analysis) instance is suite integrated with Downstream Ariba modules (Procure to Pay for example), the downstream Ariba modules that are utilizing the ITK will use a separate ITK Shared Secret which is defined under Core Administration => Integration Manager => Integration Toolkit Security. As a best practice, please feel free to reuse the same shared secret on the upstream side (Administration => Integration Manager => Integration Toolkit Security) and on the downstream side (Core Administration => Integration Manager => Integration Toolkit Security). Please provide your SA Deployment Lead with this Shared Secret or reach out to the admin or other resource on your side, that was responsible for implementing the ITK for the Ariba Procure To Pay module.
2. Go back to the Command prompt, navigate to "cd C:\ITKCI7\bin", enter the following command for example, "encryptstring.bat C:\ITKCI7\SAP\_upload.bat" (note: instead of “SAP\_upload.bat” use whatever you have named the .bat options file as, in step 6 above), and hit ENTER.



1. Enter your Integration Toolkit Security - Shared Secret that was defined directly on the site and hit ENTER (ignore the message about 24 characters as that message only applies to encrypting the customer key)



1. Copy the encrypted string
2. Create a new text file in the SA ITK Root Directory C:\ITKCI7\encryptedSharedSecret.txt



1. Edit the encryptedSharedSecret.txt file in a text editor, paste the encrypted string that was copied from the command prompt, and save the text file. ENSURE ALL WHITE SPACE IS REMOVED BEFORE AND AFTER THE ENCRYPTED STRING
2. In the options file, have "set integrationPasswordKeyPath=" point to the filename and location of the text file with the encrypted shared secret, for example,

“set integrationPasswordKeyPath=C:\ITKCI7\encryptedSharedSecret.txt”

1. **authUser**

The ITK needs an authorized user on the realm in order to upload SA data files to the site. Reach out to your Ariba Deployment Lead to

1. create an “Enterprise” user account (note: if you have implemented SSO and are unable to create an enterprise user account specifically for the ITK, you may create a “Third-Party User” instead and attempt to run the ITK with this user account).
2. add the user to the “SV Data File Manager” user group AND assign the user to each of the source systems for which data files are to be uploaded

OR

add the user to the "SV Project Manager" user group (there is no need to assign the user to source systems)

(note: this same user can be used for each SA ITK configuration per SA Source System).

Define the user in the options file for example, if “ITKUser” is the user created, uncomment "::set authUser=bob" and change to "set authUser=ITKUser".

Note: The authUser value should match (including uppercase/lowercase) the value of the userid as given in the user profile in the application (User Admin). We do not need to specify the user password in the ITK configuration, so we can leave the password parameter in the options file commented out -> "::set password=d0n+SHar3"

1. **httpsProtocolsEnabled**

List of protocols to be enabled for the connection to the SAP Ariba Server (HTTPS communication). For example: “set httpsProtocolsEnabled=TLSv1,TLSv1.1,TLSv1.2”

For the highest level of security, restrict the protocol to TLSv1.2  
“set httpsProtocolsEnabled=TLSv1.2”

1. **cipherSuitesEnabled**

Specifies the list of cipher suites to be enabled for the connection to the SAP Ariba Server (HTTPS communication). Use this parameter to restrict the cipher suite support to a limited set of cipher suites OR leave the parameter commented out to keep the default list.

1. **datafile**

This parameter points to the location of the data file that needs to be uploaded to the SA site for this source system.

For a Windows system you could set this to the name and location of the file such as, "dataFile=C:\ITKCI7\UploadDir\SpendVisData.csv" or simply set this to the location (directory) where the data file(s) to be uploaded exists and all the csv files in this directory will be automatically zipped. For example: "dataFile= C:\ITKCI7\UploadDir”. Keep in mind when the ITK runs it will upload ANYTHING IN THIS DIRECTORY. Please ensure this directory ONLY CONTAINS the exact data that needs to be uploaded, otherwise, any old files or folders in this directory will be also be uploaded!

Note: For a UNIX system, the Spend Analysis csv data files to be uploaded must be pre-zipped into a single file and this parameter would point to the name and location of this zip file.

1. **outDir**

Points to the location where the files in the specified datafile directory, will get archived to. For example: "set outDir=C:\ITKCI7\OutDir" will archive all the data files in the datafile directory to the “OutDir” folder in “C:\ITKCI7”.

1. **sourceSystem**

Defines the actual SA source system that the data file(s) being uploaded, belongs to. For example, “set sourceSystem=SAP”.

1. **logDir**

Define a logs directory for the upload process. For example, "set logDir=C:\ITKCI7\Logs". Note: Please ensure that the directory is created prior to running the data file transfer via the ITK tool.

1. **smtpMailServer**

If you would like to generate email notifications for successful and unsuccessful ITK uploads, please define the SMTP server parameter for example:

"set smtpMailServer=smtp.mycompany.com"

1. **fromEmail**

Email notifications would need to come from a valid/existing "From" e-mail address on your network (this address could be an existing generic IT email address: for example,

"set [fromEmail=ITNotifications@mycoolcompany.com](mailto:fromEmail=ITNotifications@mycoolcompany.com)").

1. **notifyEmail**

This parameter will be the email address that will receive the ITK e-mail notifications. For example, "set notifyEmail=myemail@mycompany.com". This email address can be an individual e-mail address or a distribution list.

1. **notifyonSuccess** and **notifyonFailure**

If you want to send a notification on Success and Failure, please leave the parameters as is: "set notifyonSuccess=1" and "set notifyonFailure=1". If you would like to disable either option set the parameter="0"

1. **notificationSuccessSubject** and **notificationFailureSubject**

You have the ability to customize the Subject line of the e-mail notifications. If you are implementing the SA ITK for multiple Source Systems, we recommend that you customize the Subject lines to reference that particular source system. For example, "set notificationSuccessSubject=Ariba File Transfer SAP Data Upload: Successful" and "set notificationFailureSubject=Ariba File Transfer SAP Data Upload: Failed"

1. Does the machine used for the SA ITK installation require a proxy server in order to connect to the Internet? If not, please move to the next step. If the machine does require a proxy server, uncomment and specify the proxy settings in the options file:  
   set **proxyHost**=myproxyhost  
   set **proxyPort**=8081  
   set **proxyAuthMode**=N  
   set **proxyUser**=username  
   set **proxyPassword**=password  
   set **proxyDomain**=domain
2. **additionalServerArgs**

For additional options, such as triggering the automated extended file validation options once the file has been uploaded to the Ariba site (Duplicate Row and Reference checks).

For example: "set additionalServerArgs=-sourceSystem %sourceSystem%

-checkDimensionReference true -checkDuplicateRow true"

1. **operation**

set operation=sv-upload

1. **urlPrefix**

url to use for transfer of data

set urlPrefix=https://s1.ariba.com/Sourcing/Main/ad/uploadDataFile/StarSchemaActions

If the URL you use to launch your SAP Ariba Spend Analysis site is

<https://s3.ariba.com/Sourcing/Main?realm=actualrealmname>

then

set urlPrefix=https://s3.ariba.com/Sourcing/Main/ad/uploadDataFile/StarSchemaActions

If the URL you use to launch your SAP Ariba Spend Analysis site is

<https://s1-integration.ariba.com/Sourcing/Main?realm=actualrealmname>

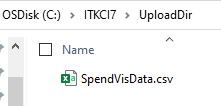
then

set urlPrefix=https://s1-integration.ariba.com/Sourcing/Main/ad/uploadDataFile/StarSchemaActions

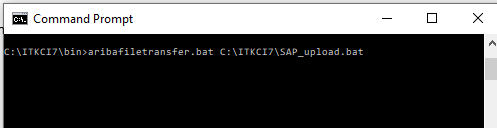
9) Save the options file “SAP\_upload.bat”

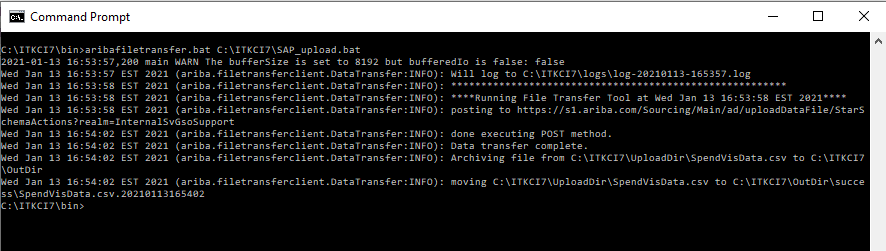
10) To test the upload:

1. Add a blank csv file say “SpendVis.csv” file to upload in the “C:\ITKCI7\UploadDir” location. (For a UNIX based system, add this csv file to a zip file)

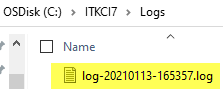


1. Open a Command Prompt and navigate to the ITK installation directory "cd C:\ITKCI7\bin"
2. Enter and run the command: "aribafiletransfer.bat C:\ITKCI7\SAP\_upload.bat"





1. If there are errors reported in the command window, make changes to the values specified in the “SAP\_upload.bat” options file as needed. Check the log file in the “C:\ITKCI7\Logs” folder, for additional info, if needed.



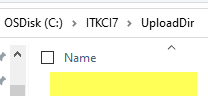
For additional logging, please enable Debug logging by appending the verbose option to a parameter called “additionalClientArgs”.

For example:

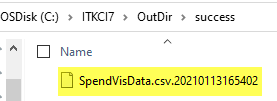
set additionalClientArgs=-verbose (for Windows batch file)

additionalClientArgs="-verbose" (for UNIX Shell script file)

1. Check the “C:/ITKCI7/UploadDir” folder to see that the Spend Analysis data file to be uploaded has been moved from this location



1. Check the “C:/ITKCI7/OutDir/success” folder to see that the Spend Analysis data file to be uploaded has been moved to this location



If there were an error in the transfer, the data file would have been moved to “C:/ITKCI7/OutDir/failed” folder

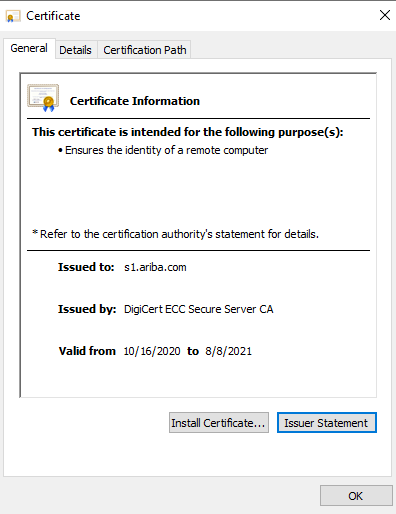
1. To check the site for the uploaded file go to Administration => Reporting Manager => Data Files. If you do not have access, please reach out to your Ariba SA Deployment Lead.
2. Delete any uploaded test files from the site and remove any test files from the SA ITK Upload directory because THE ITK WILL TRANSFER TO ARIBA SPEND ANALYSIS, ANY FILES FROM THE UPLOAD DIRECTORY. Always archive any files or folders to a location outside of the Upload directory.
3. If everything is all set, you can begin uploading the full data set for the configured source system.
4. If you need to upload data files to additional SA Source Systems, the ITK needs to be configured with a separate Options file for each Source System. In each options file, you specify the SA Source System and a directory where the source data exists, therefore this requires a separate options file per SA source system. You could copy the working upload.bat file from the initial ITK setup, create a separate upload directory per Source System, and adjust the options file as needed. The EncryptionKey.txt and encryptedSharedSecret.txt file locations can be reused for each additional options file so there is no need to regenerate these files. If the shared secret changes on the site, the ITK will stop working, and the new shared secret will need encrypted using the steps above. As long as the EncryptionKey.txt and encryptedSharedSecret.txt file names and locations do not change, the parameters for these in the option files, do not need to be adjusted.

APPENDIX

1. If there is a handshake/authentication issue between your system and the SAP Ariba web server, you might need to download and install the certificates for the Ariba web server on the system where the ITK is being installed.

To download the certificates, launch <https://s1.ariba.com> (or <https://s3.ariba.com> if the url of your SA site uses s3 instead of s1) in a web browser and click on the lock icon in the url bar and click on View Certificate.





Go to Details -> Copy to File -> Certificate Export Wizard, in order to download it.

© 2022 SAP SE or an SAP affiliate company. All rights reserved.