TAX REPORTING SUITE

MODULE IDES

VERSION 26.03



USERS'S MANUAL

Published: Oct 2026

For the latest information and to leave feedback, please visit BRIFS GmbH at
https://www.section11.ch or https://www.trsuite.ch

The information in this document and any document referenced herein is provided for informational purposes only, is provided AS IS AND WITH ALL FAULTS and cannot be understood as substituting for customized service and information that might be developed by BRIFS GmbH for a particular user based upon that user's particular environment. RELIANCE UPON THIS DOCUMENT AND ANY DOCUMENT REFERENCED HEREIN IS AT THE USER'S OWN RISK.

© 2026 BRIFS GmbH. All rights reserved.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

BRIFS GMBH PROVIDES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION CONTAINED IN THIS DOCUMENT AND ANY DOCUMENT REFERENCED HEREIN. BRIFS GmbH provides no warranty and makes no representation that the information provided in this document or any document referenced herein is suitable or appropriate for any situation, and BRIFS GmbH cannot be held liable for any claim or damage of any kind that users of this document or any document referenced herein may suffer. Your retention of and/or use of this document and/or any document referenced herein constitutes your acceptance of these terms and conditions. If you do not accept these terms and conditions, BRIFS GmbH does not provide you with any right to use any part of this document or any document referenced herein.

Complying with the applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of BRIFS GmbH.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Content

Revision History 4
The Main Window 5
IDES: Module Overview 5
IDES Menu Items 7
Common UI Objects 7
Invalid Fields 7
CLEAR Buttons 7
Data Validation 7
File Information 8
IDES Configuration 8
IDES information 8
IRS Certificate Renewal 9
SFTP 9
SFTP Host Key Verification 10
Button Bar 11
File Information 11
Create Transmission Archive 11
Sender Metadata 12
Payload 13
SFTP-Upload 15
Extract IRS Response 16
Download and Extract 16
Steps 17
Response Content 18
Extract Archive 19
Steps 19
Masterdata 20
Proxy Configuration 20

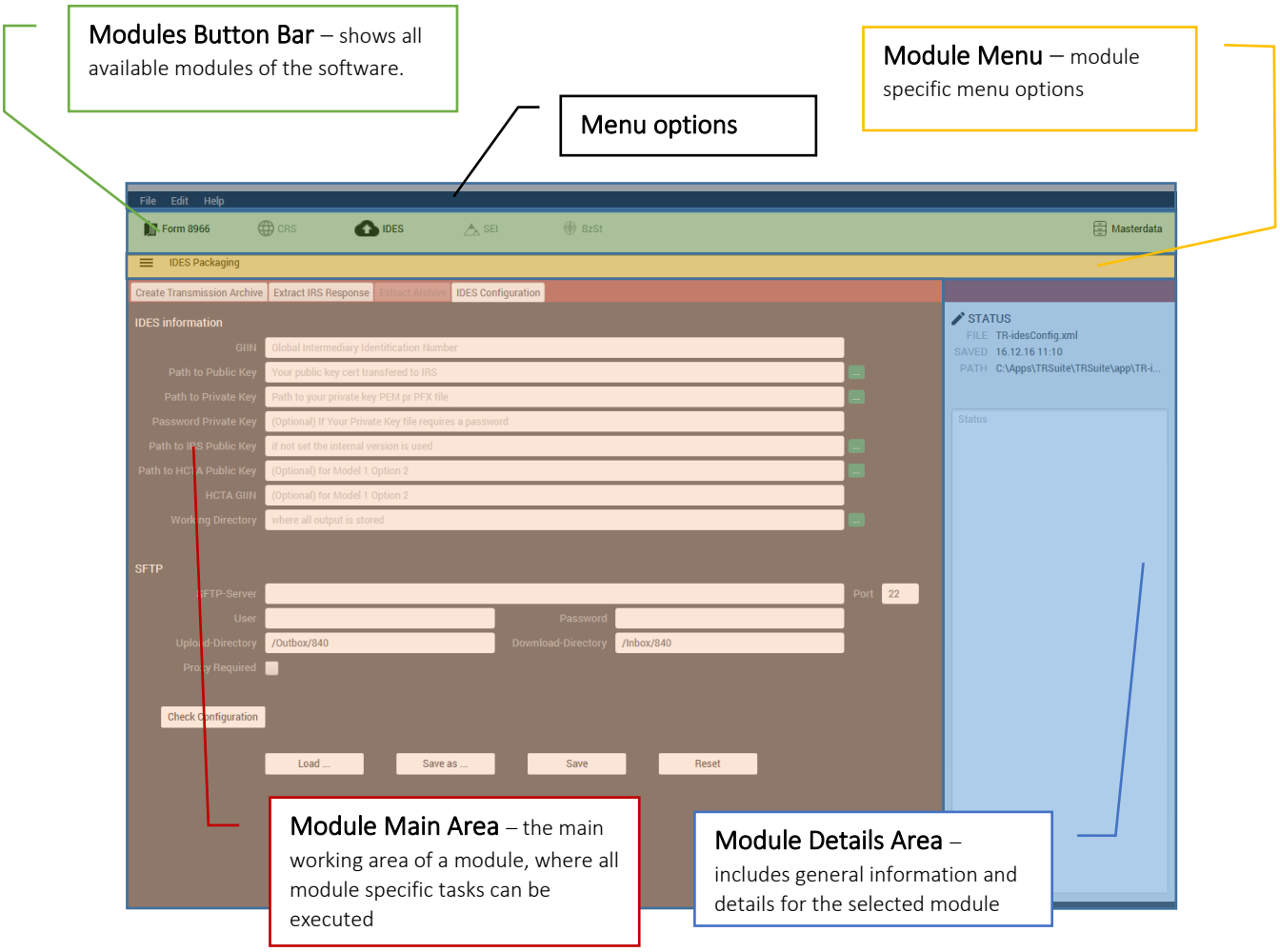
Revision History

Version	Doc Version	Revision Date	Description
1612	Rev 0	15.12.2016	Initial Revision
1703	Rev 1	07.03.2017	
1706	Rev 2	15.06.2017	No changes
1711	Rev 3	01.01.2018	
1802	Rev 4	27.02.2018	No changes
1803	Rev 5	21.03.2018	Fix: SFTP proxy authentication
1807	Rev 6	31.07.2018	Passwords encrypted in configuration files; extended validation: public/private key match
1812	Rev 7	17.12.2018	IRS certificate update, notification schema 2.4 support, Reporting period free text
1902	Rev 8	12.02.2019	Screenshots updated
1911	Rev 9	07.11.2019	Minor fixes, stability improvements, FATCA XM schema update (IRS response)
20.01	Rev 10	20.01.2020	https://www.easycrs.ch/index.php/8-trsuite/12-trsuite-release-notes-version-20-01
20.02	Rev 11	24.02.2020	https://www.easycrs.ch/index.php/8-trsuite/13-trsuite-release-notes-version-20-02
20.03	Rev 12	25.03.2020	https://www.easycrs.ch/index.php/8-trsuite/15-trsuite-release-notes-version-20-03
20.05	Rev 13	02.06.2020	https://www.easycrs.ch/index.php/8-trsuite/16-trsuite-release-notes-version-20-05
20.11	Rev 14	24.11.2020	https://www.easycrs.ch/index.php/8-trsuite/17-trsuite-release-notes-version-20-11
21.01	Rev 15	01.02.2021	https://www.easycrs.ch/index.php/8-trsuite/18-trsuite-release-notes-version-21-01
26.02	Rev 16	06.09.2026	https://www.trsuite.ch/trsuite/ReleaseNotes/RELEASE_NOTES_26.02.en.html
26.02	Rev 17	08.09.2026	IDES Sender Metadata schema 1.3, communication types
26.03	Rev 18	21.09.2026	SFTP host key verification (first connection, changed key), SFTP through an authenticating proxy
26.03	Rev 19	23.09.2026	IRS certificate: expiry warning and yearly renewal; the certificate is not checked against a CRL
26.03	Rev 20	15.10.2026	https://www.trsuite.ch/trsuite/ReleaseNotes/RELEASE_NOTES_26.03.en.html

The Main Window

The Main window is the launch point for the entire application. You can select the licensed module in the modules button bar and perform the module specific tasks within main area of the module.

Each module comes with its own module menu and detail area.

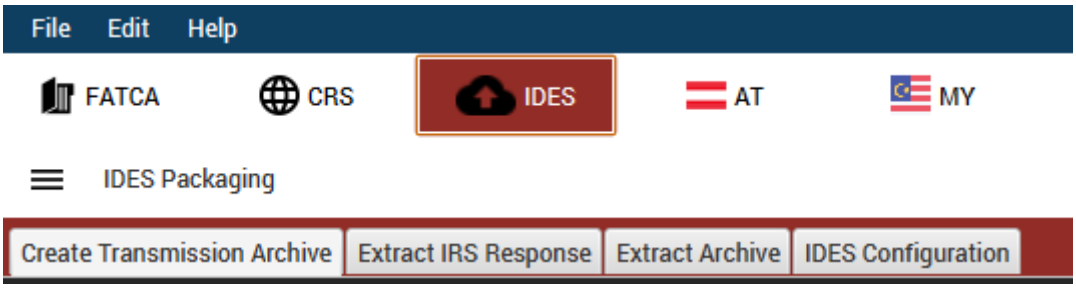


IDES: Module Overview

The International Data Exchange Service (IDES) is an electronic delivery point where Financial Institutions (FI) and Host Country Tax Authorities (HCTA) can transmit and exchange FATCA data with the United States.

As the IDES Data Transmission and File Preparation process is quite complex, the IDES module will help you to do all with one tool with only a few clicks.

This guide provides information about the IDES module of the TRSuite software package. It describes processes and procedures for generating, uploading, downloading and extracting files to and from the IRS IDES gateway.



This document may describe features and capabilities that requires a separate license and are not covered by the standard license. For information about licensing please contact support@section11.ch

The IDES module includes the following:

- IDES module specific configuration
- Create Transmission Archive
- Extract IRS Response
- Extract Transmission Archives (HCTA Version only)

The latest release of the TRSuite has added SFTP functionality and the ability to process an entire folder of transmission archives or XML files. With the options provided, a single ZIP/XML file or an entire folder can be processed or sent automatically via SFTP. This document will help explain how each option functions.

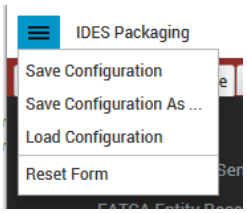
The screenshots throughout the user's manual are produced on Windows 11 using the Windows Look and Feel.

In addition to this Users Guide, the following online resources may be useful:

- IRS Publications related to FATCA
  http://www.irs.gov/pub/fatca/
- FATCA IDES Technical FAQs
  http://www.irs.gov/Businesses/Corporations/FATCA-IDES-Technical-FAQs
- IDES Alert Codes
  http://www.irs.gov/Businesses/Corporations/IDES-Alert-Codes
- IRS FATCA Report Notifications FAQ
  http://www.irs.gov/Businesses/Corporations/IRS-FATCA-Report-Notifications-Frequently-Asked-Questions
- IDES Data Preparation
  http://www.irs.gov/pub/fatca/IDES%20Data%20Prep%20User%20Tips_vF.pdf
- Download Link to the IRS X509-certificate (IRS Public Key)
  https://www.ides-support.com/Downloads/encryption-service_services_irs_gov.crt
- IDES Testing Schedule
  http://www.irs.gov/Businesses/Corporations/IDES-Testing-Schedule
- IDES-accepted Certificate Authorities and Products
  http://www.irs.gov/Businesses/Corporations/Digital-certificates

IDES Menu Items

The IDES menu includes the following elements



Menu Options	Description
Save Configuration	The Save method persists any configuration settings that have been modified since the configuration was saved last time. If a configuration file does not exist at the physical default location, a new configuration file will be created. Default path: <INSTALLATION-DIRECTORY>/app/TR-idesConfig.xml
Save Configuration As …	The Save As method persists any configuration settings that have been modified since the configuration was saved last time to the user selected path. If a configuration file does not exist at the physical default location, a new configuration file will be created.
Load Configuration	Load the configuration from an existing configuration file. Existing values will be replaced.
Reset Form	Discards all non-persist changes and loads the last known configuration.

Common UI Objects

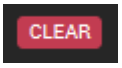
Invalid Fields

Some text fields expect specific values or formatted text, e.g. GIIN- or date-fields. If an invalid value/format is entered the text fields is marked red:



CLEAR Buttons

A CLEAR-button resets the values of all elements in the according logical region.



Data Validation

Entered data is continuously validated. If the data is not complete (all mandatory fields filled) or in a wrong format the warning symbol is displayed next to the affected section label.

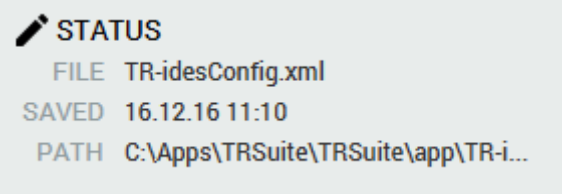


If the section is complete and correct, the green checkbox symbol is shown next to the label.



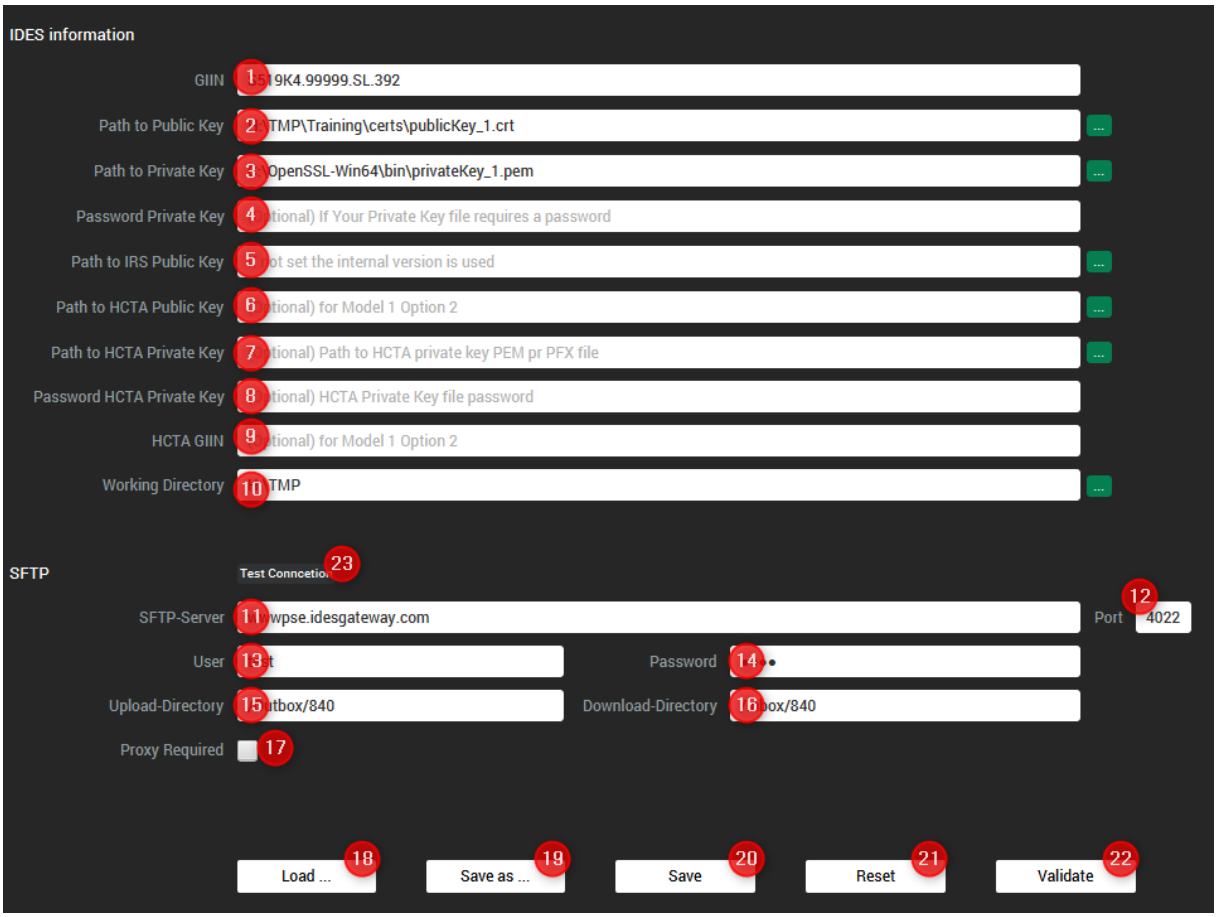
File Information

After a file is loaded or saved, the information about the file (name, last modified, absolute path) is displayed in the status pane of the detail area. The full path can be seen in the tooltip.



IDES Configuration

The configuration screen allows the user to enter all required information needed to generate a valid transmission archive and submit the data to the IRS IDES gateway.



IDES information

1) (Sender) Global Intermediary Identification Number. As a valid GIIN is crucial for a valid file, the format and availability of the GIIN is checked more strictly. If a non-valid GIIN is entered, the according text field is marked red, to indicate invalid data.
2) Your public key certificate transferred to the ISR during IDES enrollment process;
   Hint: Optional any valid X.509 certificate can be used for testing, e.g. a self-signed certificate as delivered with the application for testing purpose (see chapter testing for more details).

3) The path to your private key PEM or PFX/P12 file (NEVER share this file!) used to generate the CSR/certificate.
   Optional a valid PEM file can be used for testing, also there is one delivered with the app.
4) Optional: Password for your PEM/PFX/P12 file. Typically, SSL-Server private keys do not use passwords, still it is supported
5) Optional: The public key provided by the ISR. If no value is entered, the IRS certificate delivered with TRSuite is used. The IRS replaces this certificate once a year (see "IRS Certificate Renewal").
6) Optional: HTCA public key for model 1 option 2
7) Optional: HTCA GIIN
8) HTCA private key for decrypting FI payloads encrypted with HTCA public key
9) Password for your HTCA private key PEM/PFX/P12 file.
10) The default working directory, where all generated artifacts are stored.

IRS Certificate Renewal

TRSuite encrypts the AES key of every transmission archive with the public key of the IRS (step "Encrypt AES key for IRS"). The IRS replaces this certificate once a year, usually in September. TRSuite delivers the certificate that is current when the release is built; it is used whenever the field "Path to IRS Public Key" is empty. IDES rejects a transmission archive whose AES key was encrypted with an expired certificate.

Expiry warning: TRSuite checks the expiry date of the certificate in use, that is the file entered under "Path to IRS Public Key" or, if the field is empty, the certificate delivered with TRSuite. If the certificate has expired or expires within 30 days, TRSuite shows a warning when the IDES module is opened (once per session), reports it when you press "Validate" in the IDES Configuration, and asks for confirmation before it creates a transmission archive. The message names the expiry date and the certificate in use. When TRSuite runs without user interface, the warning is written to the log file. TRSuite does not check the certificate against a revocation list (CRL).

Renewing the certificate: download the current certificate from https://www.ides-support.com/Downloads/encryption-service_services_irs_gov.crt, save it in a folder of your choice, enter its path under "Path to IRS Public Key" in the tab "IDES Configuration" and save the configuration. Press "Validate" to check the entry. TRSuite never downloads the certificate itself, so the procedure also works on workstations without internet access. As soon as a TRSuite release delivers the new certificate, the field can be emptied again.

Older TRSuite versions: the field "Path to IRS Public Key" works the same way in all versions. After the yearly replacement by the IRS, enter the downloaded certificate there, even if your version does not show the expiry warning yet.

SFTP

The SFTP Settings will be used to connect to the SFTP server and upload the encrypted data packet directly to IDES.

11) The URL of the SFTP server to connect to
12) SFTP-Port of the server, IDES-gateway uses 4022 (usually SFTP uses port 22 but can be configured to run on nearly any port, check IRS documentation)
13) The username for the account that will be used on the SFTP server
14) The password for the account that will be used on the SFTP server
15) remote folder to upload local files

16) remote folder where to download any notifications found there
17) Check this box, if your internet connections are routed through a proxy (must be configured in the master data dialog)

SFTP Host Key Verification

Every SFTP server identifies itself with a host key. TRSuite checks this key on every connection to the IDES gateway (Test Connection, SFTP-Upload and SFTP-Download), so that your user name, your password and your transmission archives are only sent to the server you have confirmed.

First connection to a server: TRSuite does not know the key yet and shows the dialog "SFTP host key" with the name of the server, the key type and the fingerprint of the key (SHA-256 in the form shown by OpenSSH, starting with "SHA256:", followed in brackets by the MD5 value, sixteen pairs of characters separated by colons). If the operator of the server publishes the fingerprint, compare it and accept only if both are identical. The IRS does not publish the fingerprint of the IDES gateway. For IDES, make the first connection from your trusted company network (not from a public or guest network), check that the server name shown in the dialog is exactly the IDES address you intended to use, and note the fingerprint in your documentation. If several workstations or users in your organisation connect to IDES, they must all see the same fingerprint for the same server; a different fingerprint on one of them is a reason to stop and to contact your network administrator. With "Accept key" the key is stored, and TRSuite connects. "Cancel" is the default and also applies when you press Enter or Esc or close the window: nothing is stored and no connection is made; your user name and password are not transmitted.

Further connections: as long as the server presents the stored key, TRSuite connects without asking again.

Test and production environment: the key is stored per server name and port. The IDES test environment and the IDES production environment are different servers, so each of them is confirmed once. Switching between the two afterwards does not raise any further question.

Changed host key: if a known server presents a different key, TRSuite refuses the connection and shows the warning "the host key of ... has CHANGED" with the stored fingerprint and the fingerprint presented now. There are two possible reasons: the operator has replaced the key, for example after moving the service to a new server, or somebody is intercepting the connection. "Refuse connection" is the default and also applies when you press Enter or Esc or close the window; nothing is changed. Choose "Replace stored key" only if you have a confirmation that the key was replaced: an announcement of the operator (for IDES: the IDES news of the IRS or an answer of the IDES help desk), and, where you can check it, the same new fingerprint on another workstation of your organisation. TRSuite then replaces the stored key of this server, connects, and writes the old and the new fingerprint to the log file. If in doubt, refuse the connection and ask the operator of the server.

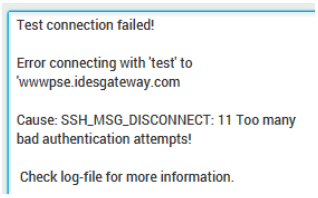
Where the keys are stored: in the file known_hosts in the folder AppData\Local\TRSuite\app of your Windows user profile. The file uses the OpenSSH format, one line per server; servers on a port other than 22 are written as [server]:port. To make TRSuite ask again for a server, close TRSuite, delete the line of that server and connect again. Each Windows user has a file of their own and confirms the key once.

Command line and unattended operation: without a user interface nobody can confirm a key. An unknown or a changed key is therefore always refused, and the message names the fingerprint and

the known_hosts file. Confirm the key once with "Test Connection" in the IDES module, using the same Windows user that runs the unattended job.

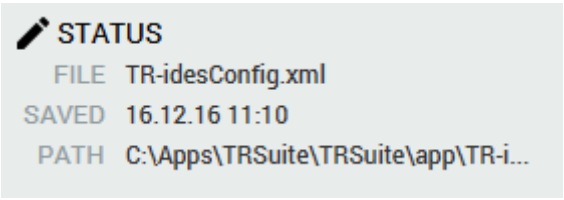
Button Bar

18) **“Load”** You can open existing configuration files by pressing the Load-Button. In the dialog box browse to select a document and click “Open” to load the document.
19) **“Save as …”** Saves the current configuration in a different location, or with a different file name or file type. Opens a file chooser dialog to let you browse to the location where you want to save the document.
20) “**Save**” Saves the current configuration to the last selected file or default location. The data is stored within an XML-File and automatically available the next time you start the program. If there are unsaved changes the save-button is colored green.
21) “**Reset**” loads the last saved configuration and overwrites all unsaved changes.
22) By pressing the “**Validate**”-Button the tool loads the given keys, validates the entered data and shows the result of the validation within a popup window.
23) “**Test Connection**” connects to the configured SFTP-Server using the provided username and password. The result of the connection test is displayed in the details area on the righthand side. On the first connection to a server, or when the key of the server has changed, the host key dialog is shown first (see “SFTP Host Key Verification”).



File Information

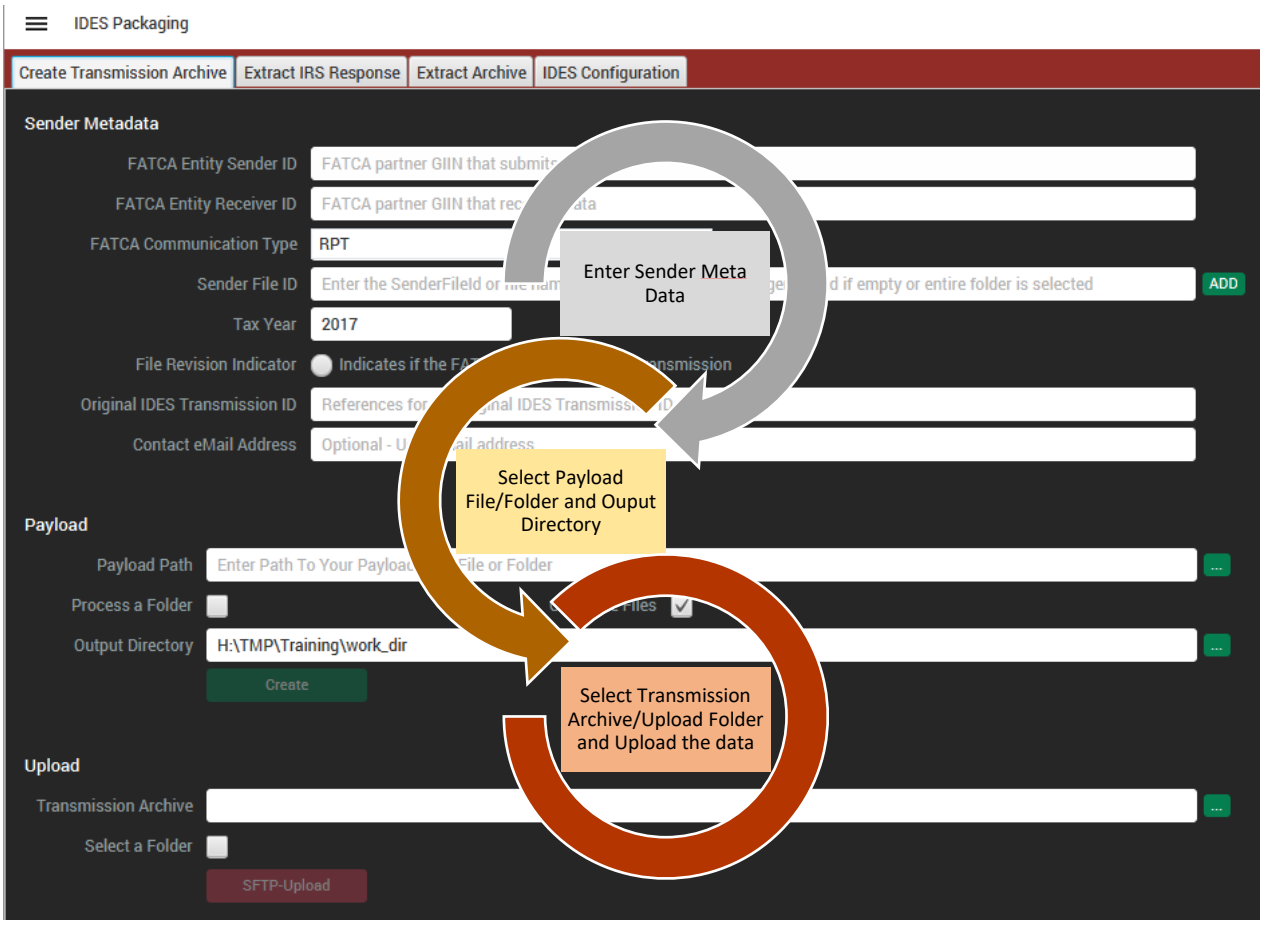
After a configuration is loaded or saved, the information about the file (name, last modified, absolute path) is displayed in the status pane of the detail area. The full path can be seen in the tooltip.



Create Transmission Archive

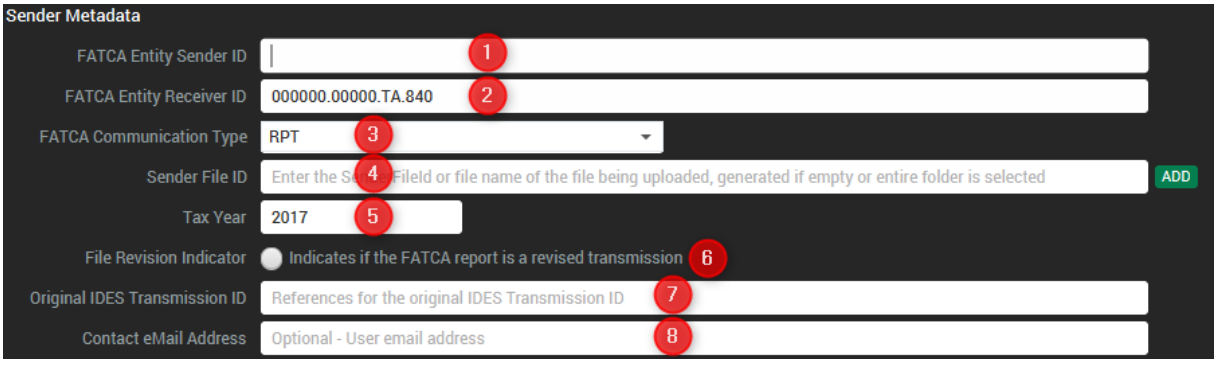
Within the “Create Transmission Archive” Tab the user can enter all required information to generate and upload valid transmission archives including a sender metadata XML-File.

The creation and upload of the data can be done with three easy steps.

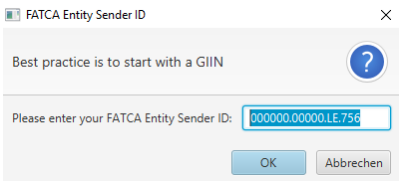


Sender Metadata

The "Sender Metadata" section allows the user to enter all required information to generate a valid sender metadata file during the archive creation process.



1) The FATCA partner GIIN submitting the data. If the GIIN is already provided on the configuration screen in the according field, the value is copied over. If no value is available an input dialog is displayed:



2) The receiver GIIN, typically the IRS. For convenience, the US-GIIN is filled when the empty text field is selected.
It is also possible to enter just the country ISO-code of the receiver. As soon as the program recognizes al valid ISO code, the according GIIN is displayed. E.g. enter "US" for the IRS GIIN

3) The communication type as defined by the IRS. For a typical transfer the report “RPT” entry is used. Notifications “NTF” you will receive typically as a response. Since schema 1.3 the communication types EOIR, ICAP, JA and TAEOI are available in addition to NTF, RPT, CAR, REG, TEI, DCI and OTH.

4) The sender file ID or file name of the file being uploaded. If no value is entered, the transmission archive file name without zip-extension ([UTC]_[NAME]) is used during the creation of the archive. When entering an empty field, a sender file id is generated. A new ID can be generated by pressing the green “ADD”-Button.

5) The tax year of the FATCA reporting. Required format: YYYY-12-31

6) File revision indicator, only selected if it transmission archive contains a revised transmission

7) (Optional) Reference for the original IDES Transmission ID, in case of a retransmission

8) (Optional) the contact email address

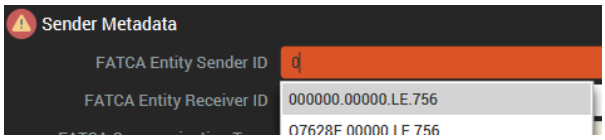
The entered data is continuously validated. If the data is not complete (all mandatory fields filled) or in a wrong format the warning symbol is displayed next to the affected section label.



If the section is complete and correct, the green checkbox symbol is shown next to the label.

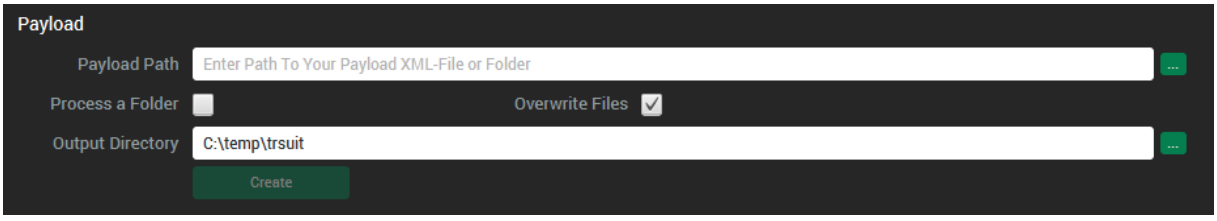


The sender id field is a learning text field. If you start typing, all previously entered GIINs are available in the dropdown list. The list is not saved and therefore not available after a restart of the program.



Payload

The Payload section let the user select the XML file(s) to be processed. The tool has the ability to process a single file or an entire folder of XML files.



If the process a folder option is enabled a folder can be selected by pressing the “…”-Button. For each FATCA XML file within the selected folder a dedicated transmission archive is generated. If all data is valid the “Create”-Button is enabled and can be pressed to start the process.

All generated files will be written to the following folder structure within the selected output directory.



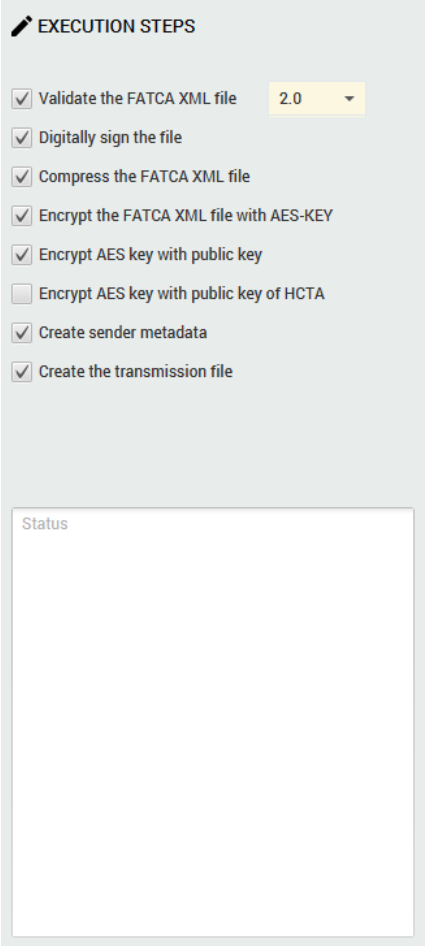
The processed XML file is either copied to the processed folder, if the transmission archive was successfully generated or to the failed folder, if the file could not be processed properly.

The generated transmission archive is moved to the upload folder. The temp folder contains all artifacts generated during the processing. All temporary output is stored in a new folder created within the working directory temp folder. The naming schema for the new folder is simply the UTC-timestamp as used for naming the transmission archive. The generated transmission archive is named, following the IDES guidelines: [UTC]_[GIIN].zip

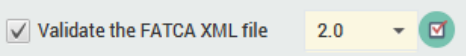
For instance, if you file is named 20150227T065715442Z_000000.00000.CH.123.zip the created folder is named: 20150227T065715442Z.

Following steps are executed during the creation process:

1) Validation of the payload xml file against the FatcaXML_v2.0.xsd and/or FatcaXML_v1.1.xsd schema. Can be selected with the drop down menu.
2) Signing the payload xml with the FI's private key
3) Compressing the signed payload xml
4) Encrypting the compressed payload file with a one-time AES-256 key
5) Encrypting the AES key with the IRS public key. Before the process starts, TRSuite checks the expiry date of the IRS certificate and asks for confirmation if it has expired or expires within 30 days (see "IRS Certificate Renewal").
6) (Optional) Encrypting the AES key with the HCTA public key
7) Creating the sender metadata file with a current timestamp
8) Creating the transmission archive and write all output to the working directory



If the process step executes without errors a success symbol is displayed next to the step label.

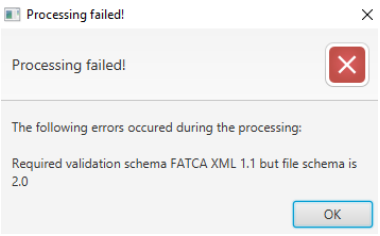


If the step fails, a warning symbol is shown.



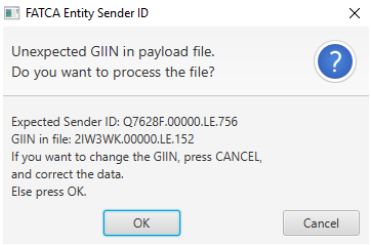
More information about the result is displayed in the status area below the process steps.

In case of an error, a localized error message is displayed within a notification dialog. The language of the message depends on your OS settings. For instance, if you use a German version of Windows the message is display in German.



A more detailed (but technical) error message is written to the log file.

During the process the Reporting FI GIIN in your payload file is compared with the GIIN entered in the entity sender ID field. If the values do not match, a warning is displayed. By pressing the “OK”-Button the mismatch is confirmed and the process continues. By pressing the “Cancel”-Button the process is stopped and the error can be corrected.



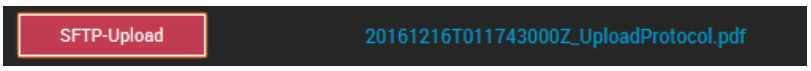
After the successful generation, the file path of the transmission archive is set to the “Transmission Archive” field in the Upload section.

SFTP-Upload

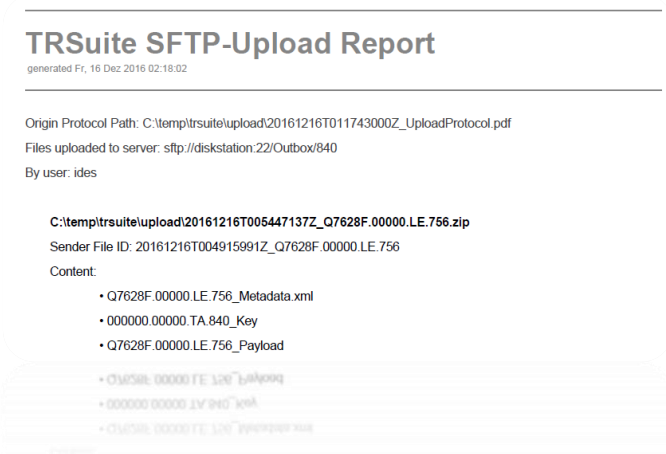
The latest release of the TRSuite has added SFTP functionality and the ability to process an entire folder of ZIP files. With the options provided, a single ZIP file or an entire folder can be sent via SFTP.



Pressing the “SFTP-Upload”-Button will connect to the Outbox/840 folder and upload a single data packet or all packets in the selected folder. After the download an upload report can be opened by pressing the displayed hyperlink If the server is not known yet or its host key has changed, the host key dialog appears before anything is transmitted (see “SFTP Host Key Verification”).



The Report contains information about the uploaded files, the SFTP-server, the SFTP-user and time.


TRSuite SFTP-Upload Report

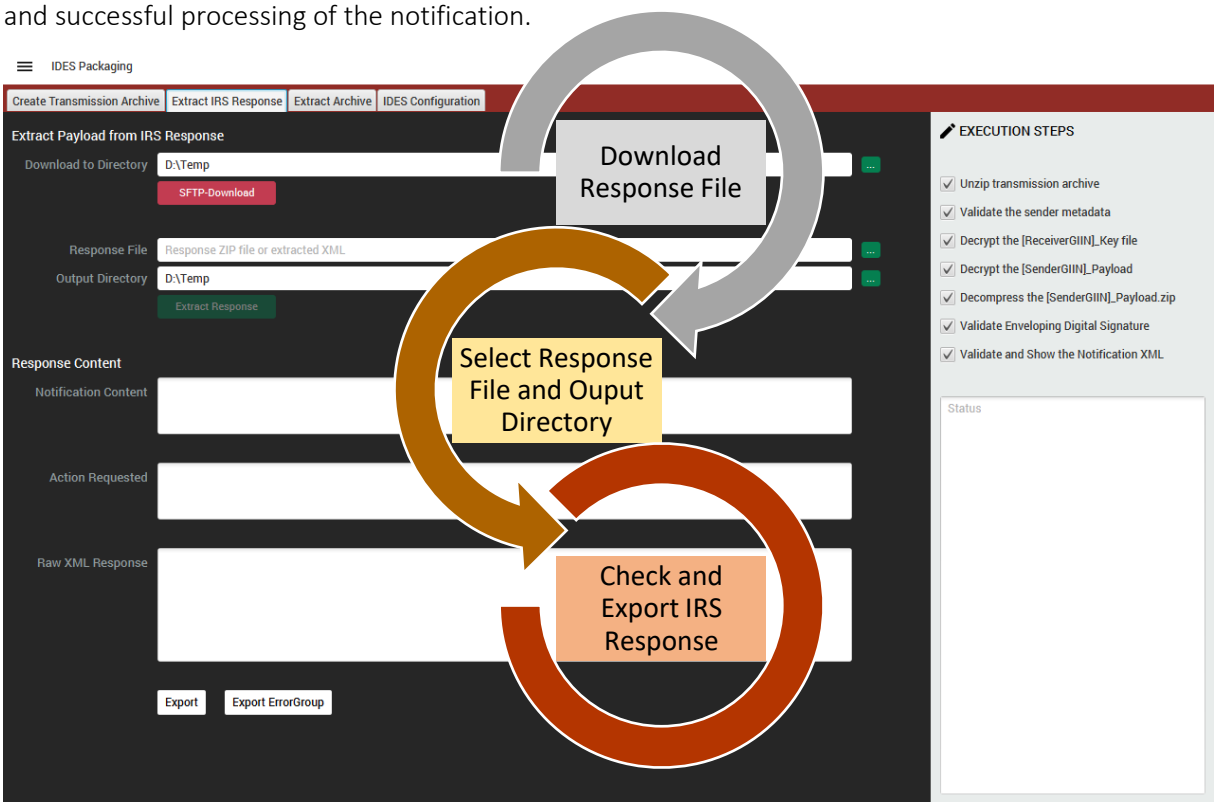
generated Fr, 16 Dez 2016 02:18:02

Origin Protocol Path: C:\temp\trsuite\upload\20161216T011743000Z_UploadProtocol.pdf
Files uploaded to server: sftp://diskstation:22/Outbox/840
By user: ides

C:\temp\trsuite\upload\20161216T005447137Z_Q7628F.00000.LE.756.zip
Sender File ID: 20161216T004915991Z_Q7628F.00000.LE.756
Content:
- Q7628F.00000.LE.756_Metadata.xml
- 000000.00000.TA.840_Key
- Q7628F.00000.LE.756_Payload

Extract IRS Response

The “Extract IRS Response” tab allows the user to select all steps the tool should execute to download, validate, show and export an IRS notification. Viewing the content is only possible after a complete and successful processing of the notification.



Download and Extract

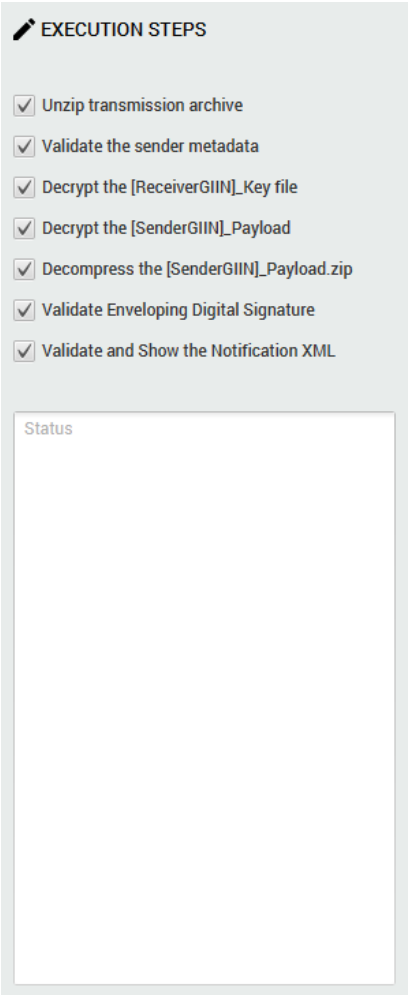


Pressing the “SFTP-Download”-Button will connect to the Inbox/840 folder of the IDES gateway and download any notifications found there to the configured download directory. If at least one file is downloaded the absolute path of the 1st file is automatically entered into the response file text field for further processing. If the server is not known yet or its host key has changed, the host key dialog appears first (see “SFTP Host Key Verification”).

If no default working directory is entered in the configuration tab, select an existing working folder before the extraction process can be started by pressing the “Extract Response” button.

Steps

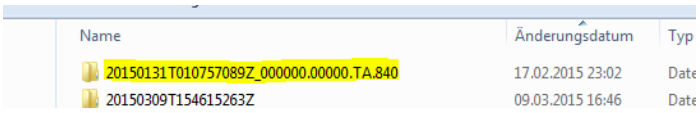
- Unzip the notification message archive
- Validate the extracted sender metadata XML file against the FATCA-IDES-SenderFileMetadata-1.3.xsd (IRS Sender Metadata schema v1.3; files created with schema 1.1 or 1.2 remain readable)
- Decrypt the [ReceiverGIIN]_Key file using the configured private key
- Decrypt the [SenderGIIN]_Payload file with the one-time AES-key extracted in step (3)
- Decompress the decrypted [SenderGIIN]_Payload.zip file
- Validate the extracted signed XML-File
- Validating the Notification XML-File against either the BASE-FATCA-NOTIFICATION-x.y.xsd, FATCA-INTERIM-VALID-FILE-NOTIFICATION-x.y.xsd or FATCA-FILE-ERROR-NOTIFICATION-x.y.xsd (supported versions 2.2/2.3) depending on the type of the notification



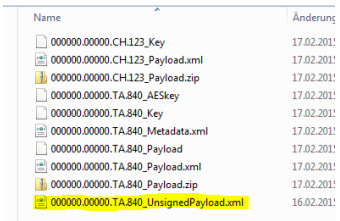
After a successful verification, you can view the content of the notification in the Response Content pane.

All generated artifacts are stored in a folder created within the configured working directory, following the given naming conventions: [UTC]_[SenderGIIN].

Typically, same as the name of the notification archive without a file extension. For instance:

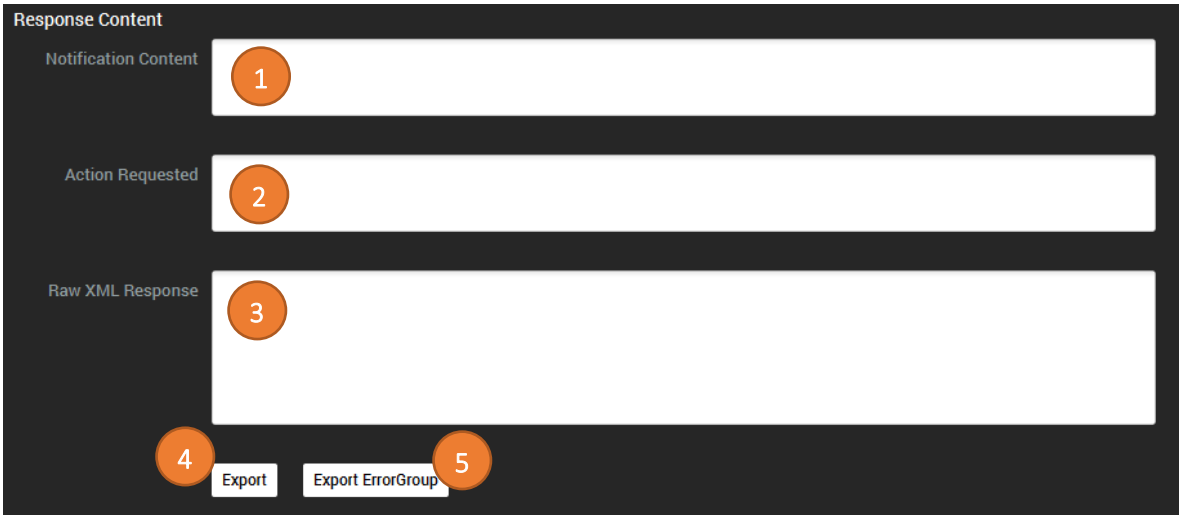


The folder contains all temporary files, generated during the process. Most important for the user is the raw XML-message [SenderGIIN]_UnsignedPayload.xml



Response Content

The content of the extracted file is shown in the Response Content pane:



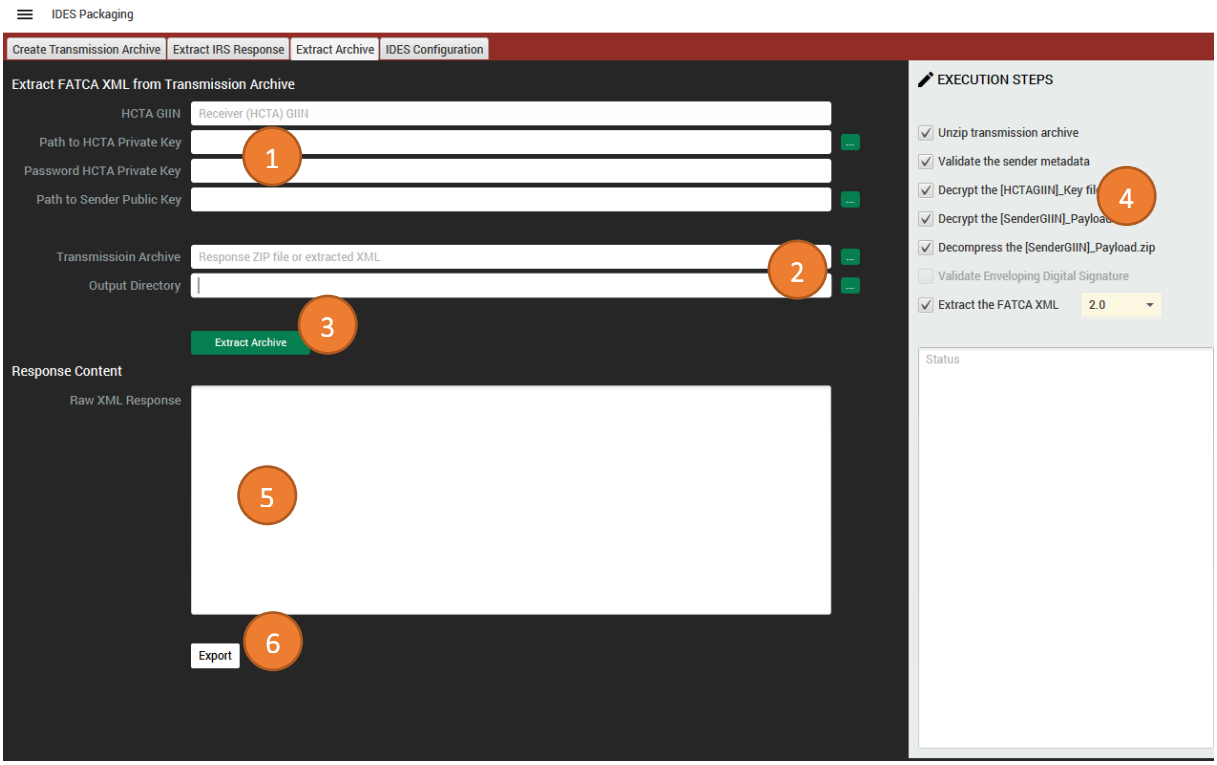
If the notification is of type error, the notification content (1) and the requested actions (2) are shown in the dedicated text areas. If it is a simple notification, only the notification is displayed, as there is no action required. The raw XML-file (3) is shown in any case.

To export the raw unsigned payload file to a location of your choice press the “Export”-Button (4). By clicking the “Export ErrorGroup” Button (5) you can export the error report to a formatted excel file at a location of your choice.

Reporting FI GIN	123456.0000.LE.756		
Reporting FI Name	New Bank		
FATCA Report Type Code	**Doc Ref ID**	**Record Level Error Code**	**Field Name**
ACCOUNT_REPORT	123456.0000.LE.756.8850655527787 6	8007	ReportingGroup/AccountReport/SubstantialOwner/Address
			ReportingGroup/AccountReport/AccountHolder/Organisation/TIN; ReportingGroup/AccountReport/AccountHolder/Individual/TIN
ACCOUNT_REPORT	123456.0000.LE.756.88211917010AdeKer472	8007	ReportingGroup/AccountReport/AccountHolder/AccHolderType
ACCOUNT_REPORT	123456.0000.LE.756.88912637004NeyMor140	8007	ReportingGroup/AccountReport/AccountHolder/Organisation/TIN; ReportingGroup/AccountReport/AccountHolder/Individual/TIN
			ReportingGroup/AccountReport/AccountHolder/AccHolderType

Extract Archive

The “Extract Archive” screen allows you to select all steps the tool should execute to extract a report delivered and signed by a financial institution (FI) or any other sender you are holding the receiver’s private key. Viewing the content is only possible after a complete and successful processing of the notification.



Before the start, fill the required HCTA/Receiver configuration either into the configuration tab or directly into the Extract Archive tab (1).

To start the extraction and verification of a FI payload, select the according delivery archive und output directory (2), mark all steps the tool should execute (3) - typically all.

Start the verification process by pressing the “Extract Archive” button (4).

Steps

First, select the encrypted payload zip file, which you received by the FI.

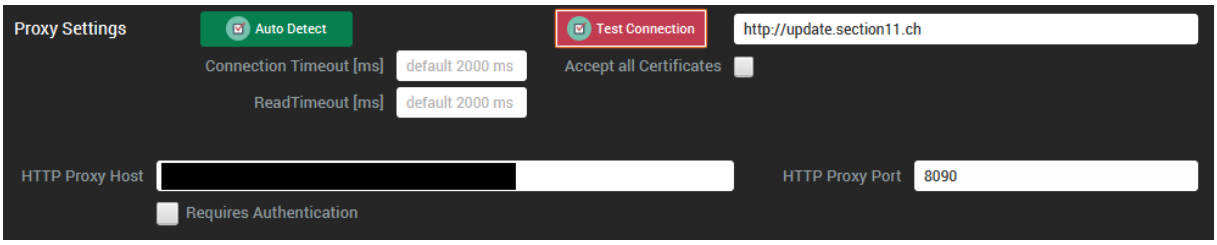
- Unzipping the transmission message archive
- Validating the extracted sender metadata XML file against the FATCA-IDES-SenderFileMetadata-1.3.xsd
- Decrypting the [HCTAGIIN/RECEIVER]_Key file using the configured private key
- Decrypting the [SenderGIIN]_Payload file with the one-time AES-key extracted in step (3)
- Decompressing the decrypted [SenderGIIN]_Payload.zip file
- Validating the extracted signed XML-File (only available, if a sender public key is entered)
- Validating the Payload XML-File the FATCA XML 2.0, 2.0.1 or 1.1 schema

After a successful extraction, you can view the content of the FATCA XML file in the “Raw XML” text area.

To export the raw payload file to a location of your choice press the “Export”-Button (6).

Proxy Configuration

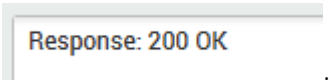
A proxy server generally sits on the gateway of a corporate network. When a client (computer) requests an object (web page, image, etc.) from an origin server (server hosted publicly on the Internet), a proxy server interrupts the communication. In such a case the proxy needs to be configured within the master data configuration to enable SFTP-Up and –Downloads.



To check, if your network settings require a proxy, press the "Test Connection"-Button without any configuration data entered. The software tries to open a connection to the given URL (e.g. http://update.section11.ch). In case of a failure the error message is displayed in the details area of the master data module:

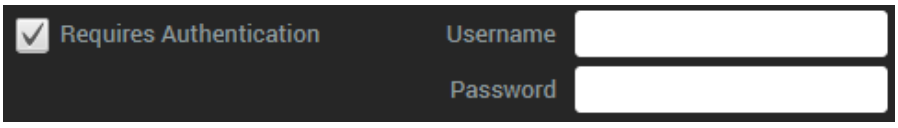


Now press the "Auto Detect" and the software tries to detect your proxy settings based on the operating system you are running. E.g. when your system uses a proxy automation script (PAC) Javascript it is used to determine the actual proxy.

Once a proxy is detected, re-try the connection test. It should now give a 

.

Some proxy servers request a login from the user before they will allow any connections. TRSuite has no support to handle this automatically. This needs to be done manually, because there is no way to read the login and password. Enter your user name and password into the displayed text fields. Please note: this login is used for the HTTP connections of TRSuite. SFTP transfers to the IDES gateway work through an HTTP proxy without login; a proxy that requires a login is not supported for SFTP, and TRSuite reports this when you connect. Ask your network administrator for a proxy rule without login for the IDES gateway, or for a direct connection.



And finally - Don't forget to save the changes.