FATCA | Foreign Account Tax Compliance Act

International Data Exchange Services (IDES)

User Guide

Publication 5190 (04-2015) Catalog Number 67386F Department of the Treasury Internal Revenue Service IRS.gov

Table of Contents

TABLE OF CONTENTS **2**

FIGURES **5**

TABLES **9**

DISCLAIMERS **11**

1. INTRODUCTION **12**

1.1. About FATCA 12

1.2. Purpose of Guide 12

1.3. Comments 13

1.4. Technical Support 13

2. INTERNATIONAL DATA EXCHANGE SERVICE (IDES) **13**

2.1. About IDES 13

2.2. Before You Begin 14

2.3. Authorized Users 14

2.4. System Availability 16

2.5. Data Security 17

2.6. File Retention 17

2.7. Requirements 18

2.8. HCTA Username and Password 19

3. OBTAIN A DIGITAL CERTIFICATE **19**

3.1. Purpose of a Digital Certificate 19

3.2. IRS Approved Certificate Authorities 19

3.3. Digital Certificate Format 20

3.4. Upload a Digital Certificate to IDES 20

3.5. Public Key Certificate 20

3.6. Certificate Maintenance 20

4. IDES ENROLLMENT **21**

4.1. Overview 21

4.2. IDES Enrollment Home Page 21

4.3. Enrollment Tab 23

4.4. Knowledge Base Tab 23

4.5. Support Tab 25

4.6. Help Desk Click to Call 26

DRAFT

4.7. IRS Public Key Tab 27
4.8. IDES Enrollment User Log In Tab 28
5. HCTA ADMINISTRATORS 29
5.1. Overview 29
5.2. Begin Enrollment 30
5.3. Create Challenge Questions 32
5.4. Create User Profile 33
5.5. Select Alert Preferences 35
5.6. Upload Digital Certificate 36
6. FI ADMINISTRATORS 38
6.1. Overview 38
6.2. Begin Enrollment 39
6.3. Create Challenge Questions 42
6.4. Create User Profile 43
6.5. Select Alert Preferences 44
6.6. Upload Digital Certificate 45
7. EXISTING ADMINISTRATORS (HCTA AND FI) 47
7.1. Add a User 47
7.2. Disable a User 49
7.3. Enable a User 52
7.4. Update the Certificate 55
7.5. Update Alert Preferences 57
7.6. Create a Metadata File 59
7.7. Reset Password 62
7.8. Download the IRS Public Key 64
8. END USERS 66
8.1. Create an Account 66
8.2. Create Challenge Questions 67
8.3. Create User Profile 68
8.4. Select Alert Preferences 69
8.5. IDES Enrollment User Log In 72
8.6. Create a Metadata File 73
8.7. Update Alert Preferences 75
8.8. Reset Password 77

DRAFT

8.9. Forgot Username 79
8.10. Forgot Password 82
9. DATA PREPARATION FOR FATCA XML REPORT 85
9.1. Overview 85
9.2. Prepare the FATCA XML File 85
Step 1 - Prepare and Validate the FATCA XML File 86
Step 1a - Sign the XML File 86
Step 2 - Compress the XML File 87
Step 3 - Encrypt the XML File with AES 256 Key 88
Step 4 - Encrypt the AES Key with Public Key of Recipient 89
Step 5 - Encrypt the AES Key – Model 1, Option 2 90
Step 6 - Create Sender Metadata File 91
Step 7 - Create a FATCA Data Packet 93
Step 8 - Transmit Data Packet using IDES 93
9.3. Receive an IRS Notification 94
10. ACCESS THE IDES GATEWAY 95
10.1. Overview 95
10.2. Reset Password 96
10.3. Session Timeout 96
10.4. User Interface Overview 96
10.5. Global Preferences 99
10.6. Alert Preferences 100
11. TRANSMIT A FATCA REPORT 100
11.1. IDES Transmission Archive 100
11.2. IDES Transmission ID 101
11.3. Retransmissions 101
11.4. Folder Structure 101
11.5. Transmit a File Using Web UI 102
11.5.1. Upload a File 102
11.5.2. Download a File 104
11.6. Model 1, Option 2 HCTA 105
11.7. Transmit a File Using SFTP 108
11.8. Connect to IDES SFTP using Windows Secure Copy (WinSCP): 108

DRAFT

12. ALERTS 110
12.1. OVERVIEW 110
12.2. RECEIVE ALERTS 111
13. IDES REPORTS 113
13.1. IDES SENTINEL WEB MONITORING 113
13.1. SYSTEM TIMEOUT 113
13.2. ACCESSIBILITY 113
13.5 CONNECT TO IDES SENTINEL MONITORING USING WEB BROWSER 115
13.5 SEARCH OPTIONS AND REPORT SUMMARY 117
13.6 SEARCH TRANSMISSION AND ALERT HISTORY 118
13.7 VIEW SEARCH RESULTS 120
13.8 SAVE SEARCH REPORTS 121
APPENDIX A: ACRONYMS 122
APPENDIX B: FILE NAMING CONVENTION 124
APPENDIX C: CERTIFICATE UPLOAD ERROR MESSAGES 125
APPENDIX D: HCTA FATCA ENTITY ID COMPOSITION 127
APPENDIX E: TYPES OF ALERTS 128
APPENDIX F: DATA PREPARATION USER TIPS 133

DRAFT

Figures

Figure 1 - IDES Process Overview. 14
Figure 2 - File Retention Flow. 18
Figure 3 – IDES enrollment home page. 22
Figure 4 – IDES overview and enrollment tool page. 23
Figure 5 - IDES Knowledge Base page. 24
Figure 6 – IDES Support page. 25
Figure 7 – Help Desk Click to Call 26
Figure 8 – Access the IRS public key. 27
Figure 9 – IRS public key certificate information. 27
Figure 10 – IDES enrollment user log in page. 28
Figure 11 – Access IDES enrollment. 30

Figure 12 – Begin the enrollment process. 31
Figure 13 – Log in as an HCTA Administrator. 31
Figure 14 – IDES GIIN found page. 32
Figure 15 – Create IDES challenge questions. 33
Figure 16 – Submit user profile information. 34
Figure 17 – Select IDES alert preferences. 35
Figure 18 – Upload a digital certificate. 36
Figure 19 – Select a digital certificate. 37
Figure 20 – Enrollment confirmed. 37
Figure 21 – Access IDES enrollment. 39
Figure 22 – Begin the enrollment process. 40
Figure 23 – Log in as an FI Administrator. 41
Figure 24 – IDES GIIN verification page 41
Figure 25 – Create IDES challenge questions. 42
Figure 26 – Submit user profile information. 43
Figure 27 – Select IDES alert preferences. 44
Figure 28 – Upload a digital certificate. 45
Figure 29 – Select a digital certificate. 46
Figure 30 – Enrollment confirmed. 46
Figure 31 – Add an end user. 47
Figure 32 – Send an enrollment invitation. 48
Figure 33 – New user added. 48
Figure 34 – IDES welcome email. 49
Figure 35 – Disable a user. 50
Figure 36 – Select a user to disable. 50
Figure 37 – Verify user to disable. 51
Figure 38 – User disabled confirmation. 51
Figure 39 – Enable a user. 52
Figure 40 – Select a user to enable. 53
Figure 41 – Verify the user to enable. 53

DRAFT

Figure 42 – User enabled confirmation. 54
Figure 43 – Update a user certificate. 55
Figure 44 – Upload a digital certificate. 55
Figure 45 – Select a digital certificate. 56
Figure 46 – Updated digital certificate confirmation. 56
Figure 47 – Update alert preferences. 57
Figure 48 – Select the user profile to update. 58
Figure 49 – Select new alert preferences. 59
Figure 50 – Create a Metadata File. 60
Figure 51 – Enter Metadata File information. 61
Figure 52 – Reset a password. 62
Figure 53 – Select the user to update. 63
Figure 54 – Create a new password for the selected user. 63
Figure 55 – Download the IRS public key 64
Figure 56 – General certificate information. 65
Figure 57 – IDES new end user welcome email. 66
Figure 58 – Create IDES challenge questions. 67
Figure 59 – Submit user profile information. 68
Figure 60 – Select IDES alert preferences. 69
Figure 61 – Enrollment Confirmation. 71
Figure 62 – IDES enrollment user log in page. 72
Figure 63 – Log in to the IDES enrollment site. 72
Figure 64 – Manage an IDES user account. 73
Figure 65 – Create a Metadata File. 74
Figure 66 – Update IDES alert preferences. 75
Figure 67 – Selecting new alert preferences. 76
Figure 68 – Reset a password. 77
Figure 69 – Create a new password. 78
Figure 70 – Request a Username reminder email. 79
Figure 71 – Enter an email address for a username reminder message. 80
DRAFT

Figure 72 – Reminder email sent confirmation. 80
Figure 73 – IDES username reminder email. 81
Figure 74 –User email address not recognized error message. 81
Figure 75 – Forgot Password reset page. 82
Figure 76 – Enter a username to reset a password. 83
Figure 77 – Email sent to users to reset a password. 83
Figure 78 – Create a new password. 84
Figure 79 - Data preparation overview 86
Figure 80 - IDES Gateway Log In Screen. 95
Figure 81 - IDES Session Timeout message. 96
Figure 82 - IDES Gateway home screen. 97
Figure 83 – Select global preferences. 99
Figure 84 – Set alert preferences 100
Figure 85 - Select and upload files. 102
Figure 86 - View file transfer status in Transfers Queue. 103
Figure 87 - Temporary file and transfer status 103
Figure 88- IDES file download screen. 104
Figure 89 – Save a file. 104
Figure 90 - Model 1 Option 2 Folder Structure 105
Figure 91 - IDES Pending status folder. 106
Figure 92 – IDES file options. 106
Figure 93 - IDES rename file options. 107
Figure 94 - Sample SFTP connection. 108
Figure 95 - SSH Authentication Disclaimer. 109
Figure 96- SFTP Warning Dialog. 109
Figure 97 – SFTP Connection. 110
Figure 98 – IDES Alert flow chart for transmission uploads. 111
Figure 99 - Sample IDES Alert e-mail message. 112
Figure 100 - IDES home page 113
Figure 101 - Accessibility keyboard shortcuts 114

DRAFT

Figure 102 - IDES Accessibility Home Page 114
Figure 103 - IDES transfer history Search options 114
Figure 104 - IDES Accessibility transfer history results 115
Figure 105 - Disclaimer Screen. 115
Figure 106 - IDES Sentinel Login Screen. 116
Figure 107 - Sentinel Monitoring home screen 116
Figure 108 - IDES Sentinel search parameters. 118
Figure 109 - Search parameter for alert codes 119
Figure 110 - IDES Sentinel monitoring search results. 119
Figure 111 - IDES Sentinel search results screen 120
Figure 112 - Detailed information dialog box 120
Figure 113 - IDES Sentinel Report Generator. 121

DRAFT

Tables

Table 1- FATCA Related Documents. 13
Table 2 - Table Valid User Types and Features. 16
Table 3 - System Requirements. 17
Table 4- IDES Enrollment Requirements. 18
Table 5 - IRS-approved Certificate Authorities 20
Table 6 – HCTA IDES Alert Preferences 36
Table 7 – FI IDES Alert Preferences 45
Table 8 – IDES Alert Preferences 70
Table 9 – Overview process to prepare and send a file. 85
Table 10 – Process to digitally sign a file. 87
Table 11- Recommended compression tools based on compression testing and supported algorithms. 88
Table 12 – Process to compress a file. 88
Table 13 – Process to encrypt an XML file with an AES key. 89
Table 14 – Process to encrypt an AES key with a public key. 90

Table 15 – Process for a Model 1 Option 2 FI to encrypt an AES key. 91
Table 16 - Sender Metadata Schema summarizes each element. 92
Table 17 – Files contained in a transmission archive or data packet. 93
Table 18- Process to open a notification message archive. 94
Table 19- IDES User Interface Overview. 98
Table 20 – IDES Gateway folders and subdirectories. 101
Table 21 – Summary description of IDES reporting process for Model 1 Option 2 HCTAs. 107
Table 22 - Summary of available reports 117
Table 25 – Table of acronyms used in this document. 123
Table 26 – IDES file naming conventions. 124
Table 27 – IDES Certificate Upload Error Messages. 126
Table 28 – IDES HCTA FATCA Entity ID composition. 127
Table 29- Types of IDES Alerts 132

DRAFT

Disclaimers

This document is a draft and is being provided to the public for information purposes only. Information in this document is indicative, and is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, for any purpose, without the express written of permission the IRS.

All screen shots that appear throughout the IDES User Guide (IRS Publication 5190) are used with the permission of the IRS. The screen shots used in this publication—or any other screen shots from IDES or its affiliated programs—may not be extracted, copied, or distributed without written approval from the IRS SPEC Office of Products, Systems, & Analysis.

DRAFT

An Additional Note about Screen Shots:

Screen shots contained in this draft are intended for illustrative purposes only and may not match the IDES Enrollment and IDES Gateway sites exactly. The FATCA IDES team will continue to update screen shots in future versions of the guide.

1. Introduction

1.1. About FATCA

The Foreign Account Tax Compliance Act (FATCA) was enacted as part of the Hiring Incentives to Restore Employment (HIRE) Act in March 2010. FATCA was created to improve transparency and address tax non-compliance by U.S. taxpayers. Generally, FATCA requires foreign financial institutions (FFIs) to report to the IRS certain information about financial accounts held by specified U.S. persons or by foreign entities with one or more substantial U.S. owners, or face 30 percent withholding on certain U.S.-source payments (withholdable payments). An FFI commits to the reporting requirement by registering and signing an FFI agreement with the IRS. In addition, FATCA requires withholding agents to withhold 30 percent on withholdable payments made to passive non-financial foreign entities (NFFEs) that do not provide information on their substantial U.S. owners to withholding agents. A NFFE may elect to report directly to the IRS certain information about its substantial U.S. owners in lieu of providing such information to withholding agents (direct reporting NFFE). FATCA also requires U.S. withholding agents to report to the IRS information about substantial US owners of a payee that is a passive NFFE, and specified US persons holding certain equity or debt interests in a payee that the withholding agent has agreed to treat as an owner-documented FFI. For more information on what to report under FATCA, see the Instructions for Form 8966, FATCA Report.

Financial Institutions (FIs) and direct reporting NFFEs that register with the IRS under FATCA are issued a Global Intermediary Identification Number (GIIN) and appear on the FFI List published by the IRS. The FFI List Search and Download tool allows users to search entities by GIIN, financial institution name, or country. For more information on FATCA, visit the FATCA Home Page.

To facilitate FATCA implementation for FIs operating in jurisdictions with laws that prevent the FIs from complying with the terms of the FFI agreement, the Treasury Department developed two alternative model intergovernmental agreements (IGAs) (Model 1 IGA and Model 2 IGA) that allow FIs operating in such jurisdictions to perform due diligence and reporting on their account holders to achieve the objectives of FATCA.

1.2. Purpose of Guide

This guide is intended to serve as a tool for FIs, direct reporting NFFEs, Host Country Tax Authorities (HCTAs), sponsoring entities, trustees of trustee-documented trusts, and U.S. withholding agents who enroll in the International Data Exchange Service (IDES) to transmit FATCA data. The document assumes that the reader is familiar with the FATCA regulations and is experienced with extensible markup language (XML) and schema technology. For the purpose of this document, direct reporting NFFEs, sponsoring entities, and trustees of trustee-documented trusts should follow the instructions set forth for FIs. Additionally, the term “U.S. withholding agent” includes a territory FI treated as a U.S. person.

DRAFT

Document	Description
FATCA Online Registration User Guide (Publication 5118)	Provides instructions for the online system to complete an electronic Form 8957, FATCA Registration
FFI List Search and Download Tool User Guide (Publication 5147)	Provides instructions on how to use the FFI List Search and Download Tool to search for an approved GIIN
FATCA XML Schema v1.1 User Guide (Publication 5124)	Explains the information required to be included in each data element of the schema
FATCA Sender Metadata Schema v1.0 User Guide (Publication 5188)	Explains the schema and elements of a FATCA metadata file
FATCA Reports Notification XML Schema v1.4 User Guide (Publication 5189)	Explains the schema and elements of FATCA notifications
Instructions for Form 8966, FATCA Report	Provides instructions for the paper Form 8966, FATCA Report

Table 1- FATCA Related Documents.

1.3. Comments

We appreciate your feedback on the quality and usefulness of this publication. Please send comments, with a reference to chapter, section, and page number(s), to lbi.fatca.ides@irs.gov.

1.4. Technical Support

IDES technical assistance is available Monday through Friday, 24 hours a day, except for U.S. federal holidays, through the IDES Customer Service Help Desk. IDES customer support will send a system alert from the help desk portal for planned outages and scheduled maintenance.

2. International Data Exchange Service (IDES)

2.1. About IDES

IDES is a secure managed file transfer service that is available to FIs and HCTAs to facilitate FATCA reporting. This reporting is provided for under U.S. Treasury Regulations, the FFI agreement, Tax Information Exchange Agreements (TIEAs), Intergovernmental Agreements (IGAs), and other guidance issued by the Treasury Department and the IRS. The data collected through IDES will be incorporated into IRS compliance operations.

IDES is accessible to enrolled users over the Internet via Hypertext Transfer Protocol Secure (HTTPS) or Secure File Transfer Protocol (SFTP). IDES provides for an end-to-end controlled file transfer with enhanced monitoring and security features. The system only accepts encrypted electronic submissions, and will allow for the transmission of FATCA reporting in the approved FATCA XML Schema v1.1 (FATCA XML). For more information on FATCA regulations, Form 8966 and instructions, FATCA XML, and other related topics, visit the FATCA Home Page.

The main function of IDES is to provide authorized users with secure exchange services for FATCA data transmissions, with the additional protection of a Public Key Infrastructure (PKI). The primary features of IDES are:

- Enrollment
- Certificate Management
- Account Management
- Secure Data Transmission
- Status of Data Transmission (Alerts and Notifications)

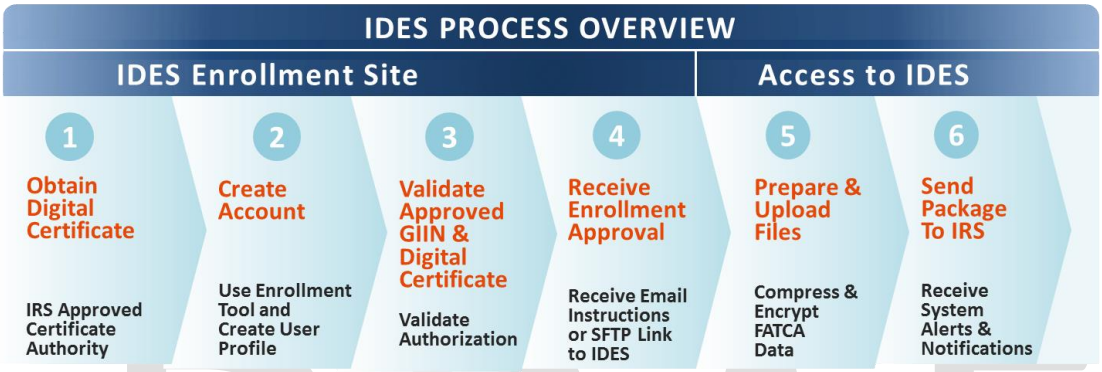


Figure 1: IDES Process Overview.

DRAFT

2.2. Before You Begin

This material is intended to supplement the contents of IDES online help and is not intended to replace technical documentation to establish and test SFTP connections. Examples shown in this document are based upon a Windows environment and may differ if using other operating systems.

2.3. Authorized Users

Authorized IDES users are FIs, direct reporting NFFEs, sponsoring entities, trustees of trustee-documented trusts, U.S. withholding agents, and HCTAs. Each authorized user has limited access to the system based on the data flow model described in their agreement with the United States (for example, an IGA or an FFI agreement) or in Treasury regulations. Note that for many IDES users, the IRS is the only valid recipient for files. The table below provides additional information regarding user access based on agreement types.

Type of Agreement	User Type	Access Description
Model 1B IGA (Non-Reciprocal) FI transmits data directly to its HCTA then the HCTA transmits data to the IRS	FI	No Access
	HCTA	On behalf of FI under the HCTA jurisdiction: ▪ Upload FATCA reporting for direct transfer to IRS ▪ Download alerts generated by IDES ▪ Download notifications and Competent

		Authority Requests (CARs) submitted by IRS
Model 1A IGA (Reciprocal) FI transmits data directly to its HCTA then the HCTA transmits data to the IRS. This is a reciprocal model with two-way transmission between the HCTA and the IRS	FI	No Access
	HCTA	On behalf of FI under the HCTA jurisdiction: ▪ Upload FATCA reporting for direct transfer to IRS ▪ Download alerts generated by IDES ▪ Download notifications and CARs submitted by IRS Reciprocal data will be exchanged with HCTA
Model 1 Option 2 FFI transmits data directly to its HCTA via IDES. The HCTA approves or rejects the FATCA reporting data. If approved, IDES releases the data to the IRS.	FI	Upload FATCA reporting to IDES for review by HCTA Download alerts generated by IDES Download notifications submitted by IRS (subject to the terms of the country's IGA)
	HCTA	Upload approved or rejected FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications and CARs submitted by IRS
Model 2 IGA and FFI agreement FFI transmits data regarding: ▪ Consenting accountholders directly to the IRS ▪ Aggregate information on non-consenting accountholders and non-consenting, non-participating FFIs directly to IRS ▪ Specific information on non-consenting accountholders and non-consenting, non-participating FFIs directly to HCTA. HCTA may deliver data to IRS after a treaty request	FI	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS (subject to the terms of the country's IGA)
	HCTA	Upload FATCA reporting regarding non-consenting accountholders and non-consenting, non-participating FFIs for direct transfer to IRS (after treaty request) Download alerts generated by IDES Download notifications and CARs submitted by IRS
Non-IGA (FFI agreement) FFI transmits data directly to the IRS	FFI	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS
	HCTA	No Access
Non-IGA (no FFI agreement)	Direct Reporting NFFE, U.S. Withholding Agent (USWA), Sponsoring Entity, or Trustee of Trustee-	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS

DRAFT

	Documented Trust	

Table 2 - Table Valid User Types and Features.

2.4. System Availability

IDES requires a username and password, which can be obtained through the IDES enrollment process. The system will be available 24 hours a day, with the exception of U.S. holidays and regularly scheduled system maintenance periods. All users will be notified of planned outages, as well as unplanned outages that are expected to last more than 8 hours.

IDES works with all major browsers and can be accessed using different FTP clients for Secure File Transfer Protocol (SFTP).

Items	Technical Specifications
Browsers for HTTPS	▪ Apple Safari 5.x, 6.x on OS X only ▪ Google Chrome 33.x or later ▪ Microsoft Internet Explorer 9, 10, 11 (IE 8 and Compatibility View are not currently supported) ▪ Mozilla Firefox 29 or later ▪ Cookies enabled
FTP clients	▪ Axway Secure Client 5.8, 6.0, 6.1 ▪ cURL 7.19 to 7.22 ▪ CuteFTP Professional 8.3.2 to 9.0.5 ▪ FileZilla Client 3.5x ▪ IglooFTP PRO 3.9 ▪ Ipswitch WS_FTP 12.2, 12.3 ▪ LFTP 3.7 to 4.3.2 ▪ SmartFTP Client 3.0, 4.0
SSH clients	▪ Axway Secure Client 5.8, 6.0, 6.1 ▪ cURL 7.19 to 7.22 ▪ FileZilla Client 3.5.x ▪ PSCP 0.60 ▪ PSFTP 0.60 ▪ Tectia Client 6.1, 6.2 ▪ VanDyke SecureFX 6.6.1 to 6.7 ▪ WinSCP 4.2.9 to 4.3.5
JavaRuntime Environment (JRE)	▪ JRE 1.6 or later
JavaScript	▪ JavaScript enabled
File Size	▪ File uploads and downloads are limited to a size of 200 MB compressed.
File Naming Conventions	▪ See Appendix B for file naming conventions. ▪ Only file extension .zip are authorized for file uploads to IDES in the user Outbox folders ▪ File names are case insensitive ▪ Do not use illegal characters in the name of files, such as colon, backslash, question mark or space

DRAFT

Table 3 - System Requirements.

Note: Axway Secure Transport Web Access Plus (508-compliant WebUI) requires JRE 1.6 or later.

2.5. Data Security

IDES provides secure file data transfers by using symmetric and asymmetric encryption schemes to encode data. IDES uses the Advanced Encryption Standard (AES), a specification for encryption of electronic data established by the United States National Institute of Standards and Technology (NIST).

When a supported web browser connects to IDES via HTTPS, the Transport Layer Security (TLS) cryptographic protocol provides communication security over the Internet and the session is encrypted for data confidentiality. When a supported FTP client connects to IDES via SFTP, the Secure Shell (SSH) network protocol provides secure file transfer functionality over a reliable data stream. The IDES Enrollment website requires account authentication through the use of strong passwords. Files cannot be opened, read, or decrypted at any point during data transmission.

2.6. File Retention

IDES provides secured temporary file storage for data transmissions and prohibits long term data storage. Data packets that contain errors, such as files with an unencrypted payload or virus, will be automatically deleted.
Generally, each file transmitted from the U.S. to a receiver remains available for download for a period of 7 days, based on the date the file was created.

A user receives an IDES Alert or Notification that a transmission is available for download. The file will remain available for download in the receiver's account inbox for 7 days. An inbox folder may contain several different transmitted files at the same time, each with a different payload. For the purpose of this document, the term payload will be used to describe the body of the data packet (e.g. a FATCA XML document) that serves as the fundamental purpose of the data transmission.

If the receiver does not download the file within 7 days, the files expires and will be automatically deleted. After a file is deleted, it cannot be retrieved, downloaded or restored. If the receiver initiates the file download within 7 days, the file should be downloaded within 24 hours from the time the download is initiated. After 24 hours, the file expires and will be automatically deleted.

The file retention times vary slightly based on model types. Please refer to 11.6 for more details on file retention times for files sent under Model 1 Option 2.

DRAFT

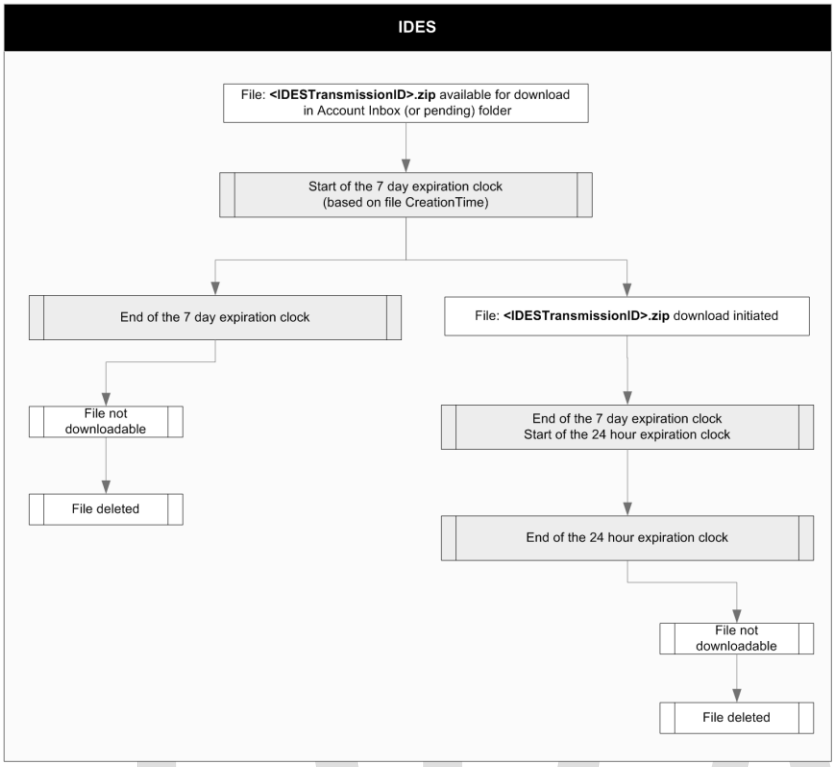


Figure 2- File Retention Flow.

2.7. Requirements

Certain requirements are needed to create a new account on the IDES Enrollment site. Requirements differ for HCTA and FI users.

Valid User Type		
Requirements	**HCTA**	**FI**
Registered GIIN See IRS FFI List for more information	N/A	X
HCTA FATCA Entity ID See Appendix D: for more information	The IRS provided usernames to your Competent Authority. Contact the IRS for more information	N/A
Valid certificate issued by an IRS approved certificate authority (CA) See Obtaining a Certificate for more information	X	X
Public and Private Key	X	X
Email address of additional users	X	X

Table 4- IDES Enrollment Requirements.

DRAFT

Note: For U.S. withholding agents that do not have a requirement to obtain a GIIN but are required to report using the FATCA XML, a separate web link will direct the user to a modified enrollment page. These users will receive a FATCA Entity ID that will be treated like a GIIN for the purpose of IDES enrollment only. For information on how to obtain a GIIN, refer to the FATCA Online Registration System User Guide.

2.8. HCTA Username and Password

All countries under Model 1 IGAs have a pre-assigned username and HCTA FATCA Entity ID. Each HCTA FATCA Entity ID is in the format: **000000.00000.TA.<ISO>**. ISO is the ISO 3166-1 numeric standard country code. Please refer to Appendix D: for more information.

The first time a user logs on to IDES, the user is required to change its assigned username and create a password. A letter containing information on the username and enrollment instructions will be sent to an appropriate contact from each country based on their agreement with the United States. For additional information, contact FATCA IDES at lbi.fatca.ides@irs.gov.

3. Obtain a Digital Certificate

3.1. Purpose of a Digital Certificate

Certificates and their related private keys are used to sign and decrypt messages between the sending party and the IRS. A digital certificate binds an identity to a public key. A certificate authority (CA) issues a certificate after an identity proofing process to verify the certificate owner. The individual identified in the certificate has possession and control over the private key associated with the public key found in the certificate.

3.2. IRS Approved Certificate Authorities

The IRS only accepts certificates issued by approved CAs. A published list of certificate authorities and acceptable digital certificate products is available on IRS.gov.

Certificate Authority	Type of Certificate	External Website Links
Digicert®	SSL Plus™ (Single Name)	https://www.digicert.com/welcome/ssl-plus.htm
Entrust®	Standard SSL	http://www.entrust.net/ssl-certificates/standard.htm
GlobalSign®	Organization SSL	https://www.globalsign.com/ssl/organization-ssl/
IdenTrust	TrustID Server (SSL)	https://www.identrust.com/certificates/buy_trustid_server.htmlhttp://identrust.com/irs/fatca/index.html

StartCom®	StartSSL™ EV	https://www.startssl.com/?app=30
Symantec/Verisign	Secure Site SSL	http://www.symantec.com/ssl-certificates/secure-site/?inid=vrsn_symc_ssl_SS
Thawte®	SSL Web Server	http://www.thawte.com/ssl/web-server-ssl-certificates/index.html

Table 5 - IRS-approved Certificate Authorities.

3.3. Digital Certificate Format

Before you begin the IDES enrollment process, each entity should obtain one valid digital certificate issued by an approved certificate authority (CA). IDES will ONLY accept digital certificates issued by an approved CA. Supported formats for the digital certificates are:

- Distinguished Encoding Rules (DER) binary X.509
- Privacy Enhanced eMail (PEM) ASCII (Base-64) encoded X.509

IDES will convert digital certificates received in DER format to Base64 for storage and retrieval.
If a digital certificate is not in DER or PEM format, use Windows 7 to convert your digital certificate to DER or PEM as follows:

- Open the digital certificate with a .CRT filename extension
- Select the Details tab
- Select the "Copy to File…" button
- In the Certificate Export Wizard, select the format you want to use as either "DER encoded binary X.509 (.CER)" or "Base-64 encoded X.509 (.CER)".

3.4. Upload a Digital Certificate to IDES

After an FI or HCTA administrator obtains a digital certificate, the user will provide the certificate to IDES during the enrollment process. Upon upload, the certificate is validated with the Certificate Authority (CA) that issued the certificate. IDES stores the certificate and makes it available to other IDES users who will use it to verify digital signatures and encrypt symmetric key files. It is the responsibility of IDES users to verify that the certificate is still valid at the time they attempt to use it. Please refer to 5.6 for more information on how to upload a digital certificate to an IDES account.

3.5. Public Key Certificate

A public key certificate, also known as a digital certificate, is an electronic document used to prove ownership of a public key. The IRS public key certificate can be downloaded during IDES enrollment. The Administrator will upload the digital certificate for its FI or HCTA during enrollment. All public keys or certificates are made available for all IDES users.

3.6. Certificate Maintenance

IDES uses a Public Key Infrastructure (PKI) to manage and revoke digital certificates. The CA sets the lifetime of each digital certificate, typically up to one year. IDES requires one digital certificate per FI or HCTA.

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked, meaning that they are not trustworthy, and should not be used. CRLs are always issued by the trusted CA and are publicly available. IDES validates all digital certificates against the most current CRL published from each trusted CA to identify any revoked digital certificates. A revoked digital certificate will be deleted from IDES, along with the associated public key contained in the digital certificate. IDES will immediately deactivate the user account associated with a revoked digital certificate.

DRAFT

The Online Certificate Status Protocol (OCSP) is an Internet protocol designed for real-time verification of digital certificates against a database of revoked digital certificates. IDES tests all digital certificates using the OCSP to verify whether the digital certificates are valid. For example, when a transmission uses an expired digital certificate, IDES tests the certificate using the OCSP, confirms the certificate is revoked, and deletes the transmitted file. Users are not able to transmit the file until a valid digital certificate is resubmitted.

4. IDES Enrollment

4.1. Overview

IDES Enrollment is required for FIs and HCTAs to access the IDES environment. Users must enter a valid GIIN and certificate to enroll. FIs or HCTAs with invalid or expired certificates cannot enroll.

IDES Enrollment Options:

- Add, Update and Delete a User
- Update Certificate
- Disable/Enable a User
- Select Alert Preferences
- Create Metadata File

DRAFT

4.2. IDES Enrollment Home Page

The IDES Enrollment site can be accessed through:

- IDES Enrollment Web User Interface
- Secure File Transfer Protocol (SFTP)

The IDES Enrollment site contains links to various IDES resources and includes five main tabs in addition to the Home tab:

- Enrollment
- Knowledge Base
- Support
- IRS Public Key
- IDES Enrollment User Log In

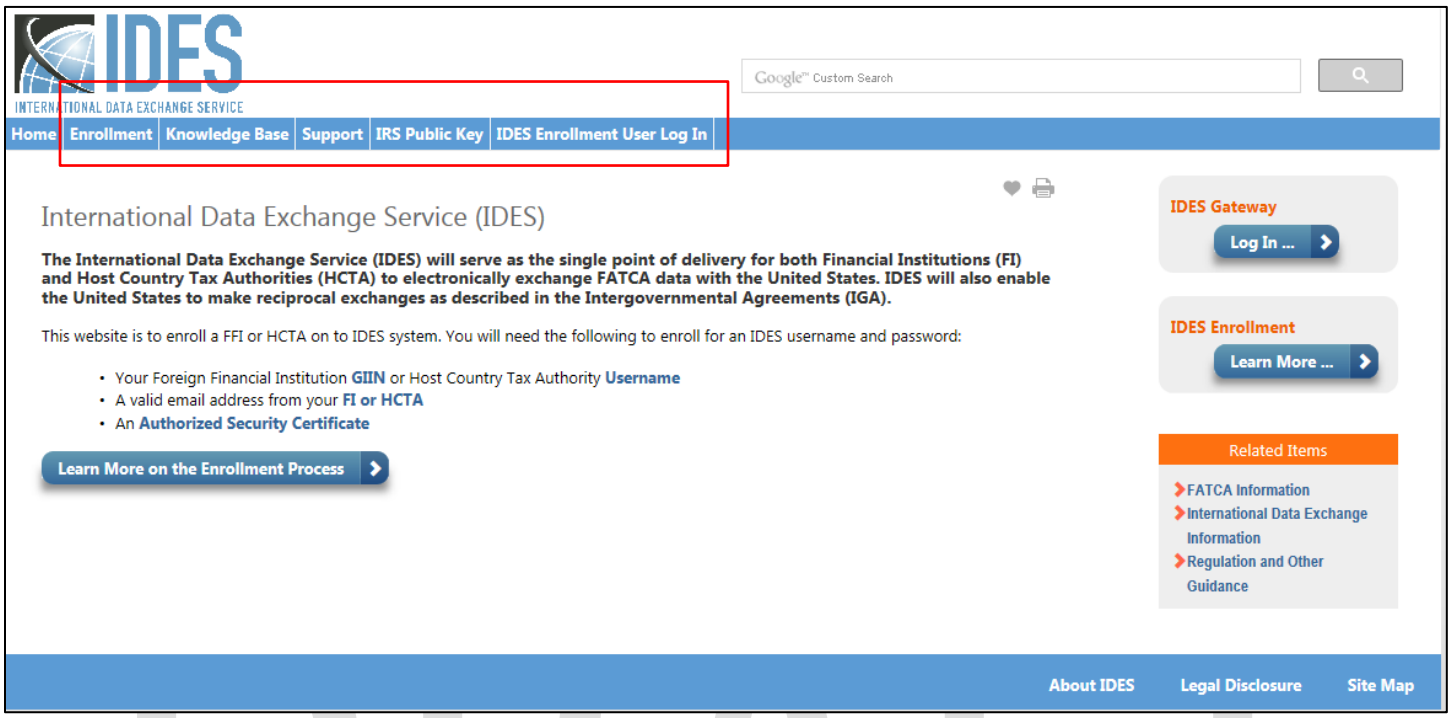


Figure 3 – IDES enrollment home page.

DRAFT

4.3. Enrollment Tab

The Enrollment tab describes the IDES enrollment process and provides users with access to create an IDES account. The Enrollment tab also links to the IDES Gateway, a web application that allows enrolled HCTAs and FIs to securely upload and download FATCA data over the Internet using both HTTPS and SFTP protocols.

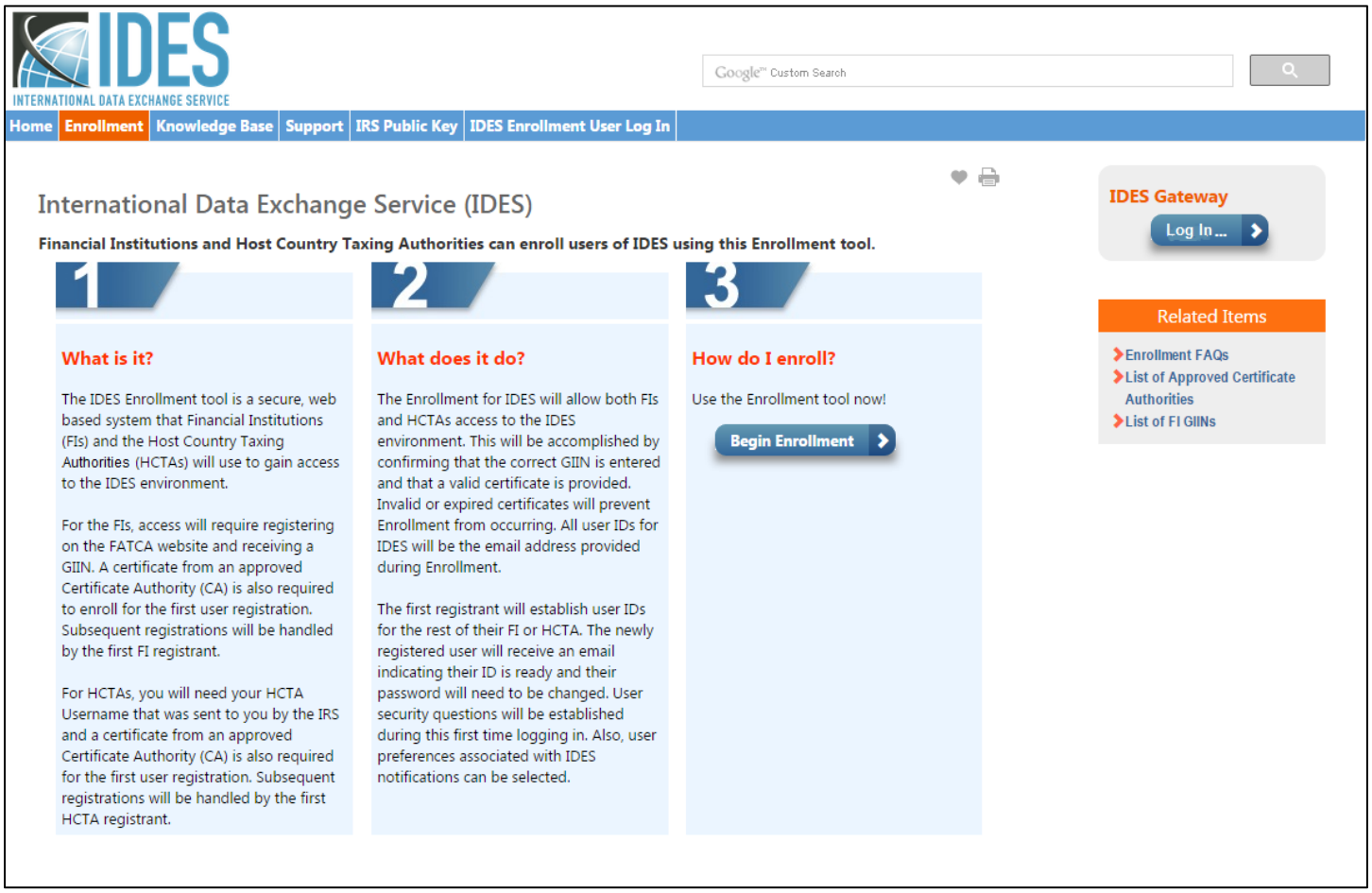


Figure 4 – IDES overview and enrollment tool page.

4.4. Knowledge Base Tab

The Knowledge Base tab directs users to important IDES documentation such as user guides and an interactive knowledge base.

Users can access the following resources from the Knowledge Base tab:

- Interactive IDES Knowledge Base
- IDES User Guides
- IDES Frequently Asked Questions (FAQs)

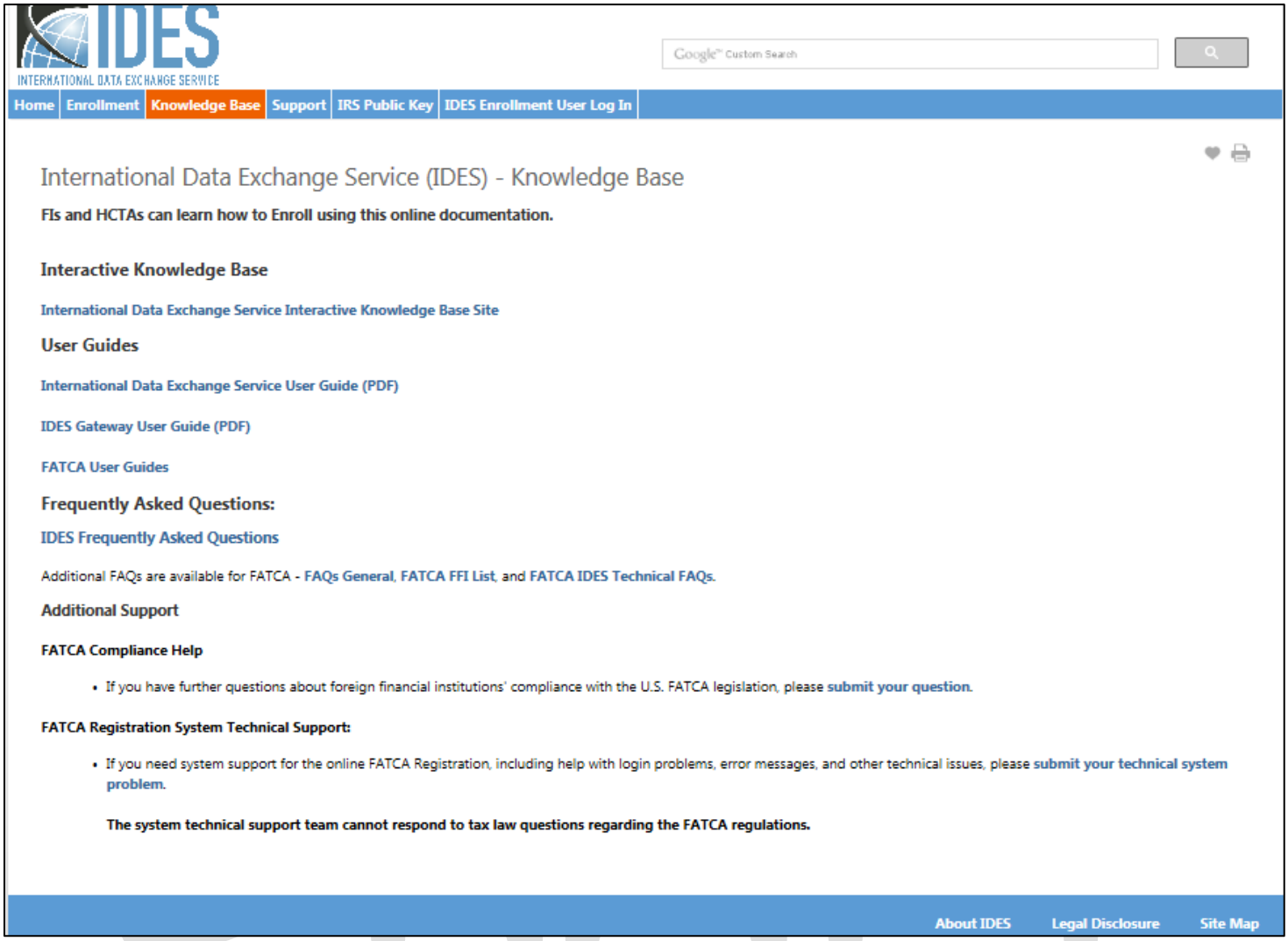


Figure 5 - IDES Knowledge Base page.

4.5. Support Tab

The IDES help desk is available to assist users with log in problems, error messages, and other technical issues. The Support tab provides contact information for the help desk and hours of operation. The help desk can be contacted by phone or via an online form which allows users to submit technical system problems. The click to call feature allows users to dial the help desk directly from the internet browser. Please note that the help desk is available in English only.

Users can access the following resources from the Support tab:

- Email Support
- Phone Support
- Help Desk Hours of Operation
- Submit Technical System Problems

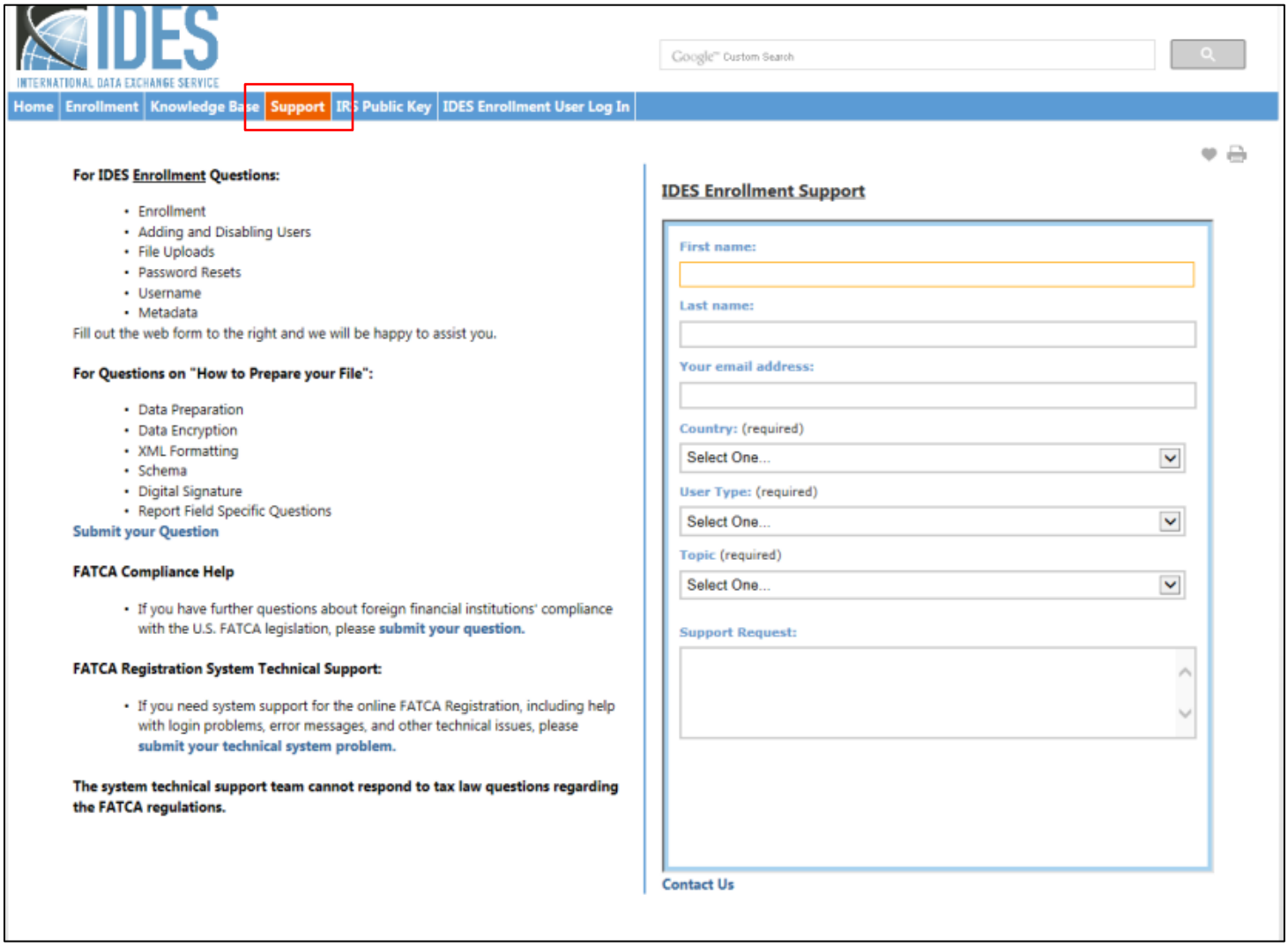


Figure 6 – IDES Support page.

4.6. Help Desk Click to Call

Figure 7 – Help Desk Click to Call

1. From the **IDES Support** page, select **IDES Help Desk – Click to Call** button.
2. In the **Enter Your Phone Number:** drop down box, select a country and enter phone number.
3. Select **Click to Call.**
4. The help desk will contact you.

DRAFT

4.7. IRS Public Key Tab

The IRS Public Key is a certificate that can be downloaded from the IDES Enrollment site. This certificate should be included in the FATCA transmission archive transmitted to the IRS.

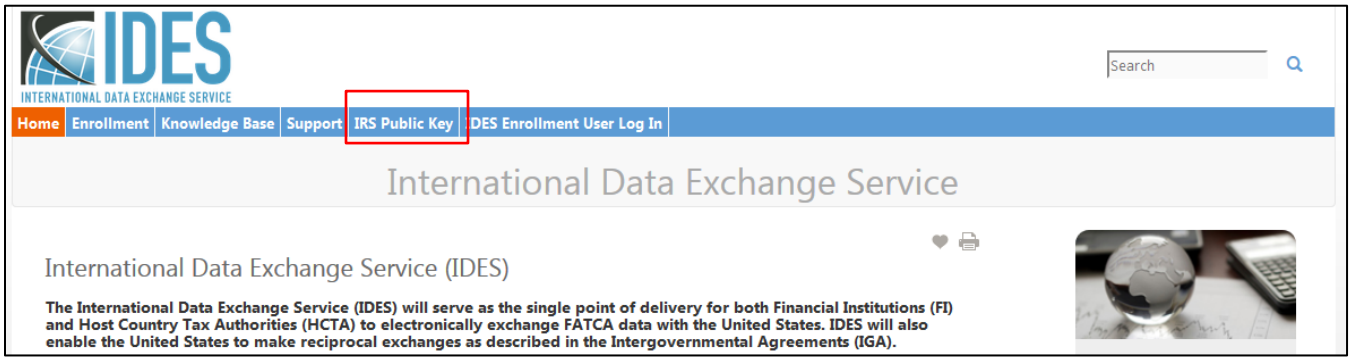


Figure 8 – Access the IRS public key.

1. From the IDES Support home page, click the **IRS Public Key** tab.

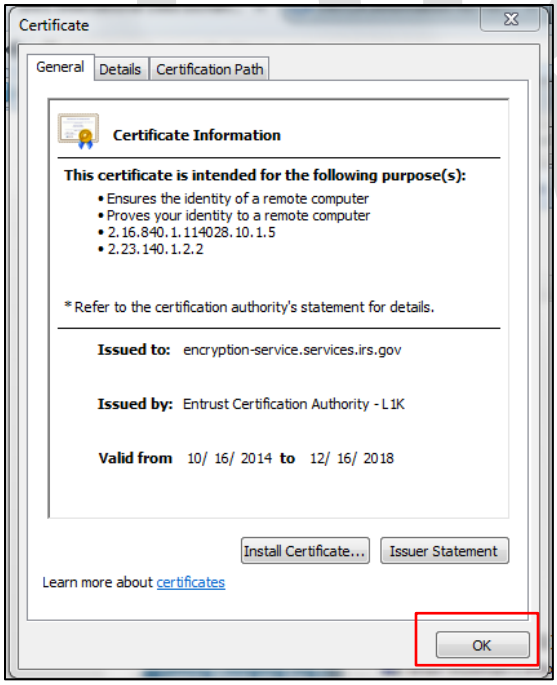


Figure 9 – IRS public key certificate information.

2. Download and save the IRS Public Key Certificate to your computer.
3. The certificate should be included in the transmission archive .zip file transmitted to the IRS via the IDES Gateway.

DRAFT

4.8. IDES Enrollment User Log In Tab

The IDES Enrollment User Log In tab allows returning users to access the IDES Enrollment site. HCTA Administrators, FI Administrators, and end users are able to log in after they have created an IDES account.

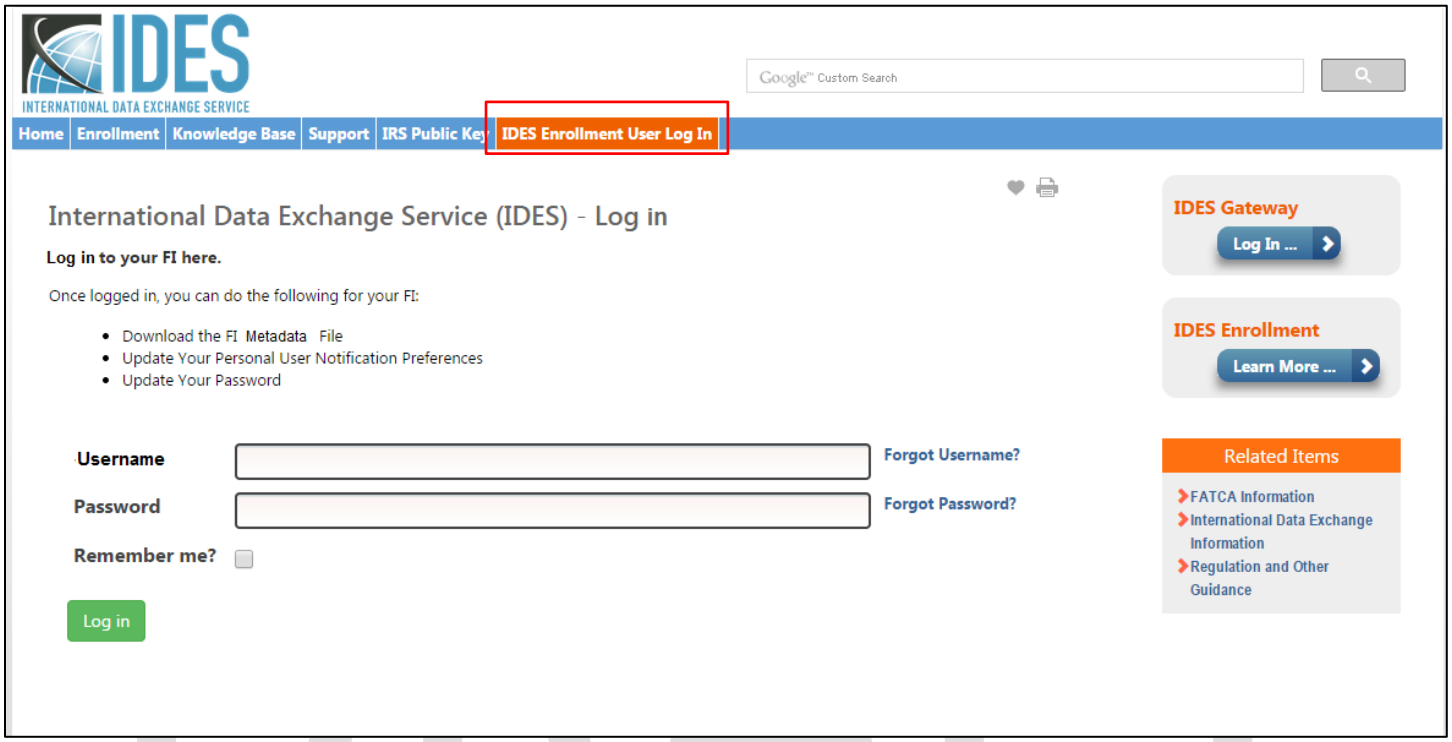


Figure 10 – IDES enrollment user log in page.

DRAFT

5. HCTA Administrators

5.1. Overview

HCTAs will play the following roles under the IGAs:

- **Model 1 IGA HCTA:** The partner jurisdiction agrees to report to the IRS specified information about the U.S. accounts maintained by all relevant FIs located in the jurisdiction.
- **Model 2 IGA HCTA:** The partner jurisdiction agrees to direct and enable all relevant FIs located in the jurisdiction to report specified information about their U.S. accounts directly to the IRS.

HCTAs will need their IRS assigned username in order to create an IDES account. The first user that registers for an IDES account, on behalf of their HCTA, is considered the Administrator. HCTA Administrators are able to add end users, disable and enable end users, update the certificate, update alert notifications, create a metadata file, reset passwords, and download the IRS Public Key.

Authorized end users (users under the HCTA Administrator) have limited capabilities and may update their alert notifications, create a metadata file, and reset their password.

To create an account, the HCTA Administrator will create challenge questions and a password. The HCTA Administrator will then upload their digital certificate received from an IRS-approved certificate authority.

Note: To replace an existing administrator, please contact IDES help desk support.

DRAFT

5.2. Begin Enrollment

The IDES Enrollment site can be accessed at https://www.ides-support.com.

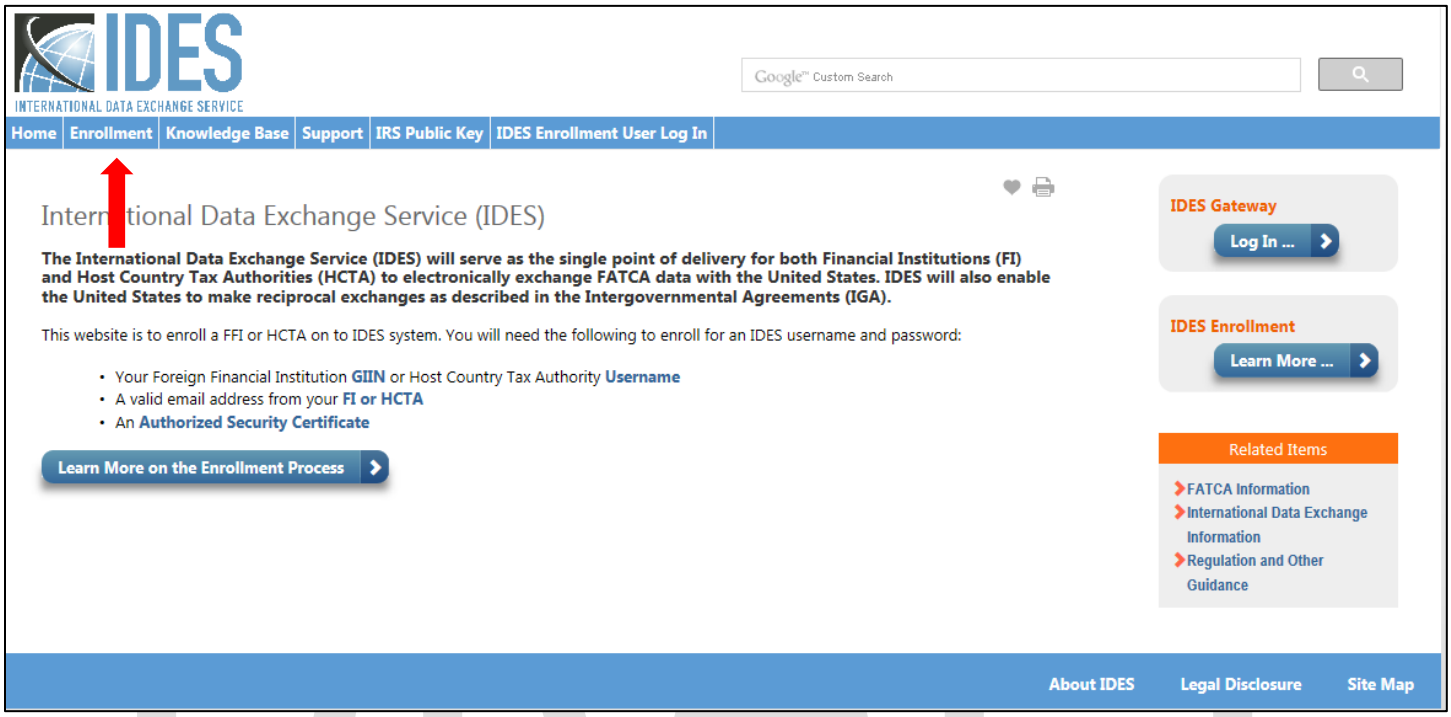


Figure 11 – Access IDES enrollment.

1. Click on the **Enrollment** tab.

DRAFT

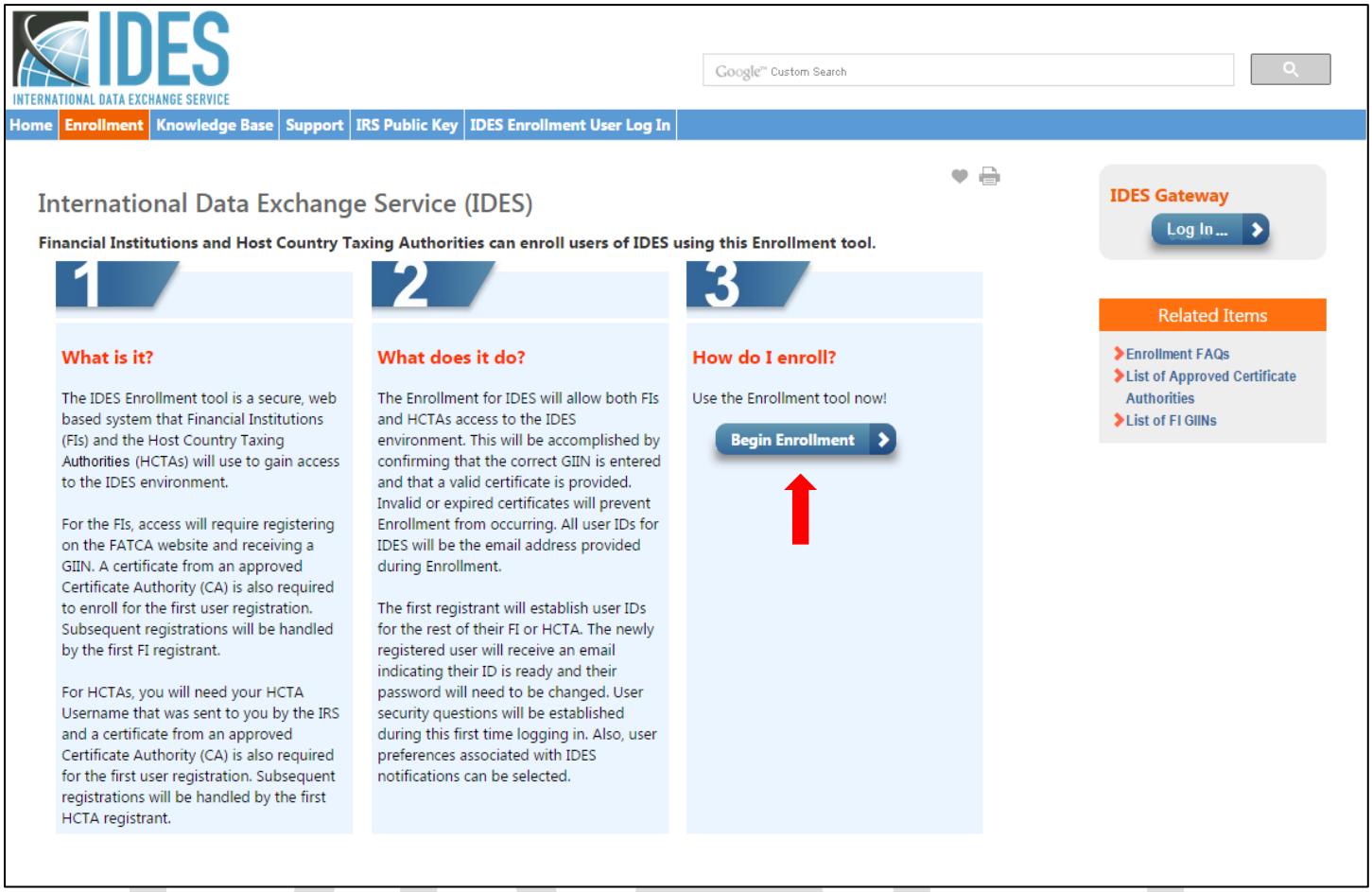


Figure 12 – Begin the enrollment process.

2. Click on **Begin Enrollment** to start the enrollment process as an HCTA Administrator.

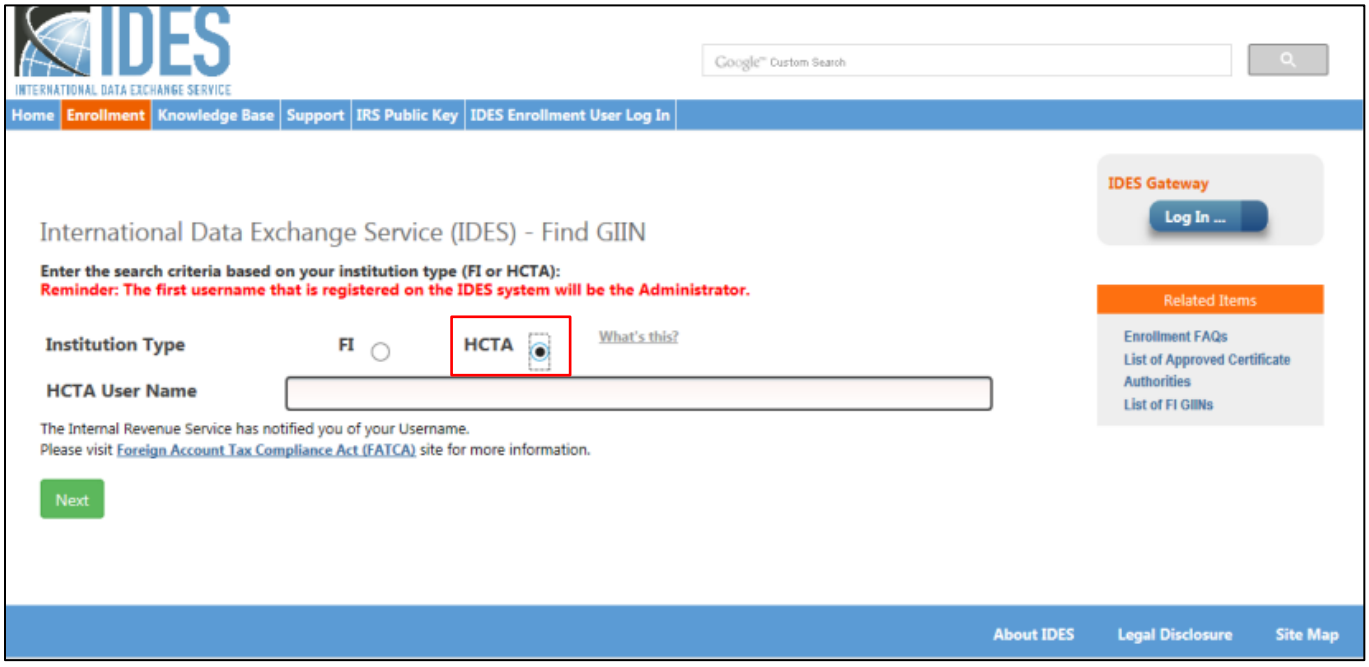


Figure 13 – Log in as an HCTA Administrator.

3. Select **HCTA**.
4. In **HCTA Username**, enter your username assigned by the IRS. If you have not received an HCTA username, contact your local Competent Authority or IDES help desk support.
5. Click **Next** to continue.

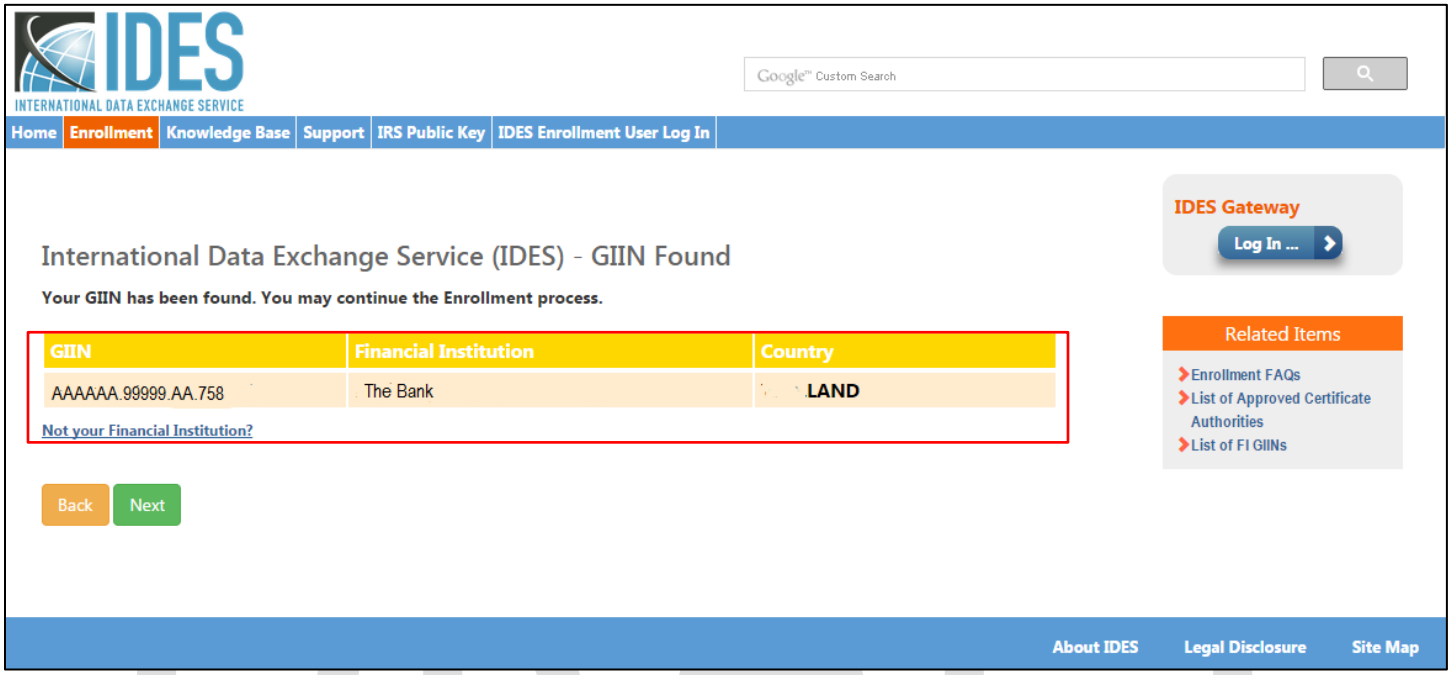


Figure 14 – IDES GIIN found page.

6. Confirm information and verify **GIIN**, **Financial Institution/HCTA** and **Country** are correct. Note that the Financial Institution name and GIIN must exactly match the name and GIIN as shown on the IRS FFI List.
7. Click **Next** to continue and set up **Challenge Questions**.

5.3. Create Challenge Questions

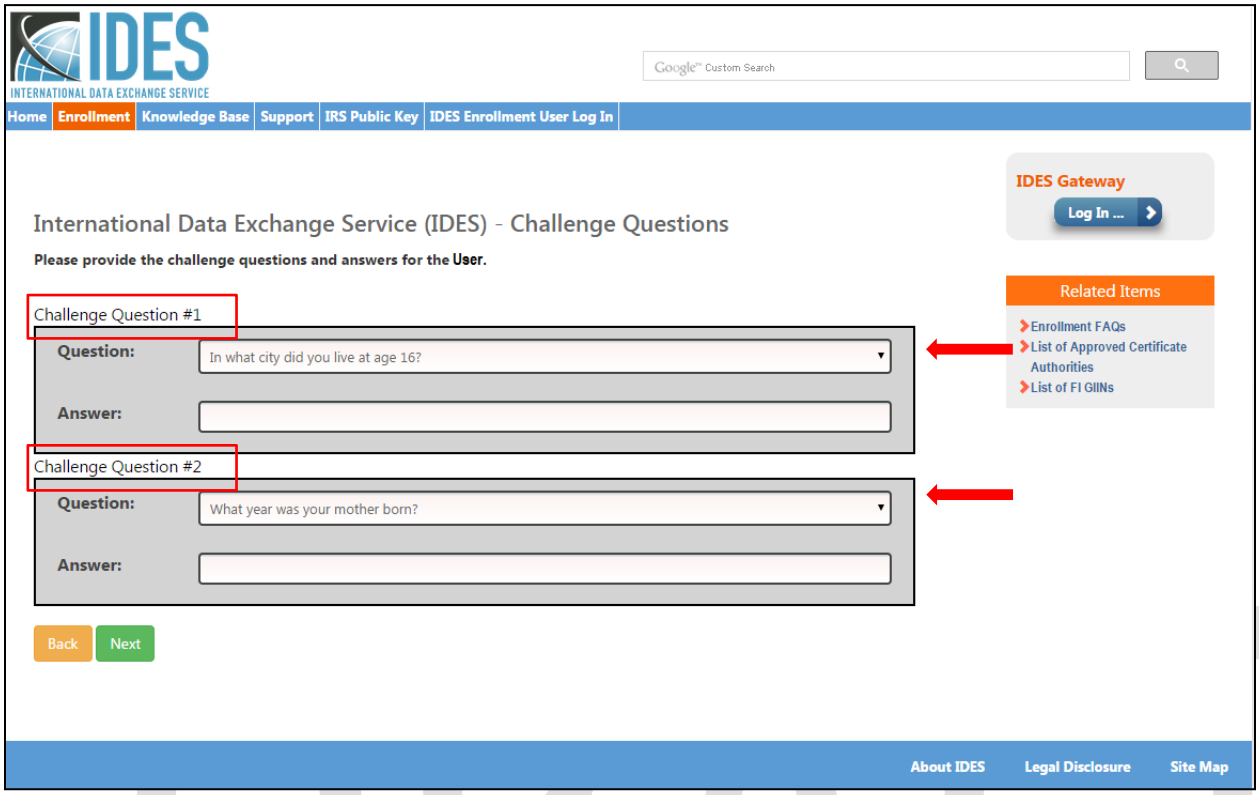


Figure 15 – Create IDES challenge questions.

1. **Challenge Question #1**
   a. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   b. Answer: Type a response to the challenge question.
2. **Challenge Question #2**
   a. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   b. Answer: Type a response to the challenge question.
3. Click **Next** to continue and set up a **Username**

IMPORTANT: Remember to document your answers to your challenge questions. Users will need these answers to reset a password or to contact the IDES Help Desk. Note that challenge question responses must exactly match the responses as originally submitted.

5.4. Create User Profile

DRAFT

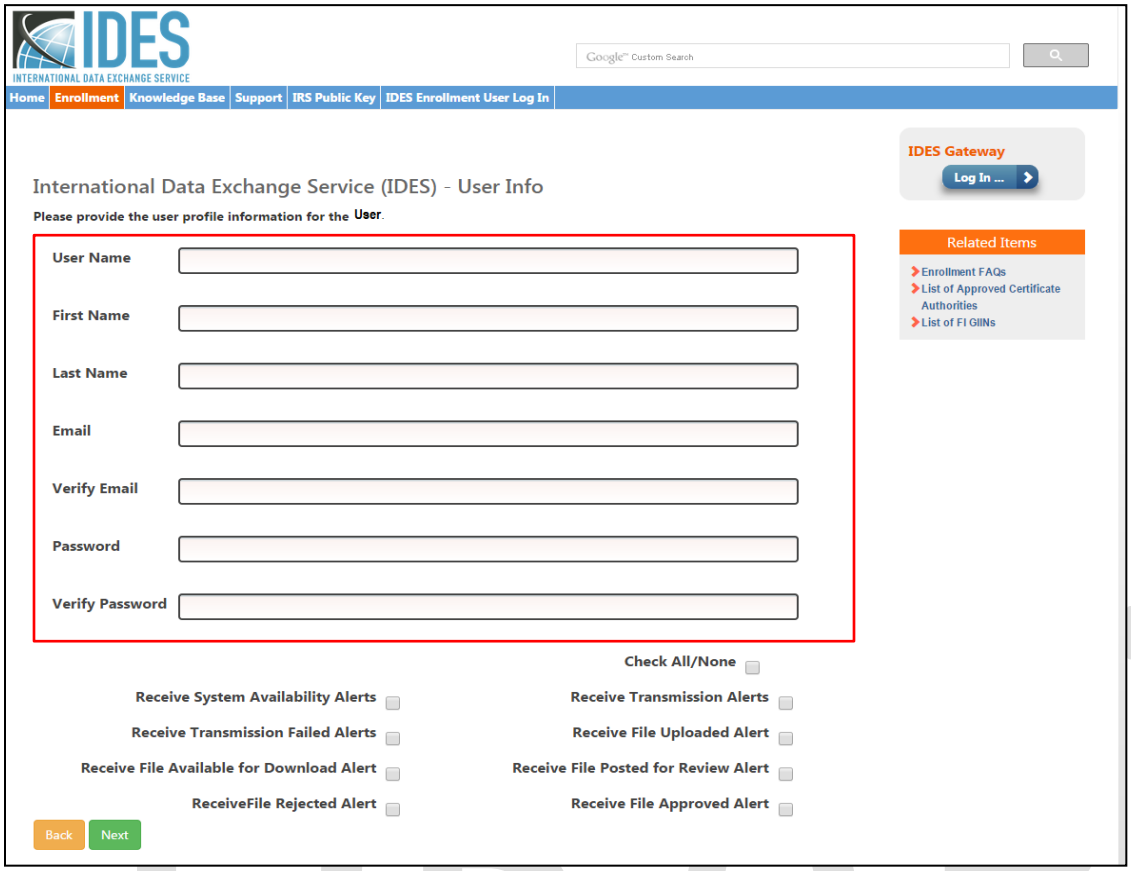


Figure 16 – Submit user profile information.

1. **Username** – Enter your new username. We recommend first initial and last name. If the username is already taken, you will receive an error message.
2. **First Name** – Enter your first name.
3. **Last Name** – Enter your last name.
4. **Email** – Enter your email address.
    a. It is mandatory to use a unique email address for enrollment as the system will not allow for duplicate email addresses. The email address may be a personal email address or a shared mailbox address.
5. **Verify Email** – Enter your email address again (must match the previous entry). If it does not match, you will receive an error message.
6. **Password** – Create a valid password.
    a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .).
    b. If you enter a password that does not meet the guidelines, you will receive an error message.
7. **Verify Password** – Re-type your password (must match the previous entry). If it does not match, you will receive an error message.

DRAFT

5.5. Select Alert Preferences

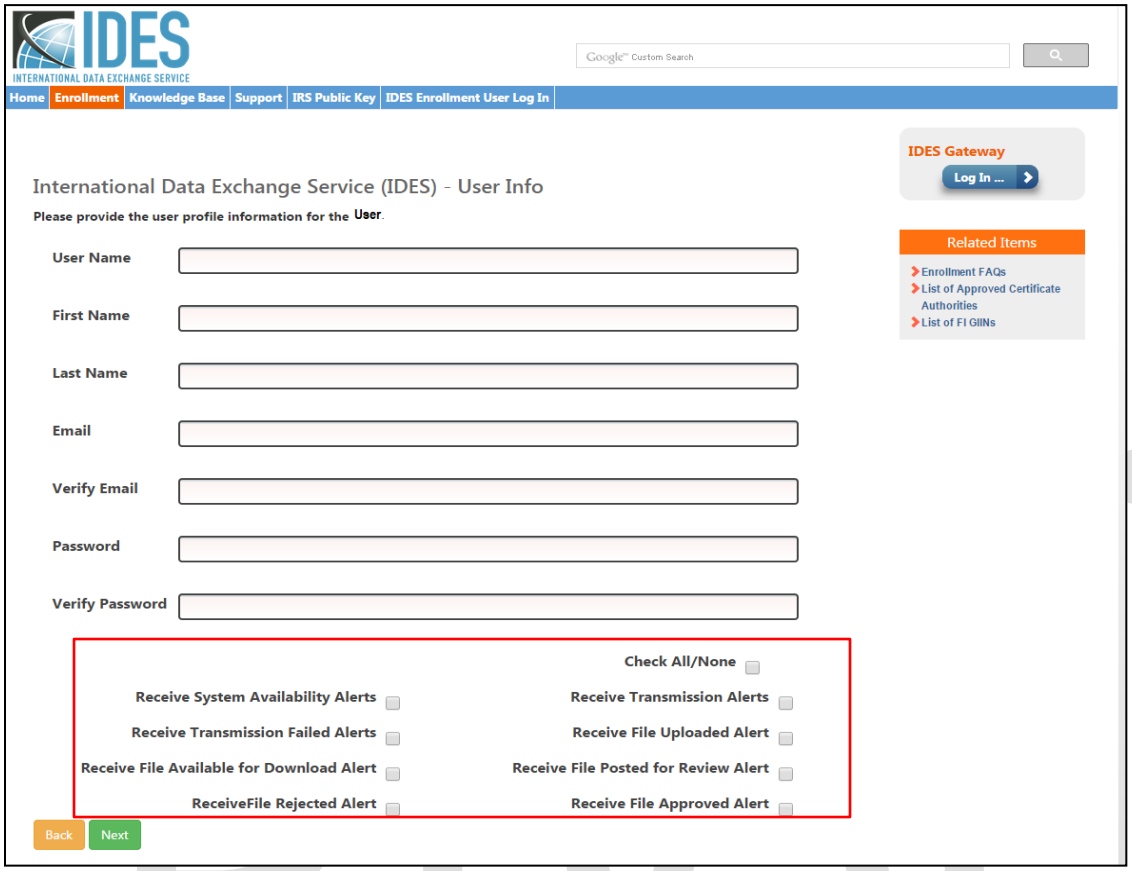


Figure 17 – Select IDES alert preferences.

1. **Select Alert Preferences** – Click on the box next to the alerts you wish to receive by email. You can click the **Check All/None** box to choose all alerts or to remove all alerts. You must select user preferences to receive alerts. There are eight Alert Preferences.

Alert Preference	Description
a. System Availability Alert	IDES Enrollment and/or IDES Gateway are unavailable.
b. Transmission Failed Alert	Transmission uploaded via the IDES Gateway failed for one of several reasons (e.g., virus, encryption validation, naming convention, package content). The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission failed.
c. File Available for Download Alert	The user has a file to download on the IDES Gateway. This is not functional at this time.
d. File Rejected Alert (for Model 1 Option 2 countries)	Transmission upload was rejected by the HCTA. The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission was rejected.

e. Transmission Alert	Receive all IDES Alerts (See Alerts **b,c,d,f,g,h**).
f. File Uploaded Alert	Received transmission is uploaded to the IRS for review.
g. File Posted for Review Alert (for Model 1 Option 2 countries)	Sent to the HCTA when an FI uploads a report.
h. File Approved Alert (for Model 1 Option 2 countries)	Sent after HCTA has approved the FI file.

Table 6 – HCTA IDES Alert Preferences

Note that Alert Preferences may be modified at a later date.

2. Click **Next** to continue to upload digital certificate.

5.6. Upload Digital Certificate

Each entity should obtain a digital certificate issued by an approved CA. The digital certificates should be in a DER or PEM format. For more information, refer to 19.

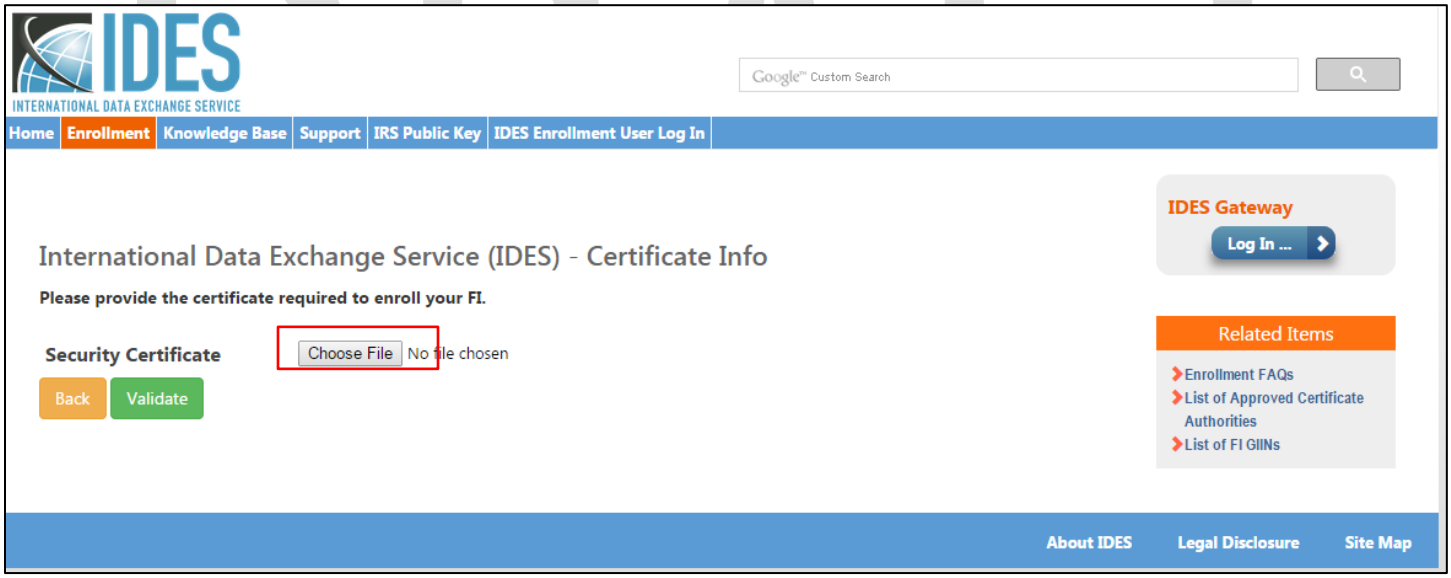


Figure 18 – Upload a digital certificate.

1. Click **Choose File** to search for the certificate located on your computer.

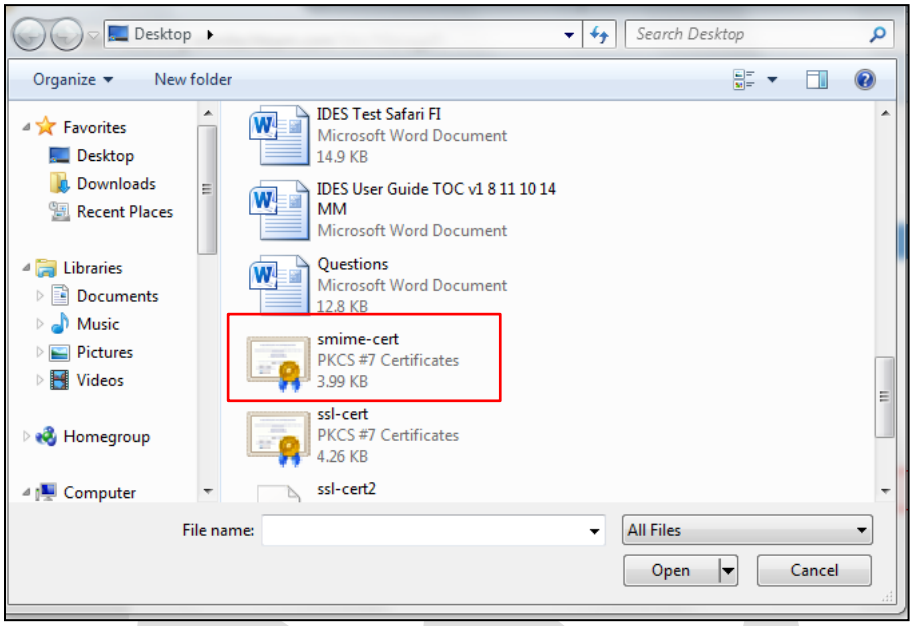


Figure 19 – Select a digital certificate.

2. Select the Active/Valid certificate file from your computer.
3. Click **Open.**
4. Click **Validate.**
    a. If you receive an error message, refer to Appendix C: Certificate Upload Error Messages or contact IDES customer support for assistance.

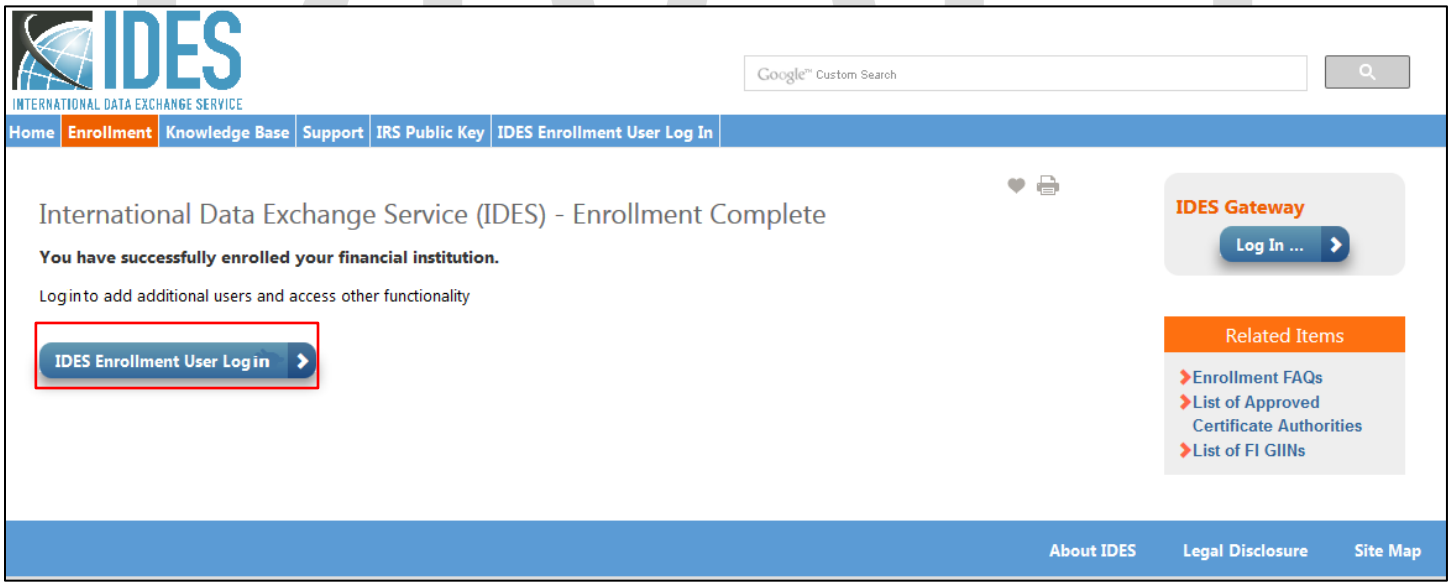


Figure 20 – Enrollment confirmed.

5. After you have validated your certificate, the enrollment process is complete. You will receive an email from the IDES help support desk that verifies your access to the IDES Gateway.
6. Click **IDES Enrollment User Log In** to log in as the HCTA Administrator.

DRAFT

6. FI Administrators

6.1. Overview

Only registered FIs that have a valid GIIN may create an IDES account. The first user that registers for an IDES account, on behalf of their FI, is considered the administrator. The FI administrator is able to add, disable and enable end users, update the certificate, update alert preferences, create a metadata file, reset passwords, and download the IRS Public Key.

Financial Institutions include, but are not limited to:

- Depository institutions (for example, banks).
- Custodial institutions (for example, mutual funds).
- Investment entities (for example, hedge funds or private equity funds).
- Certain types of insurance companies that have cash value products or annuities.

End users (users under the FI Administrator) will be able to update their alert preferences, create a metadata file, and reset their password. To create an account, the FI Administrator will create challenge questions and a password. The FI Administrator will also upload the digital certificate received from an IRS approved Certificate Authority.

DRAFT

6.2. Begin Enrollment

The IDES enrollment site can be accessed at https://www.ides-support.com.

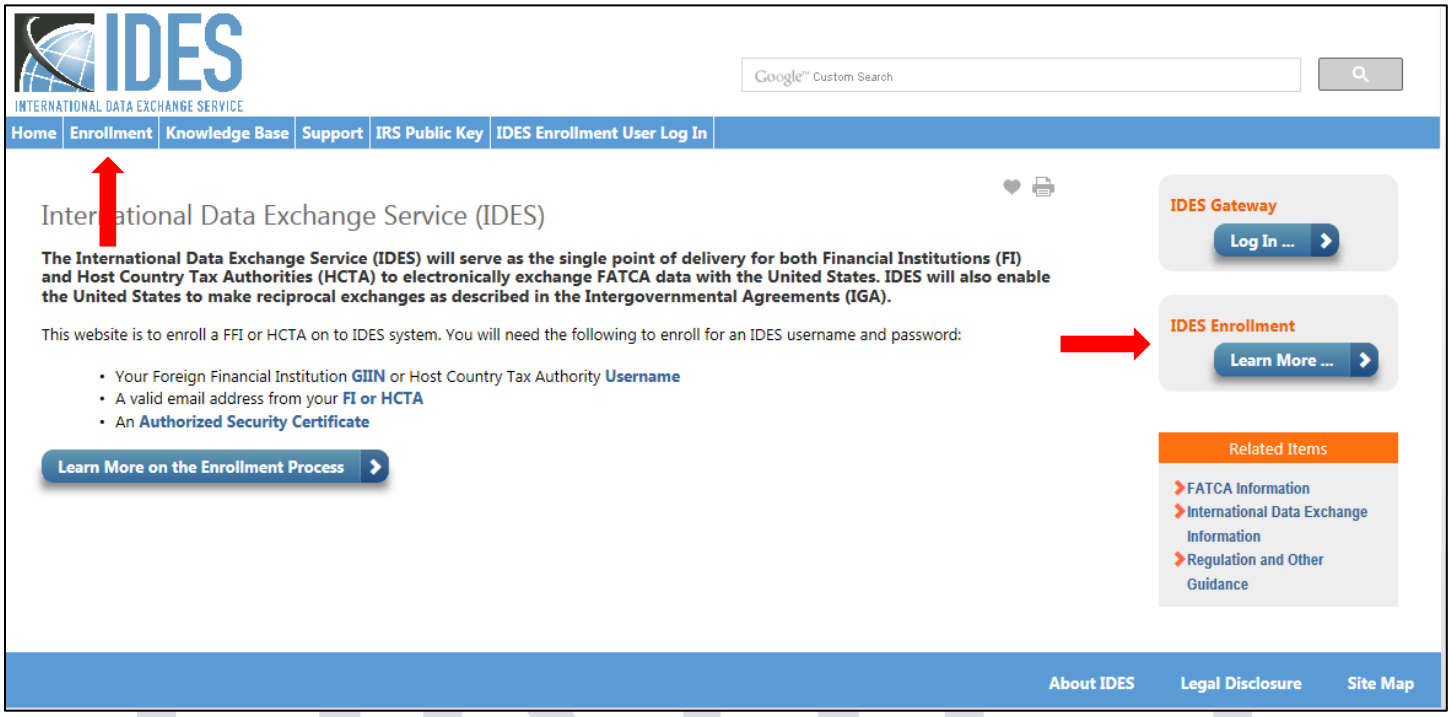


Figure 21 – Access IDES enrollment.

1. Click **Learn More** under IDES Enrollment or select the **Enrollment** tab.

DRAFT

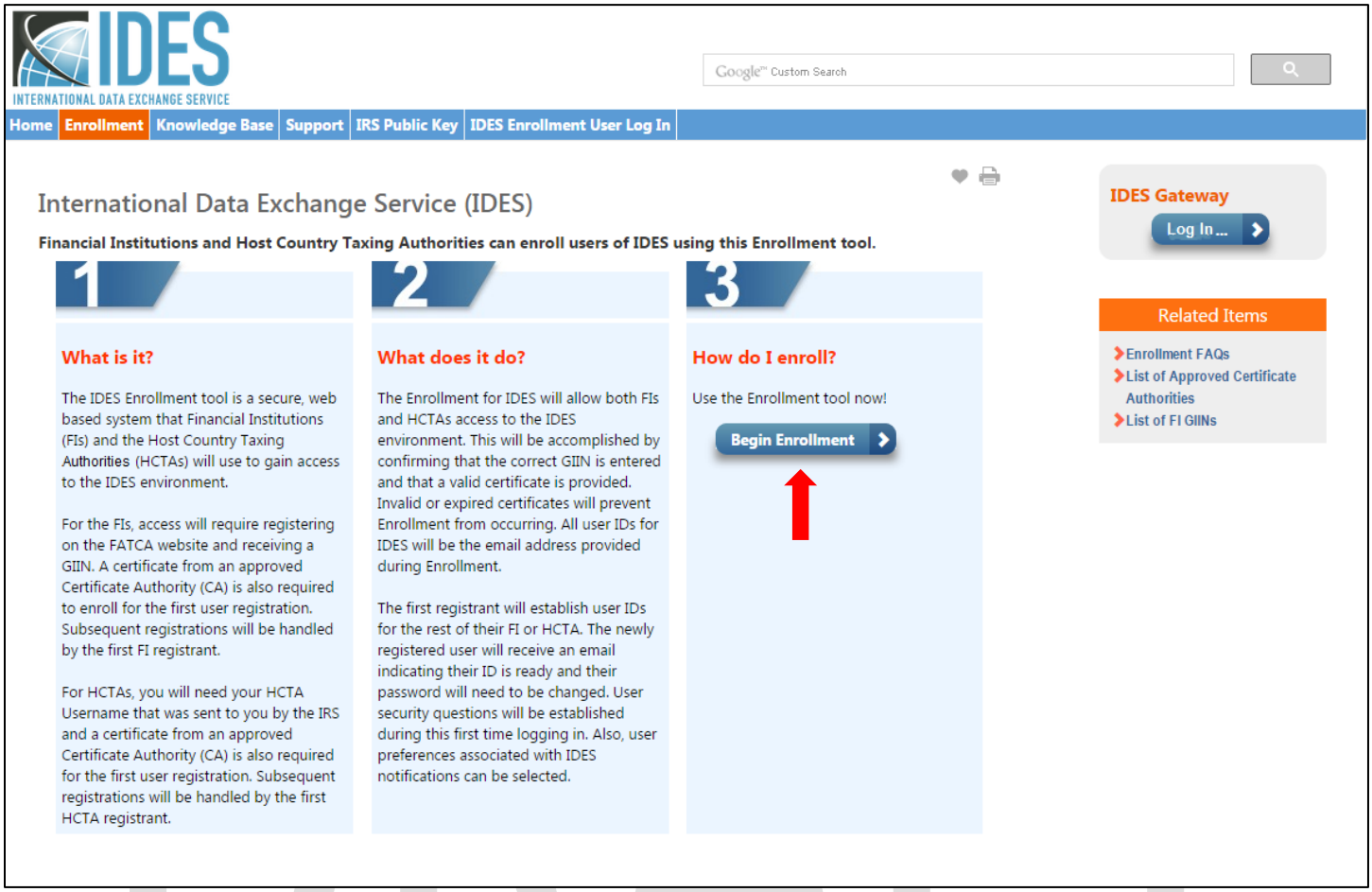


Figure 22 – Begin the enrollment process.

2. Click **Begin Enrollment** to start the enrollment process as an FI Administrator.

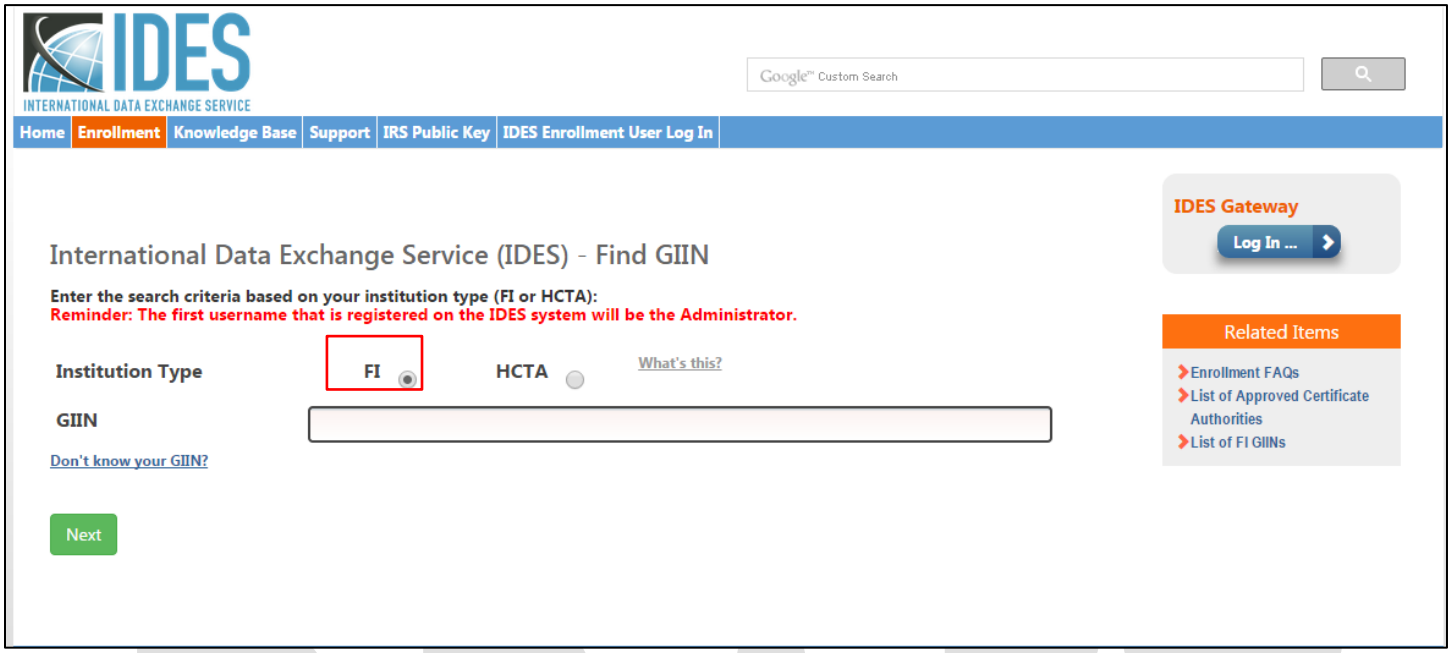


Figure 23 – Log in as an FI Administrator.

3. Select **Institution Type**, click **FI**.
4. **GIIN** – Enter the FI's GIIN in the 19-character format XXXXXX.XXXXX.XX.XXX.
5. Click **Next**.

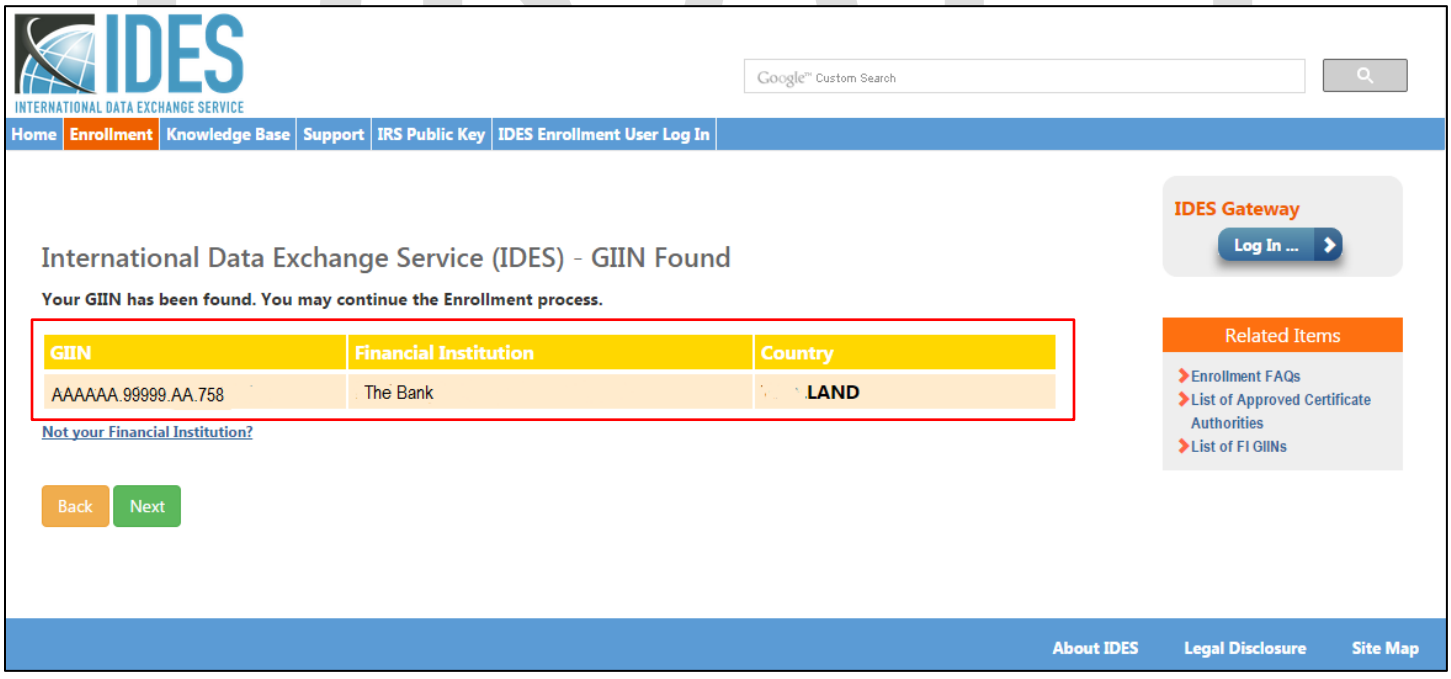


Figure 24 – IDES GIIN verification page

6. Confirm information and verify the **GIIN**, **Financial Institution** and **Country** are correct.
7. Click **Next** to continue and set up **Challenge Questions**.

DRAFT

6.3. Create Challenge Questions

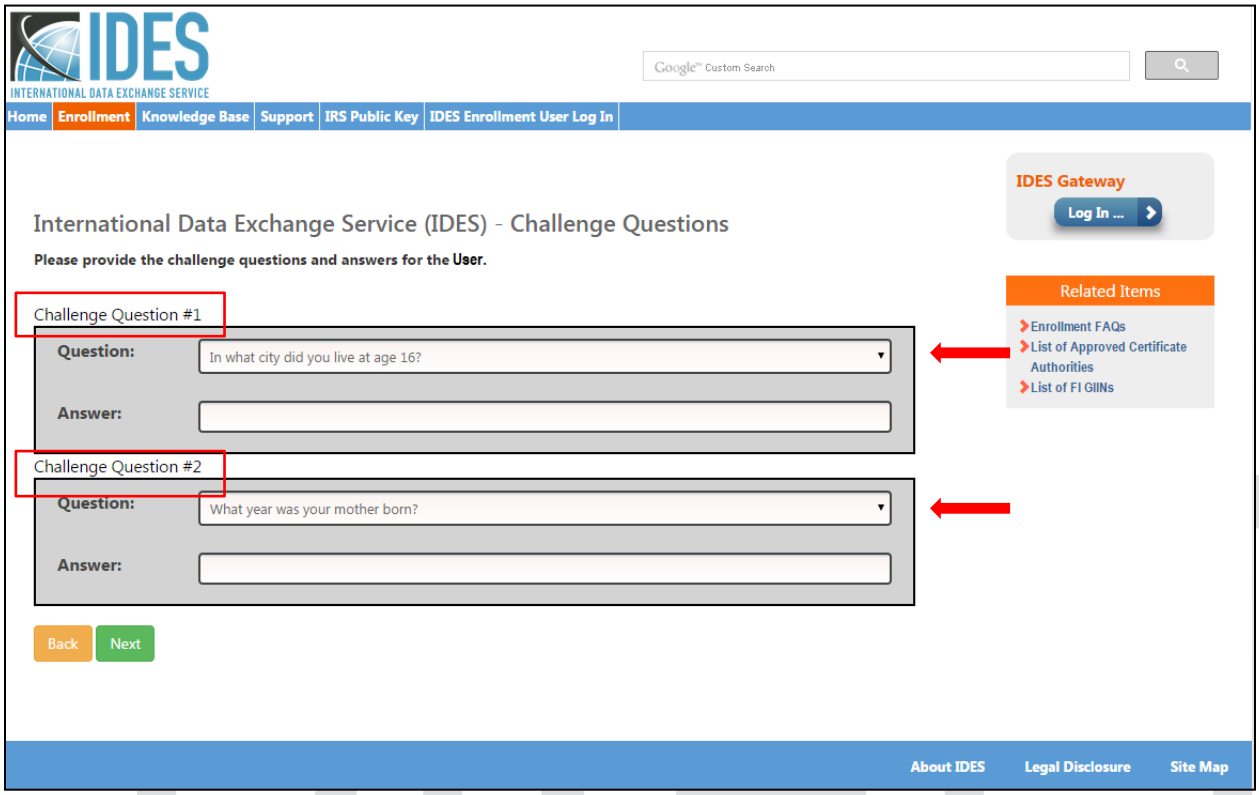


Figure 25 – Create IDES challenge questions.

1. **Challenge Question #1**
    a. **Question:** Select the drop-down arrow to view a list of questions. Select a challenge question.
    b. **Answer:** Type a response to the challenge question.
2. **Challenge Question #2**
    a. **Question:** Select the drop-down arrow to view a list of questions. Select a challenge question.
    b. **Answer:** Type a response to the challenge question.
3. Click **Next** to continue and set up a **Username**.

IMPORTANT: Remember to document answers to the challenge questions. Users will need these to reset a password or to contact the IDES Help Desk. Note that challenge question responses must exactly match the responses as originally submitted.

6.4. Create User Profile

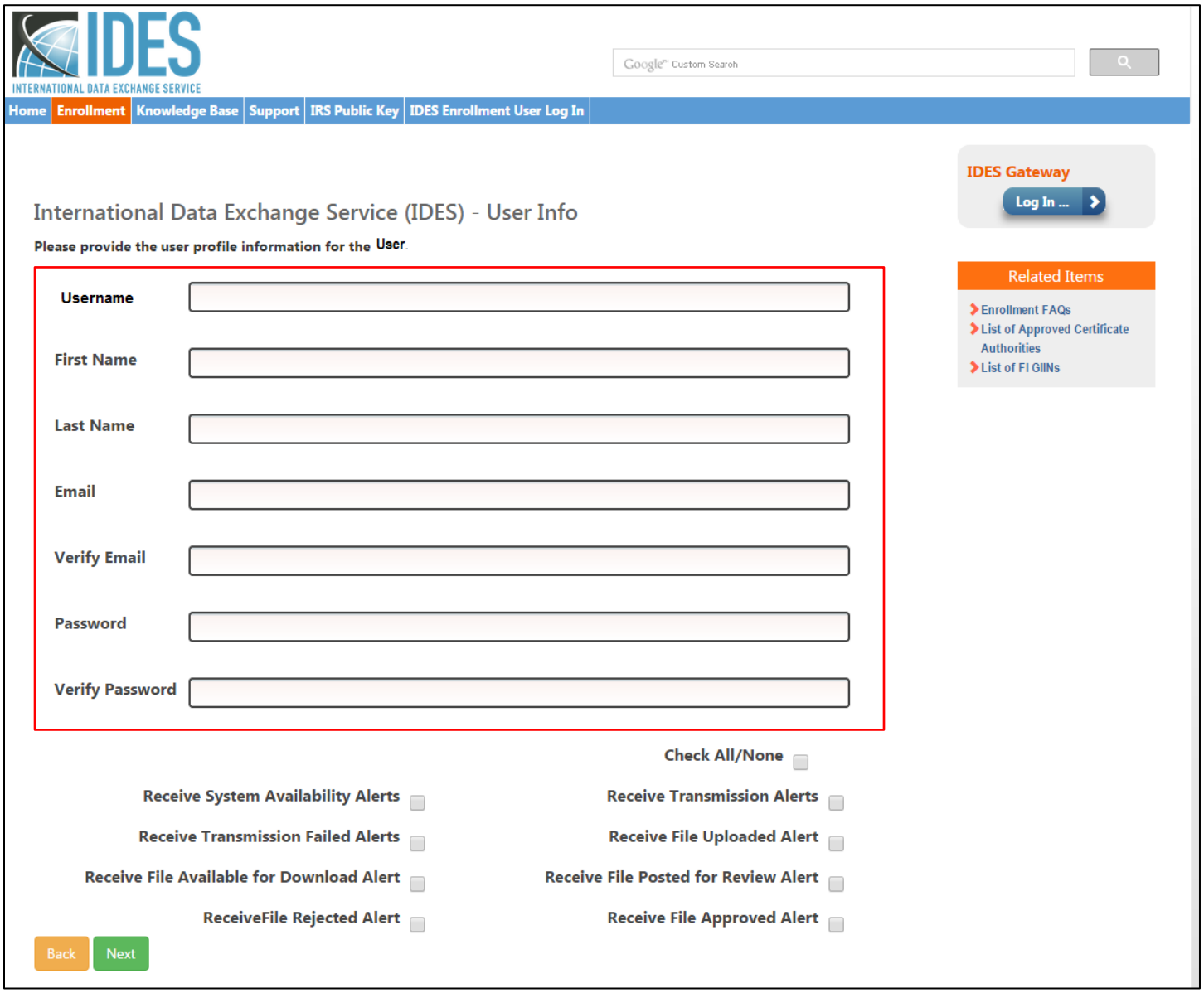


Figure 26 – Submit user profile information.

1. **Username** – Enter your new username. We recommend first initial and last name. If the username is already taken you will receive an error message.
2. **First Name** – Enter your first name.
3. **Last Name** – Enter your last name.
4. **Email** – Enter your email address.
    a. It is mandatory to use a unique email address for enrollment as the system will not allow for duplicate email addresses. The email address may be a personal email address or a shared mailbox address.
5. **Verify Email** – Enter your email address again (must match the previous entry). If it does not match, you will receive an error message.
6. **Password** – Create a valid password.
    a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .).
    b. If you enter a password that does not meet the guidelines, you will receive an error message.

7. **Verify Password** – Re-type your password (must match the previous entry). If it does not match, you will receive an error message.

6.5. Select Alert Preferences

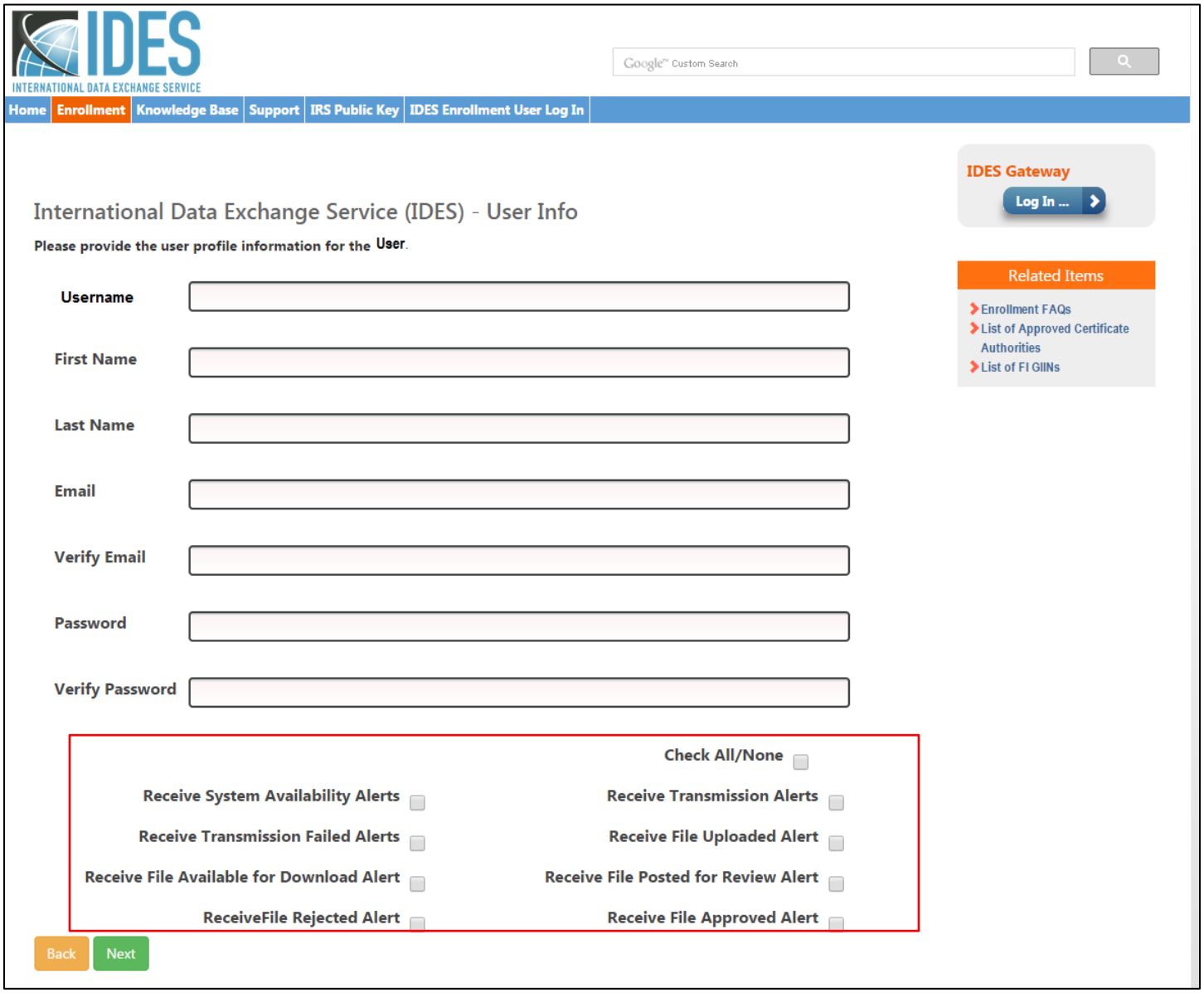


Figure 27 – Select IDES alert preferences.

1. **Select Alert Preferences** – Click on the box next to the alerts you wish to receive by email. You can click the **Check All/None** box to choose all alerts or to remove all alerts. There are eight Alert Preferences

Alert Preference	Description
a. System Availability Alert	IDES Enrollment and/or IDES Gateway are unavailable.
b. Transmission Failed Alert	Transmission uploaded via the IDES Gateway failed for one of several reasons (e.g., virus, encryption validation, naming convention, package content). The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission failed.
c. File Available for Download Alert	The user has a file to download on the IDES Gateway. This is not functional at this time.
d. File Rejected Alert (for Model 1 Option 2 countries)	Transmission upload was rejected by the HCTA. The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission was rejected.
e. Transmission Alert	Receive all IDES Alerts (See Alerts **b,c,d,f,g,h**).
f. File Uploaded Alert	Received transmission is uploaded to the IRS for review.
g. File Posted for Review Alert (for Model 1 Option 2 countries)	Sent to the HCTA when an FI uploads a report.
h. File Approved Alert (for Model 1 Option 2 countries)	Sent after HCTA has approved the FI file.

Table 7 – FI IDES Alert Preferences

2. Click **Next** to continue to upload digital certificate.

6.6. Upload Digital Certificate

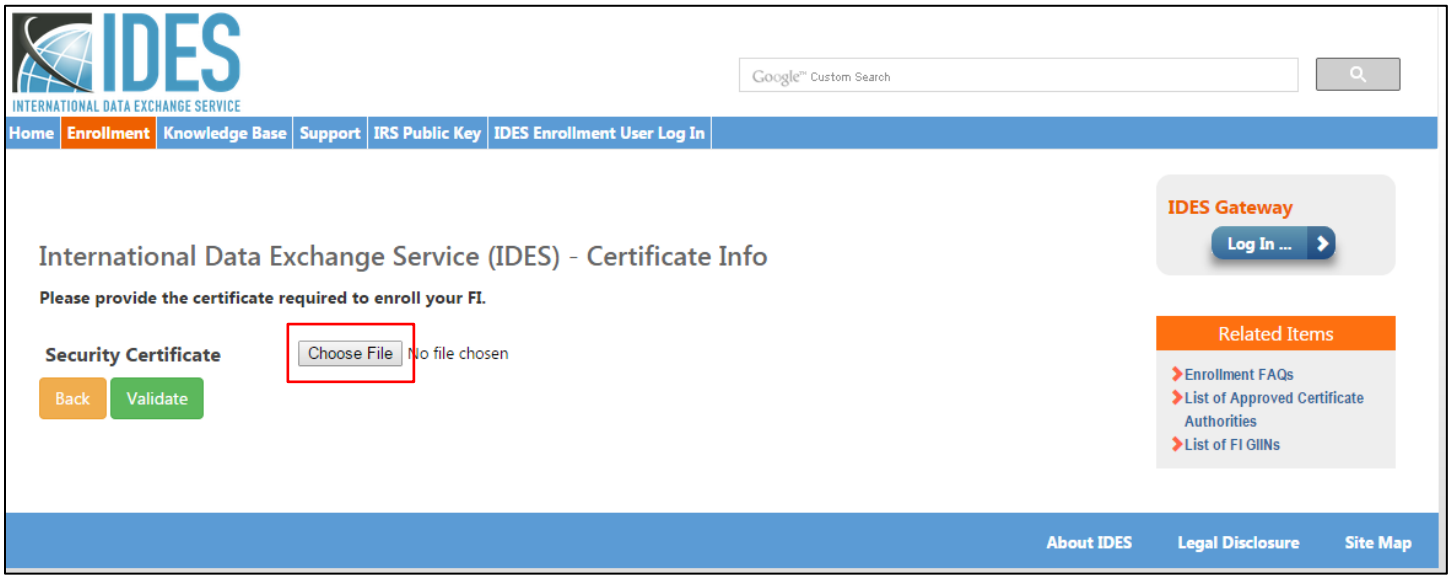


Figure 28 – Upload a digital certificate.

DRAFT

1. Click **Choose File** to search for the security certificate located on computer.

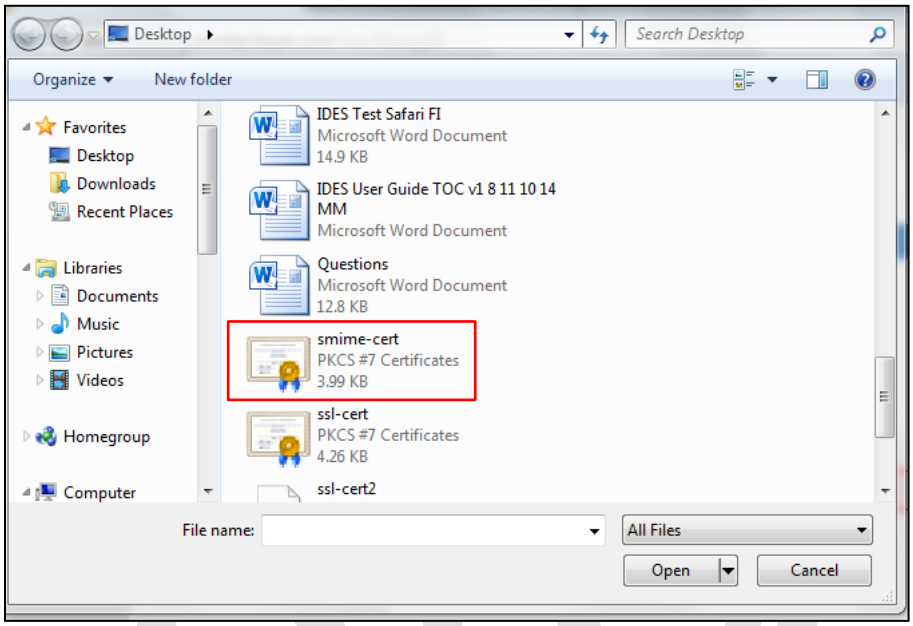


Figure 29 – Select a digital certificate.

2. Select the Active/Valid certificate file from your computer.
3. Click **Open.**
4. Click **Validate.**
    a. If you receive an error message, refer to Appendix C: Certificate Upload Error Messages or contact IDES customer support for assistance.

Important: Each entity should obtain a digital certificate issued by an approved CA. The digital certificates should be in a DER or PEM format.

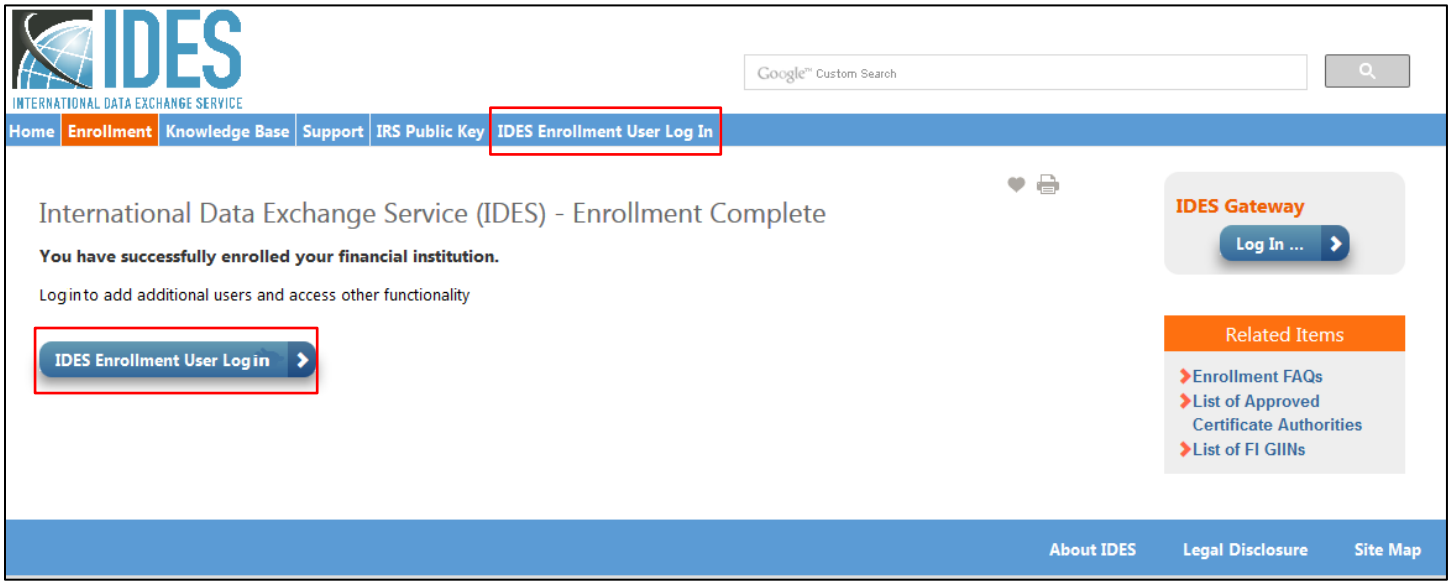


Figure 30 – Enrollment confirmed.

DRAFT

5. After you have validated your certificate, the enrollment process is complete. You will receive an email from the IDES help desk that verifies your authorization to access IDES Gateway.
6. Click **IDES Enrollment User Log In** to log in as the FI Administrator.

7. Existing Administrators (HCTA and FI)

HCTA and FI Administrators can add end users, disable and enable end users, update the certificate, update alert preferences, create a metadata file, reset passwords, and download the IRS public key.

7.1. Add a User

End users added under FI and HCTA Administrator accounts are able to perform the following functions:

- Create a Metadata File.
- Update Alert Notifications.
- Reset Password.
- Download the IRS Public Key.

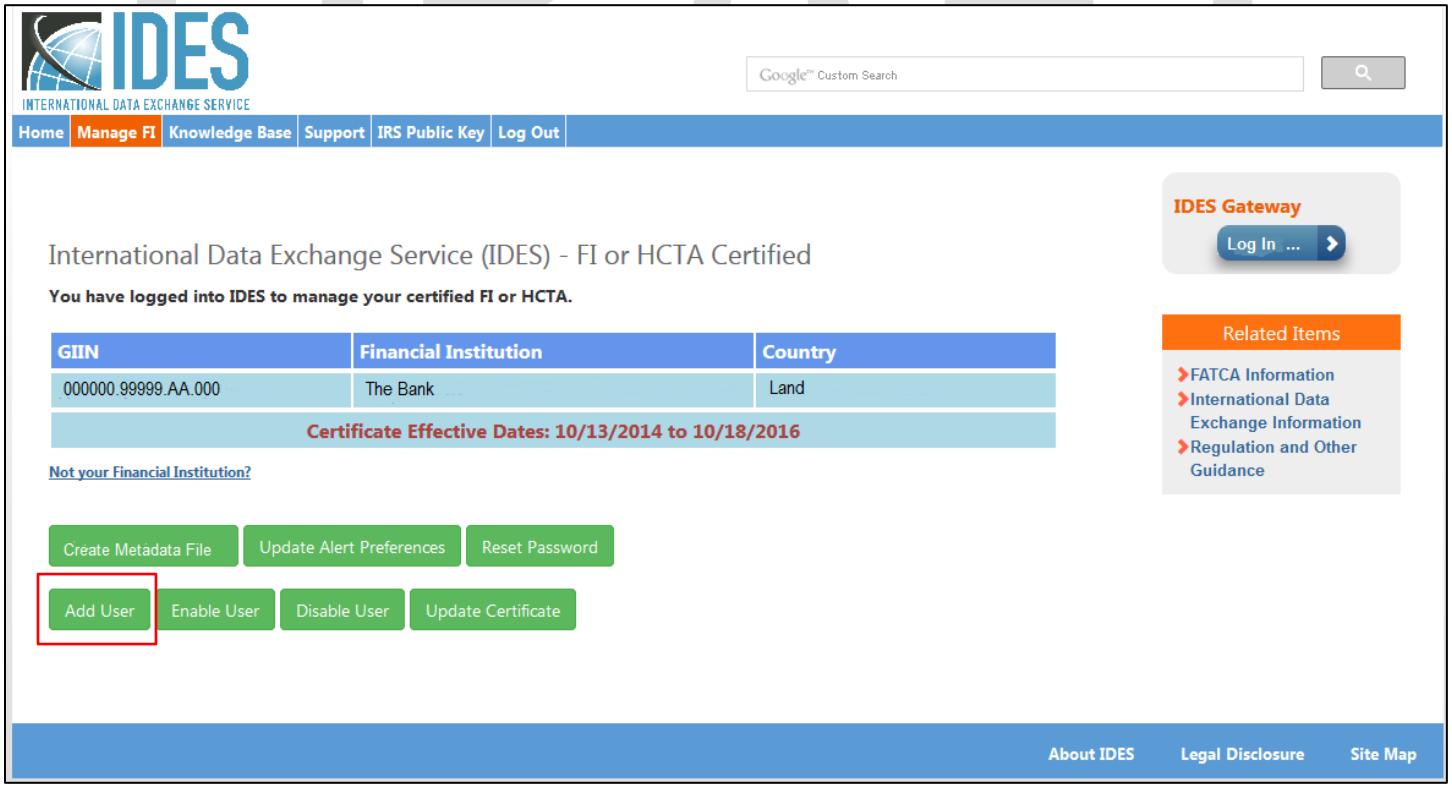


Figure 31 – Add an end user.

1. Click **Add User.**

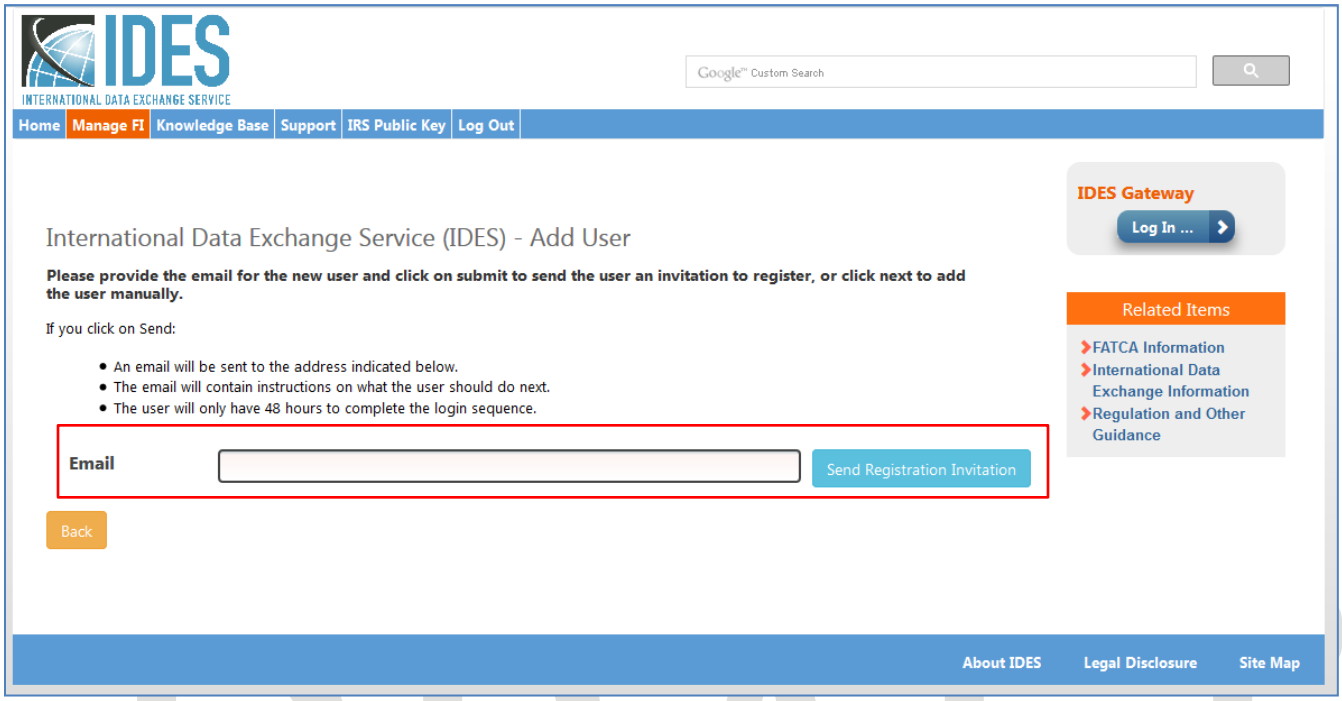


Figure 32 – Send an enrollment invitation.

2. **Email** - Type in email address of new end user.
3. Click **Send Enrollment Invitation**.

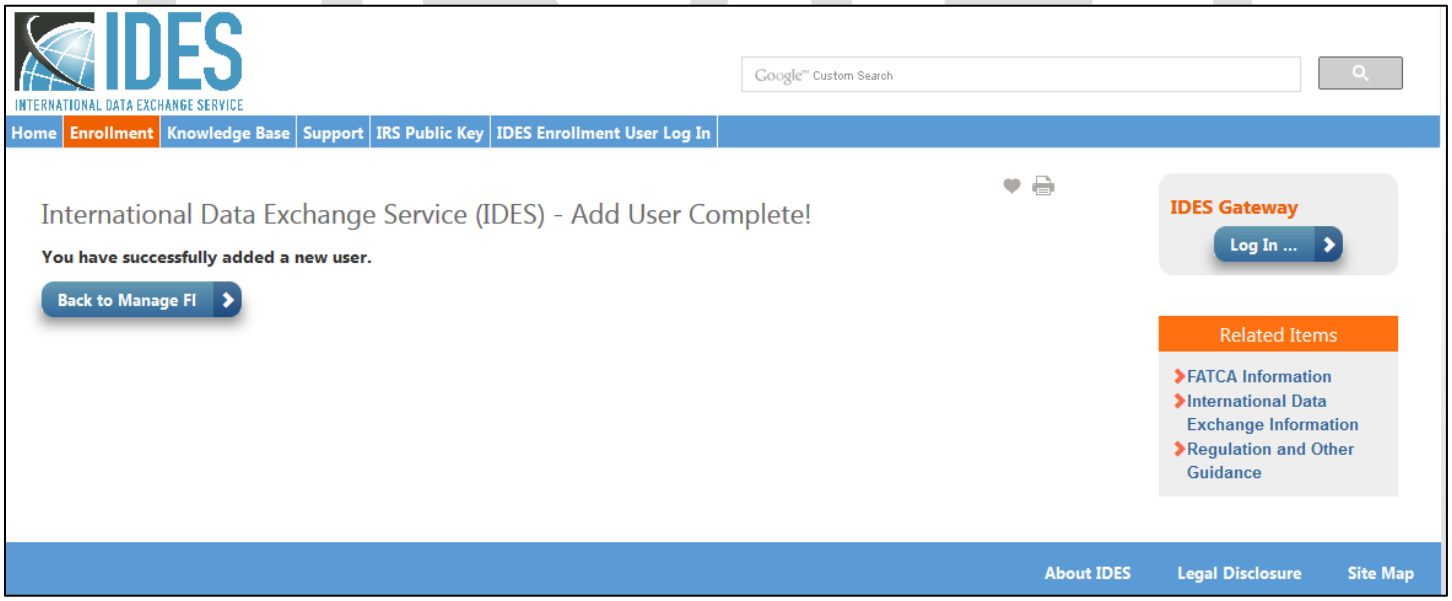


Figure 33 – New user added.

4. The new end user will receive an email to register. The link in the email is valid for 48 hours.
5. Confirmation of End User **Enrollment Invitation** email has been sent.

Welcome to International Data Exchange Service! Your corporate administrator has registered you as an authorized user.

To log in to International Data Exchange Service (IDES), complete the following steps:

1. Click on this link to enroll in IDES.
2. Create password challenge questions. Challenge questions will be used to prompt you if you forget your password. By correctly responding to the challenge questions, you can reset your password without contacting the IDES help desk.
3. Create your IDES user name and password.

SHARING USER IDs AND PASSWORDS IS NOT ALLOWED. If you have additional people who will use IDES, they must obtain their own user IDs. You are responsible for any activity associated with your user ID, so do not share your password with anyone, including the IDES help desk.

Need help?

If you need help using IDES or have questions about IDES policies, please contact IDES Customer Support by phone at 1-800-613-IDES (4773) or by email at helpdesk@ides-support.com. IDES Customer Support is available 24 hours a day except on U.S. federal holidays .

Additionally, the IDES team is always interested in improving our service. Please contact us through IDES Customer Support with suggestions on how to make IDES work better for you.

We are excited that you have joined IDES and we are committed to helping your organization.

Regards,
The IDES Team

Figure 34 – IDES welcome email.

6. The new end user will receive a copy of the above email. If the end user does not receive this email, contact IDES customer support for assistance.

7.2. Disable a User

Administrators can disable an end user at any time. Administrators are not authorized to delete accounts, but disabling an end user account will prevent the end user from accessing their IDES account. Administrators may enable this end user at a later date.

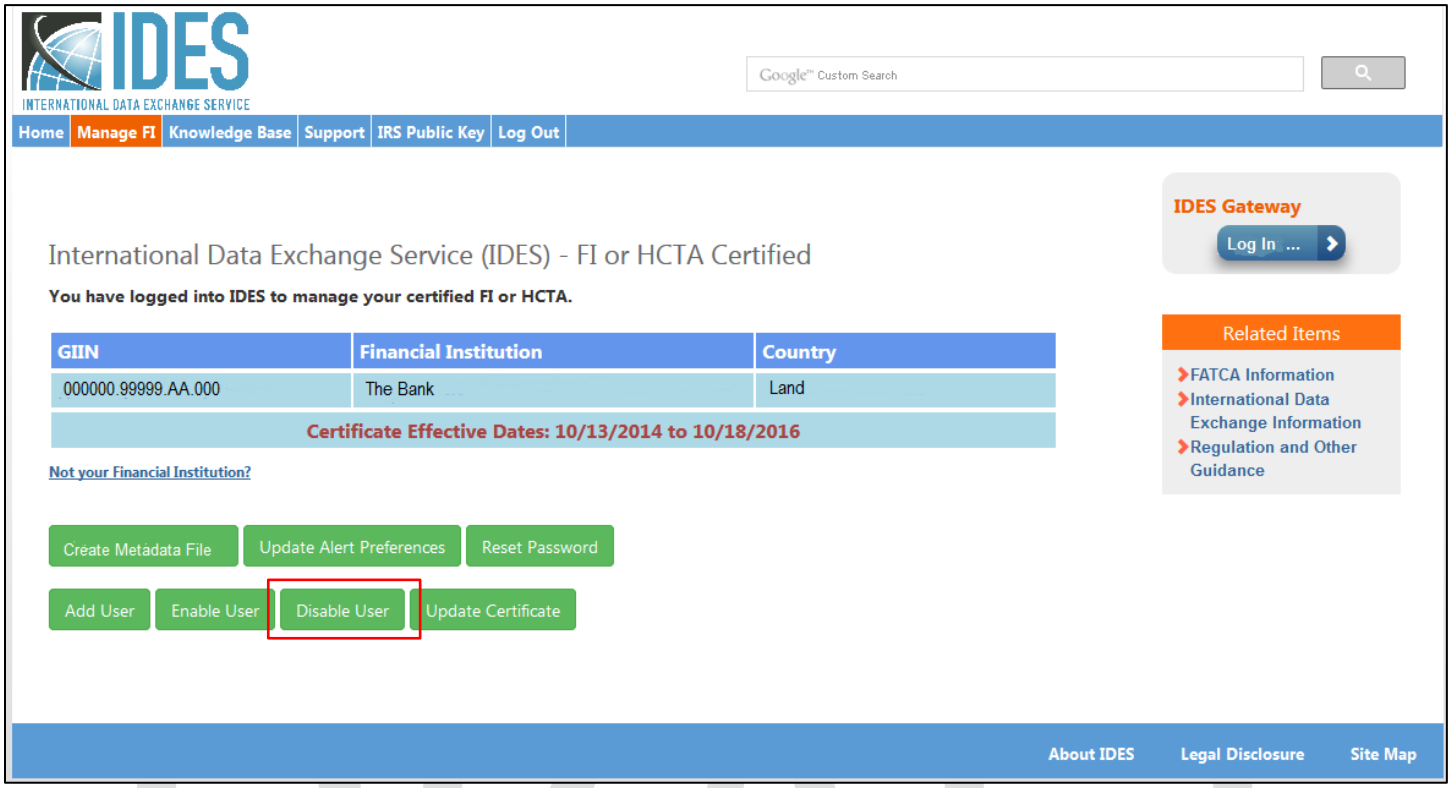


Figure 35 – Disable a user.

1. Click **Disable User**.

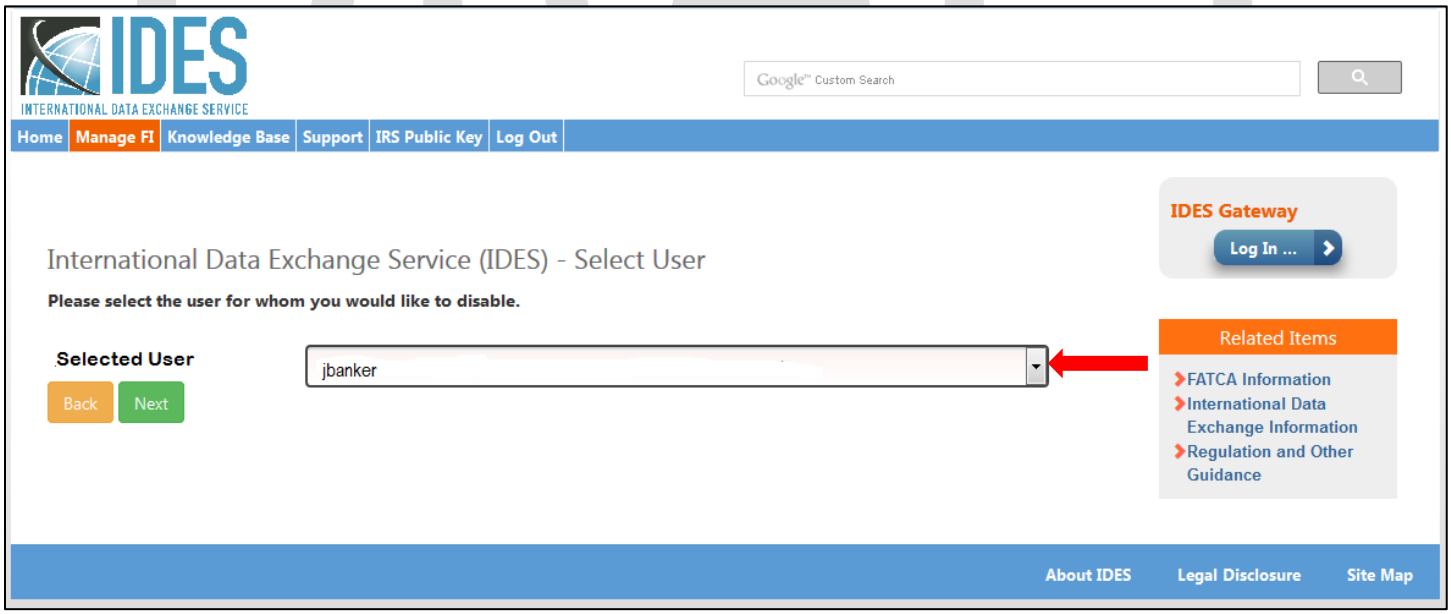


Figure 36 – Select a user to disable.

2. **Selected User** – Select the end user that you want to disable from the drop down box by clicking the arrow.
3. Click **Next**.

DRAFT

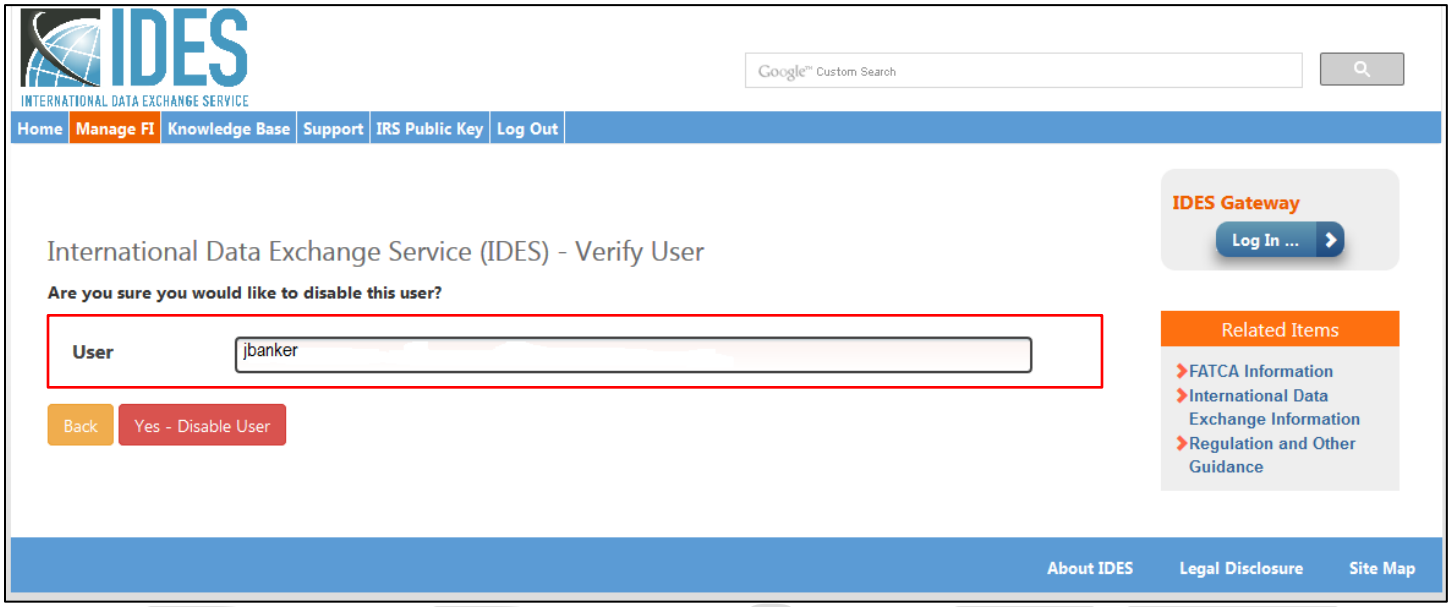


Figure 37 – Verify user to disable.

4. **User** – Verify that you have selected the correct username.
5. Click **Yes – Disable User**.

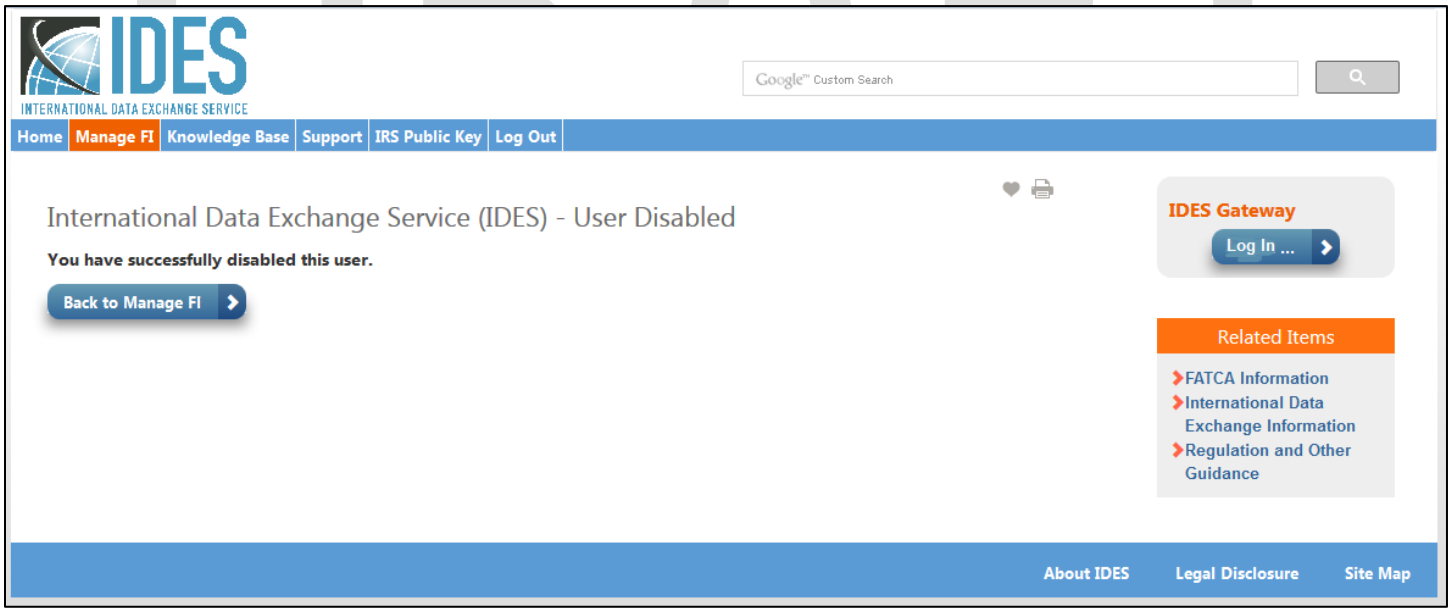


Figure 38 – User disabled confirmation.

6. Receive confirmation that the end user has been disabled.

DRAFT

7.3. Enable a User

Administrators can only use the Enable User option to enable end users that were previously disabled. To add a new end user, administrators must follow the process for Add a User.

After the Administrator has enabled the end user, the account and previous password will be active again. If the end user does not remember his or her password, the Administrator can reset the password or the end user can follow the Forgot Password process.

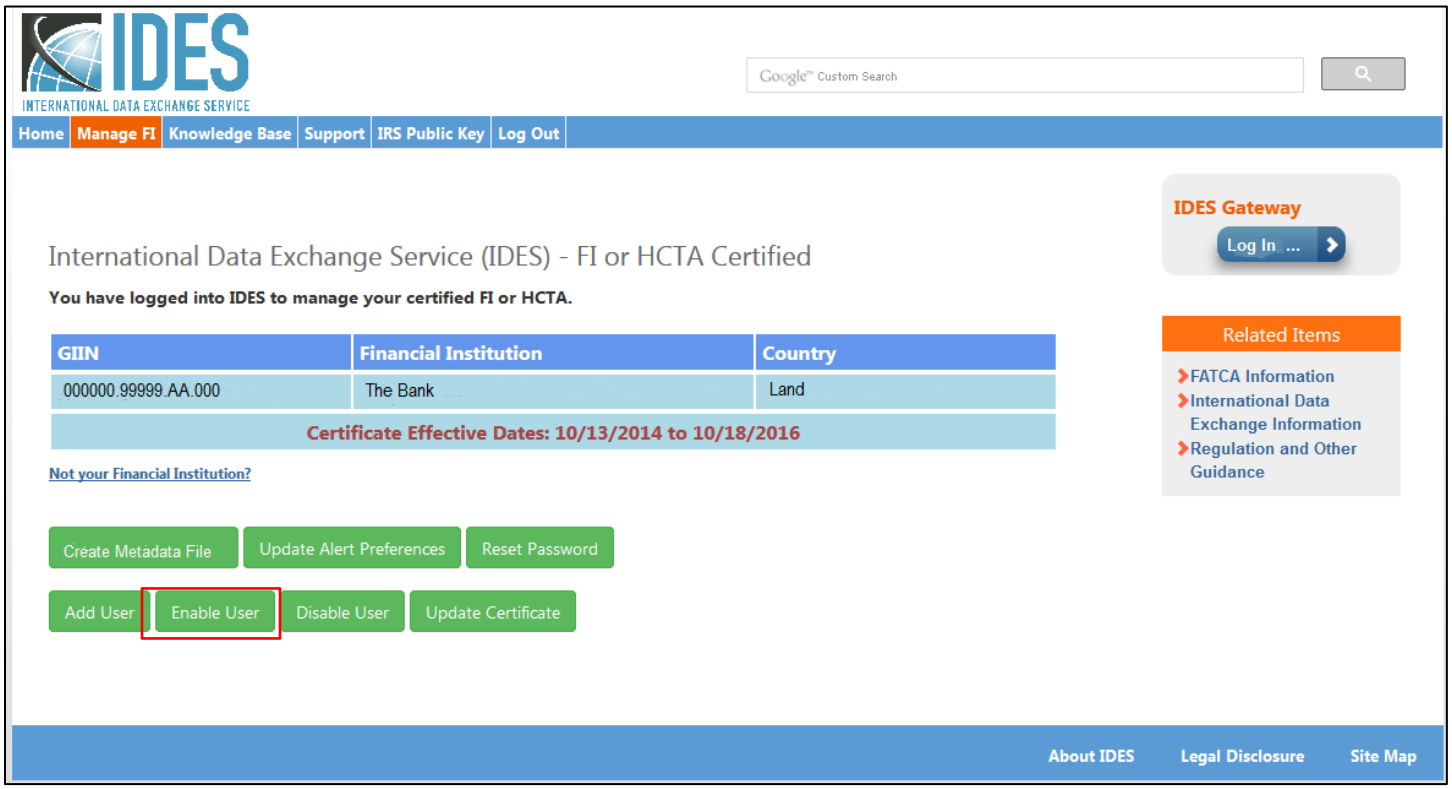


Figure 39 – Enable a user.

1. Click **Enable User.**

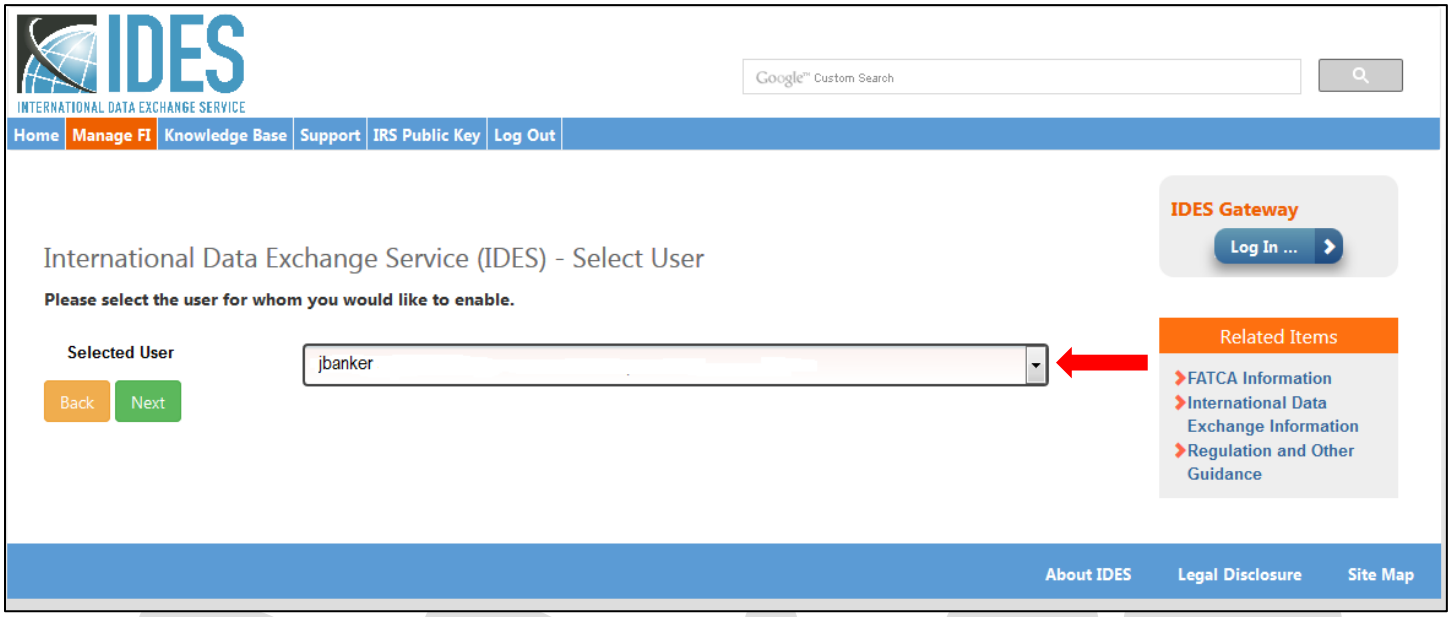


Figure 40 – Select a user to enable.

2. **Selected User** – Select the end user that you want to enable from the drop down box by clicking the arrow.
3. Click **Next** to confirm.

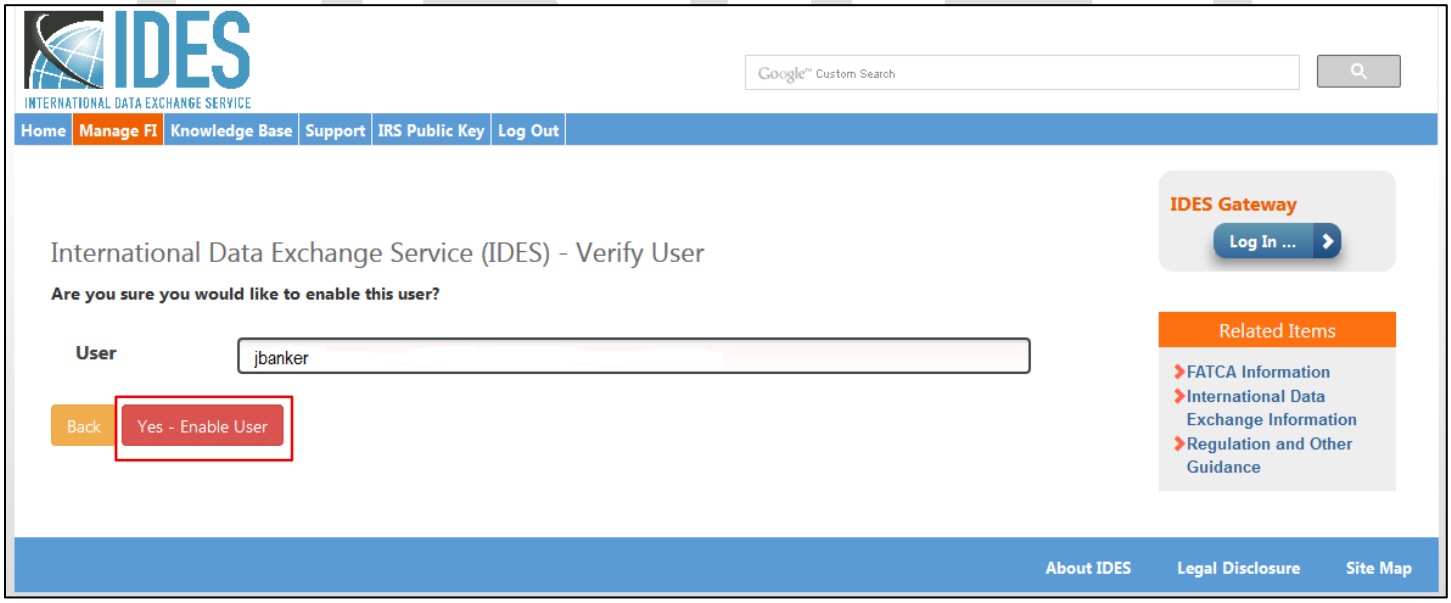


Figure 41 – Verify the user to enable.

4. **User** – Verify the user to enable.
5. Click **Yes – Enable User**.

DRAFT

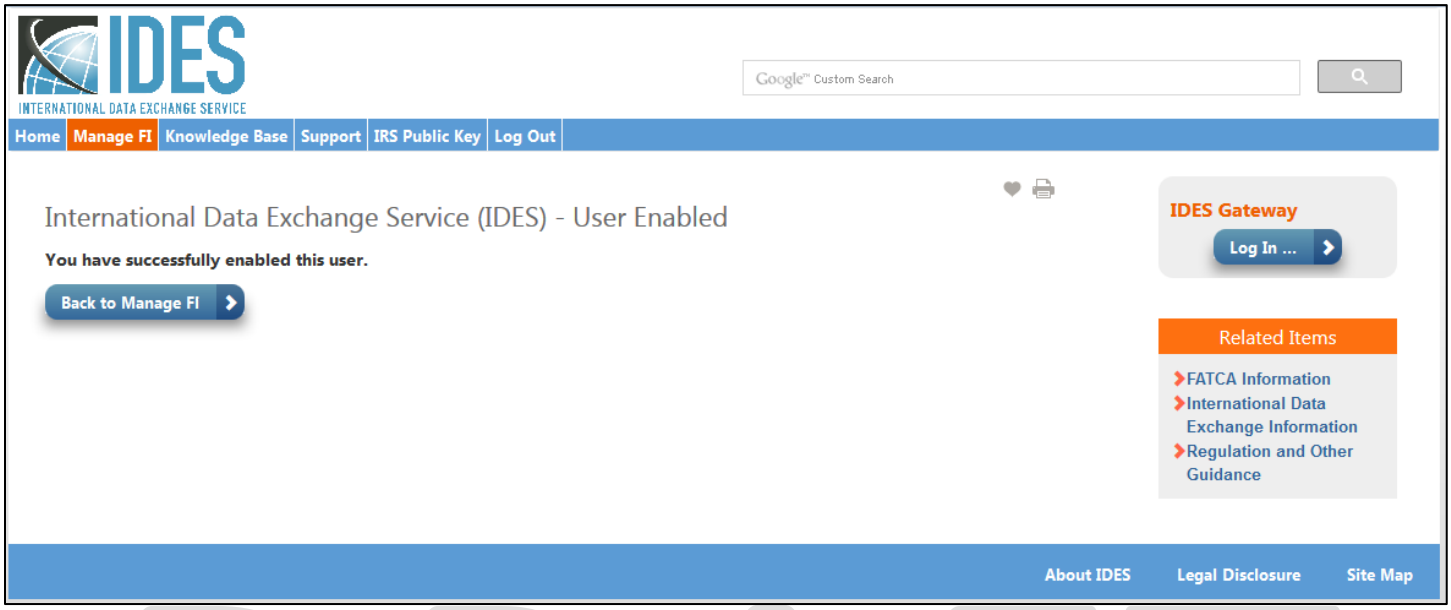


Figure 42 –User enabled confirmation.

6. Receive confirmation that the end user has been enabled.

DRAFT

7.4. Update the Certificate

Administrators will need to update invalid or expired certificates.

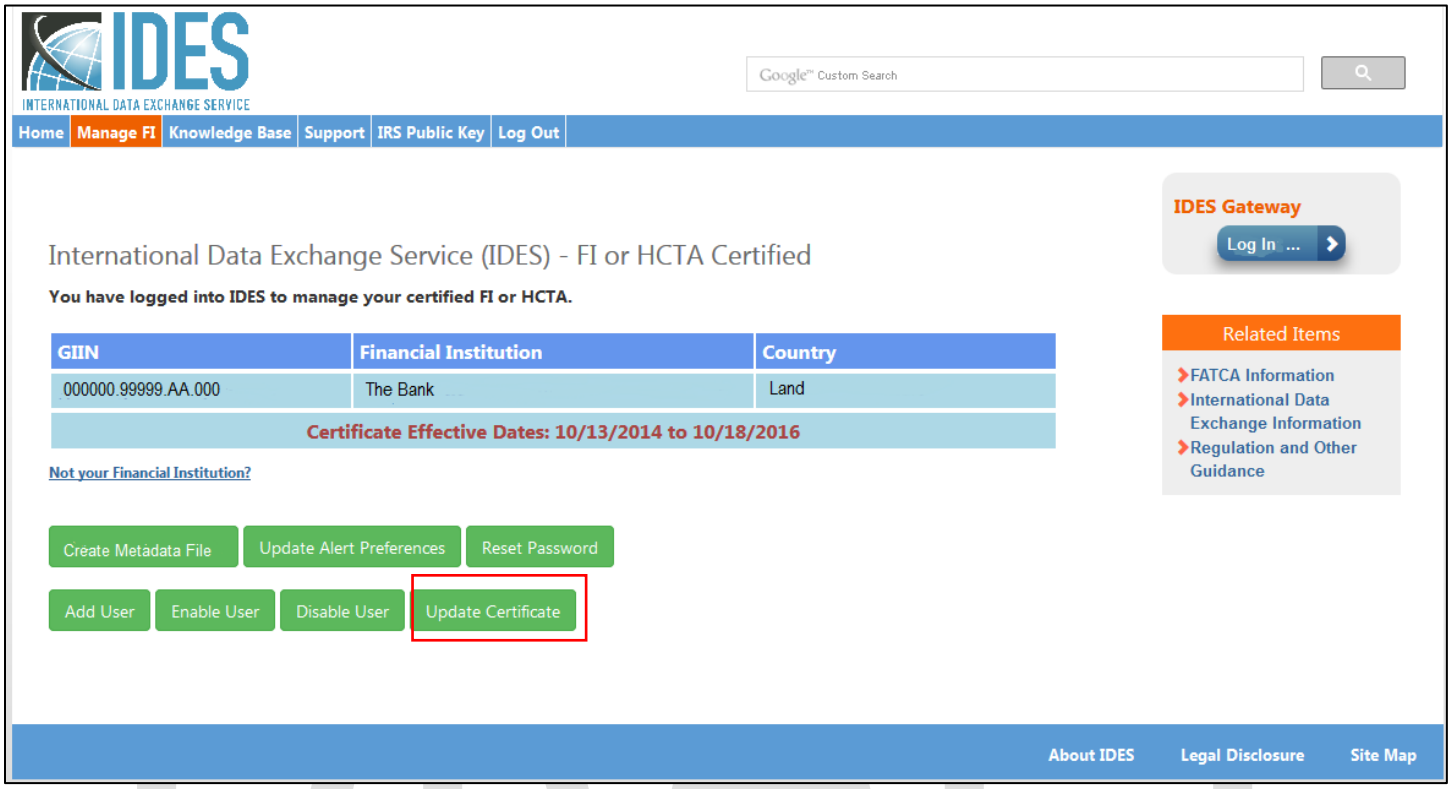


Figure 43 – Update a user certificate.

1. Click on **Update Certificate.**

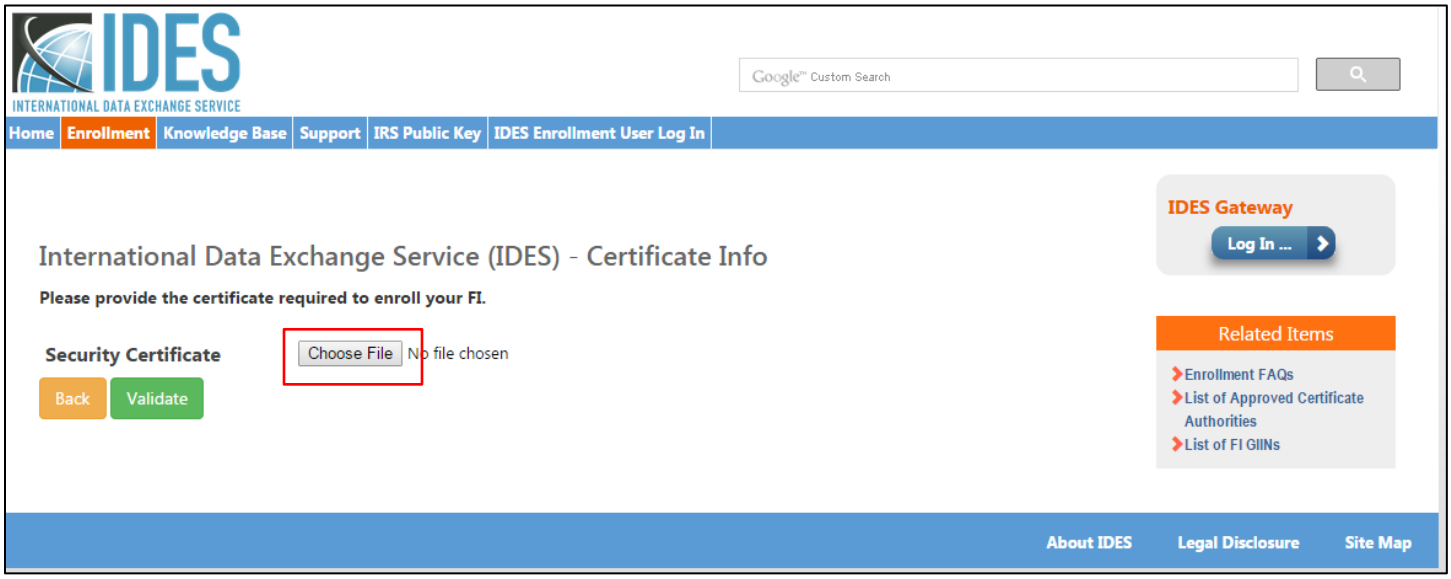


Figure 44 – Upload a digital certificate.

2. Click **Choose File** to upload the new certificate from your computer.

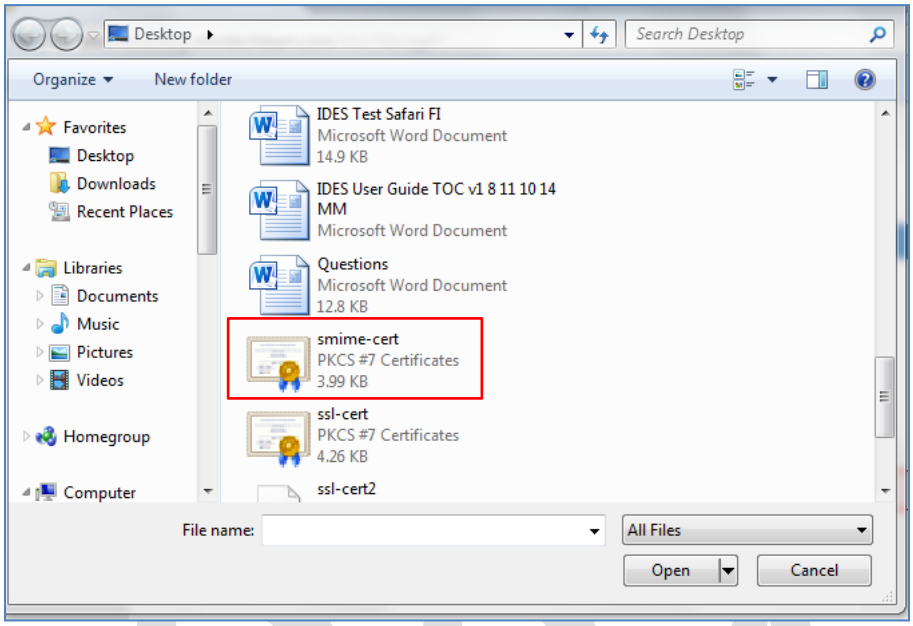


Figure 45 – Select a digital certificate.

3. Click on the certificate file then click **Open** to load the file.

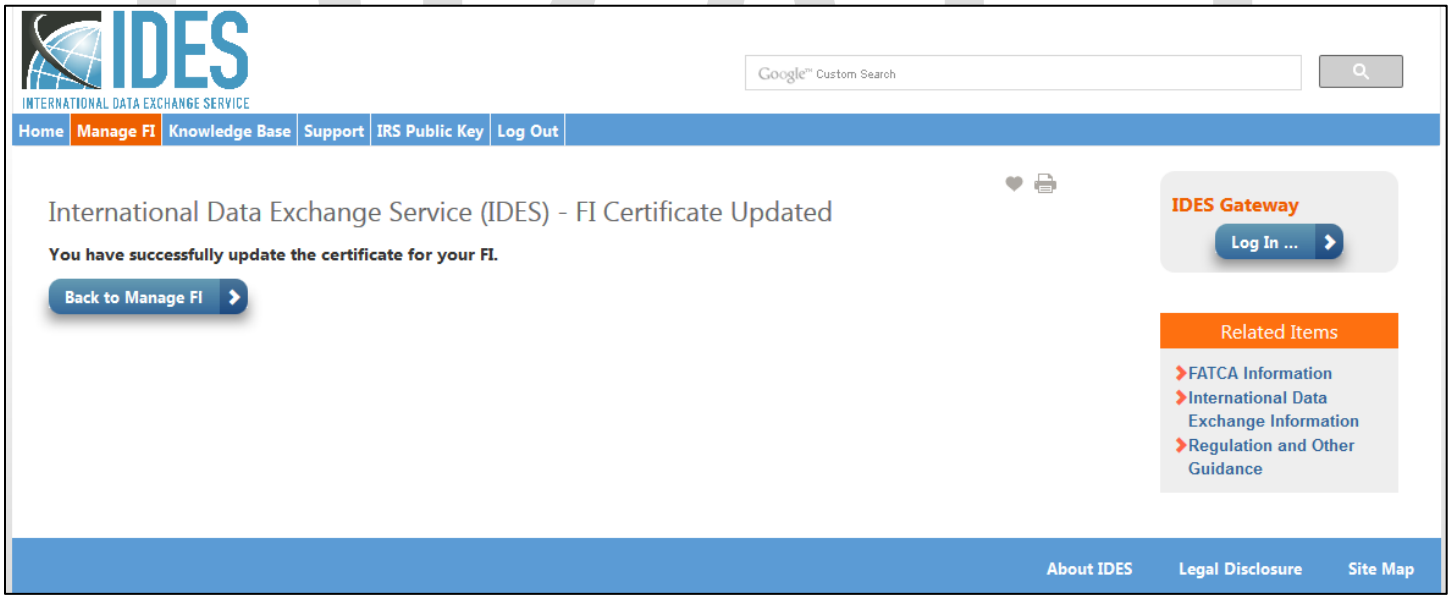


Figure 46 –Updated digital certificate confirmation.

4. Click **Validate** to complete the upload of the new certificate. If you receive a certificate error message, refer to Appendix C: Certificate Upload Error Messages for a complete list or contact IDES customer support.
5. Review confirmation screen of successful certificate update.

7.5. Update Alert Preferences

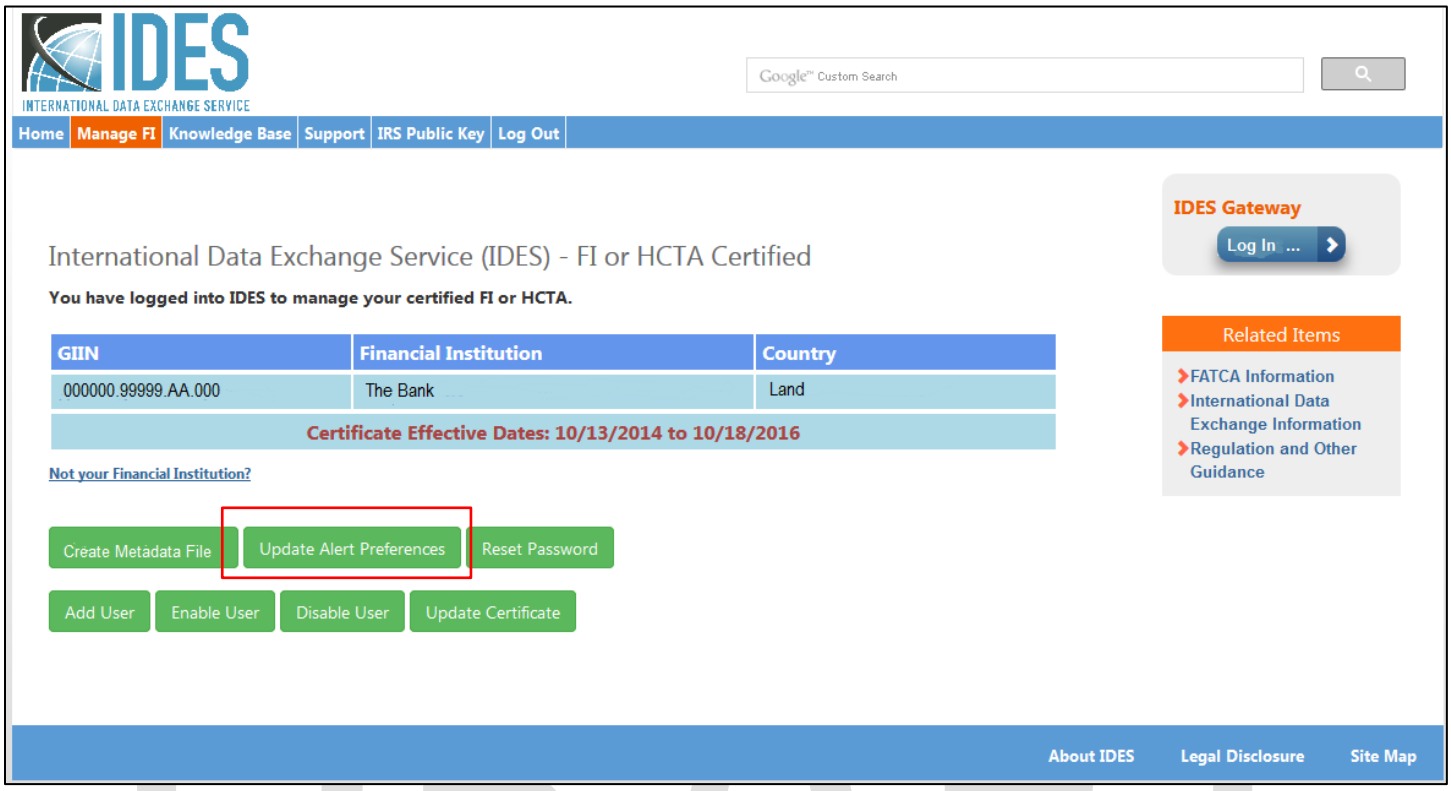


Figure 47 – Update alert preferences.

1. Click **Update Alert Preferences.**

DRAFT

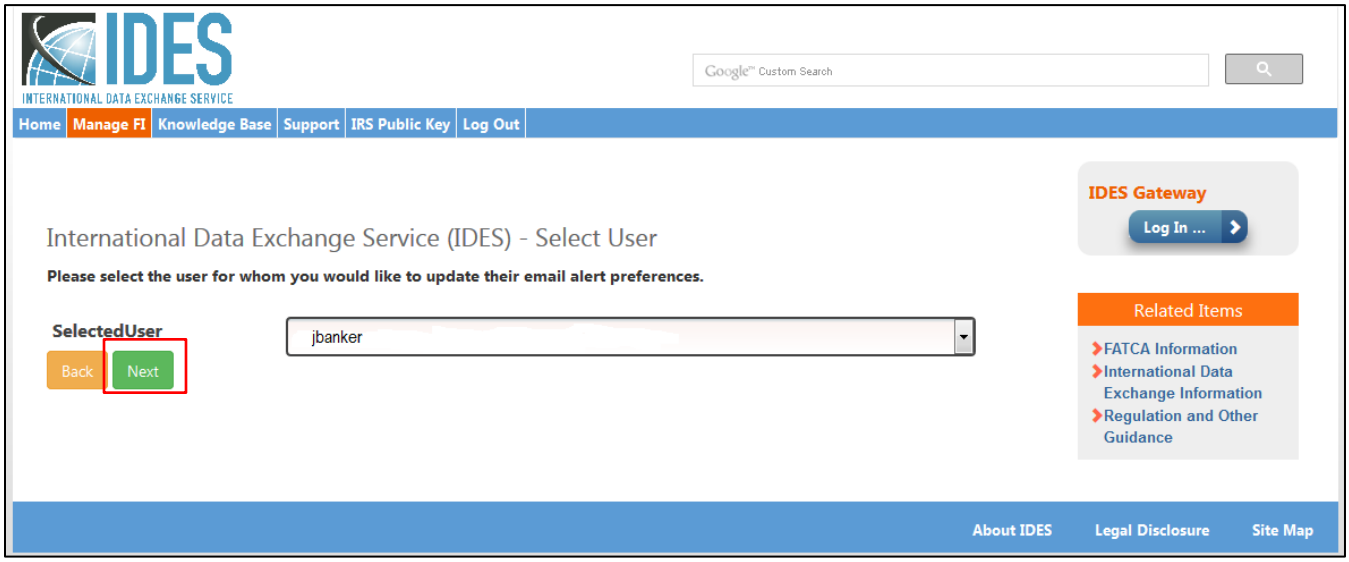


Figure 48 – Select the user profile to update.

DRAFT

2. **Select User** – Select the User to update their email alert preferences.
3. Click **Next.**

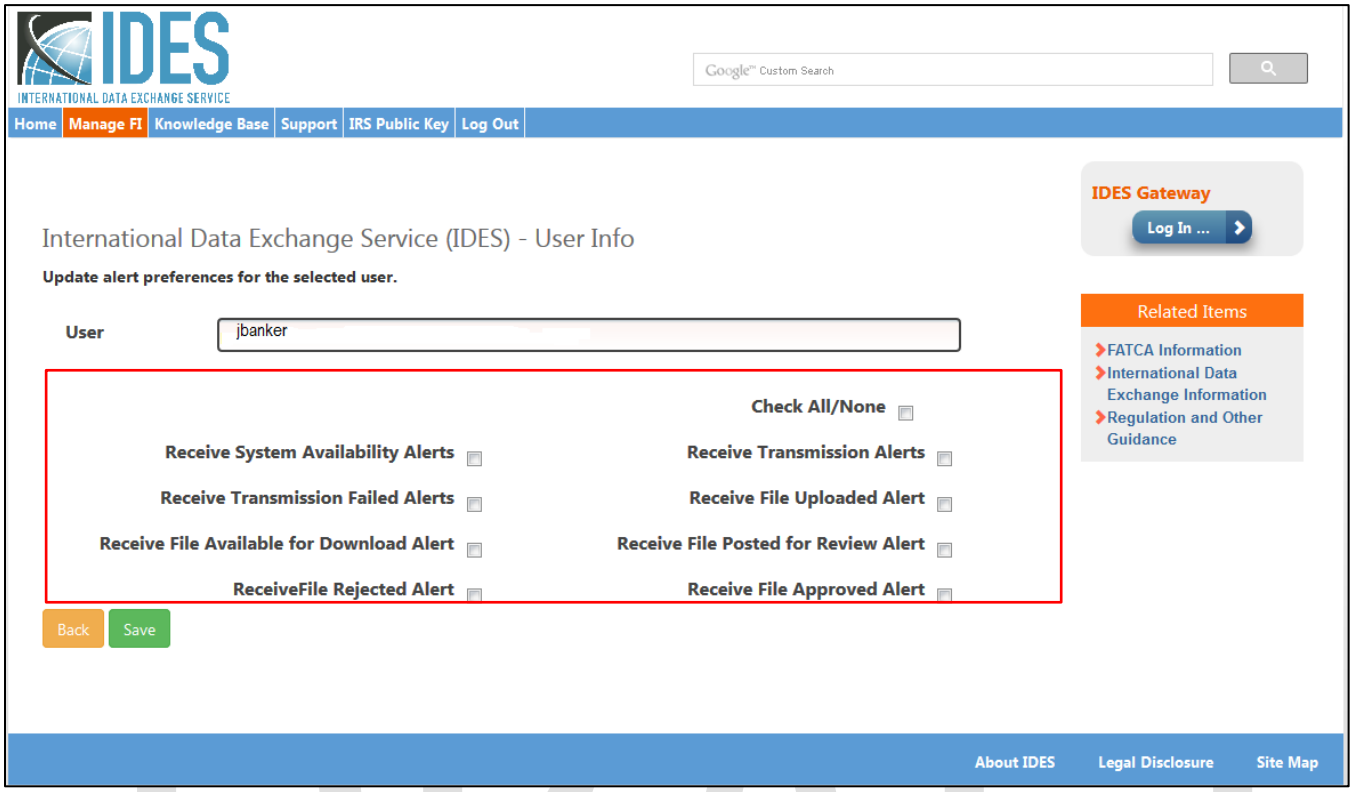


Figure 49 – Select new alert preferences.

4. **User** – Verify the username whose alert preferences are being updated.
5. Click on the checkbox next to the Alert(s) to receive via email. You can click the **Check All/None** box to choose all alerts or to remove all alerts. There are eight Alert Preferences. Refer to Select Alert Preferences for full instructions.
6. Click **Save**.

7.6. Create a Metadata File

Metadata is a collection of data about the content and characteristics of the FATCA reporting files. It is used to ensure the transmission archives are correctly processed. The metadata file will be included in the transmission archive and may also be created during the data preparation phase. HCTAs and FIs should create and validate metadata files using the FATCA IDES Metadata XML Schema v1.0.

DRAFT

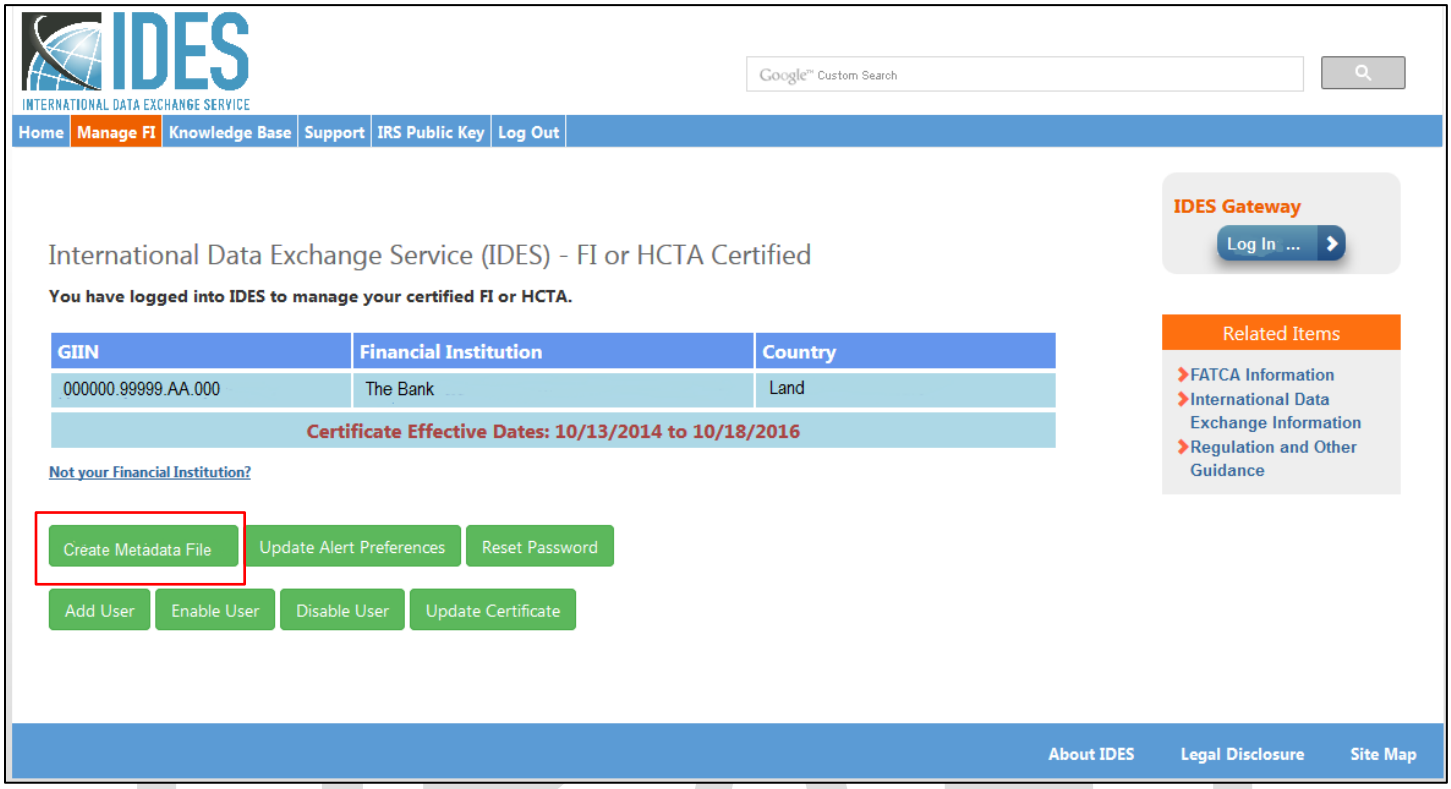


Figure 50 – Create a Metadata File.

1. Click **Create Metadata File.**

DRAFT

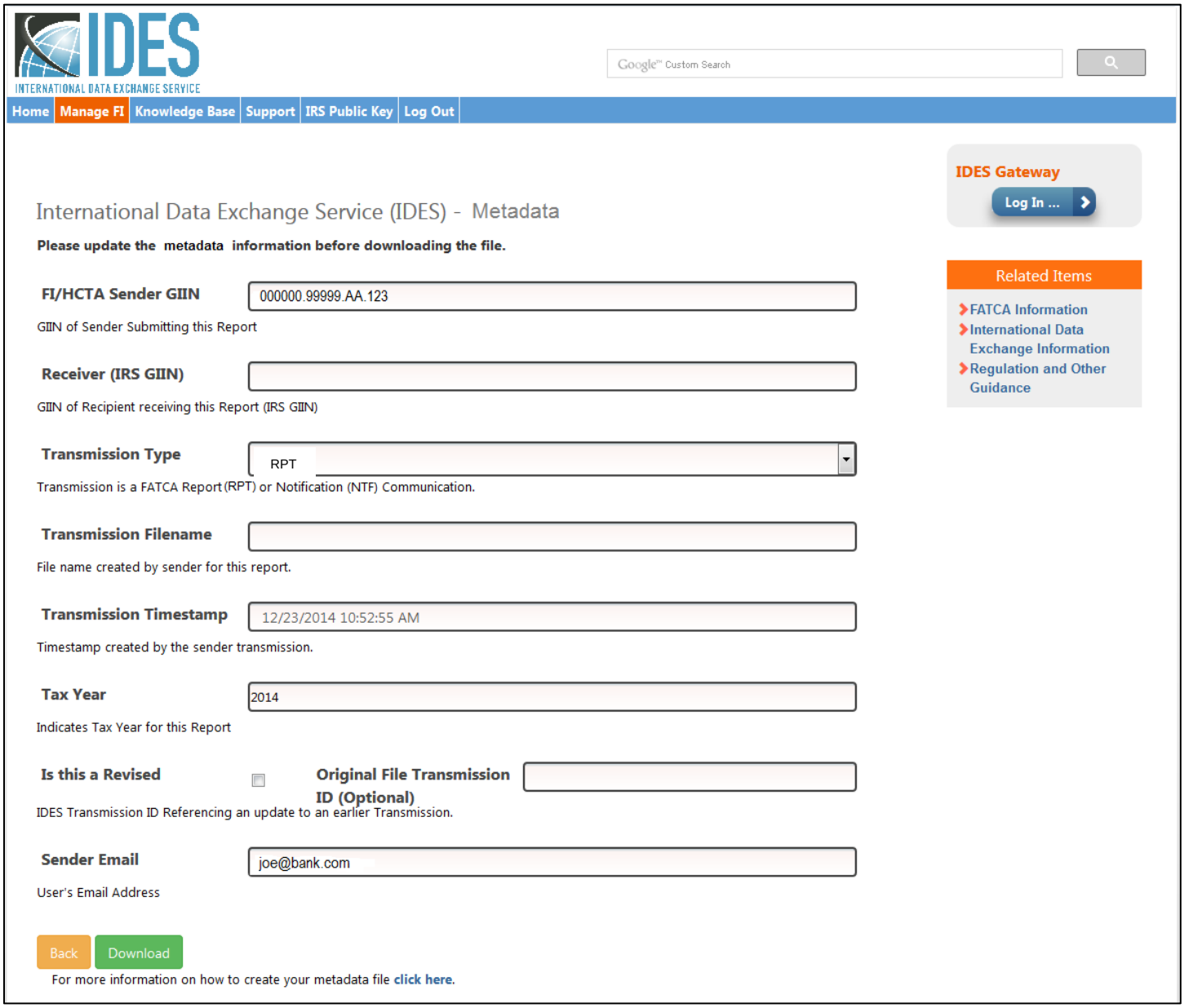


Figure 51 – Enter Metadata File information.

2. **FI/HCTA Sender GIIN** – Enter the FATCAIDESSenderId.
3. **Receiver (IRS) GIIN** – Enter the FATCAEntityReceiverId or recipient receiving the data.
    a. For example, the U.S. HCTA FATCA Entity ID: 000000.00000.TA.840
4. **Transmission Type** – Select the transmission type:
    a. RPT = FATCA Report Communication
    b. NTF = FATCA Notification Communication **(Not used)**
5. **Transmission Filename –** Enter the SenderFileId or file name of the file being uploaded.
6. **Transmission Timestamp –** Reference the timestamp created by the sender transmission.
7. **Tax Year –** Enter the FATCA reporting data tax year.
8. **Is This a Revised –** Select checkbox if the report is a revision to a previously uploaded file.
9. **Original File Transmission ID (Optional) –** Enter the file name of the original file.
10. **Sender Email (Optional) –** Enter your email address.
11. Click **Download** and review the metadata elements. The metadata file should be validated against the FATCA Metadata XML Schema v1.0.

12. Save the file on your computer. The unencrypted metadata file must be included in the transmission archive and the filename is FATCAEntitySenderId_Metadata.xml. The file names are case sensitive and any variation in name, extension or format will cause a transmission failure. See Create a FATCA XML Report for more details.

.

7.7. Reset Password

FI and HCTA Administrators can reset the passwords of all end users under the administrator account.

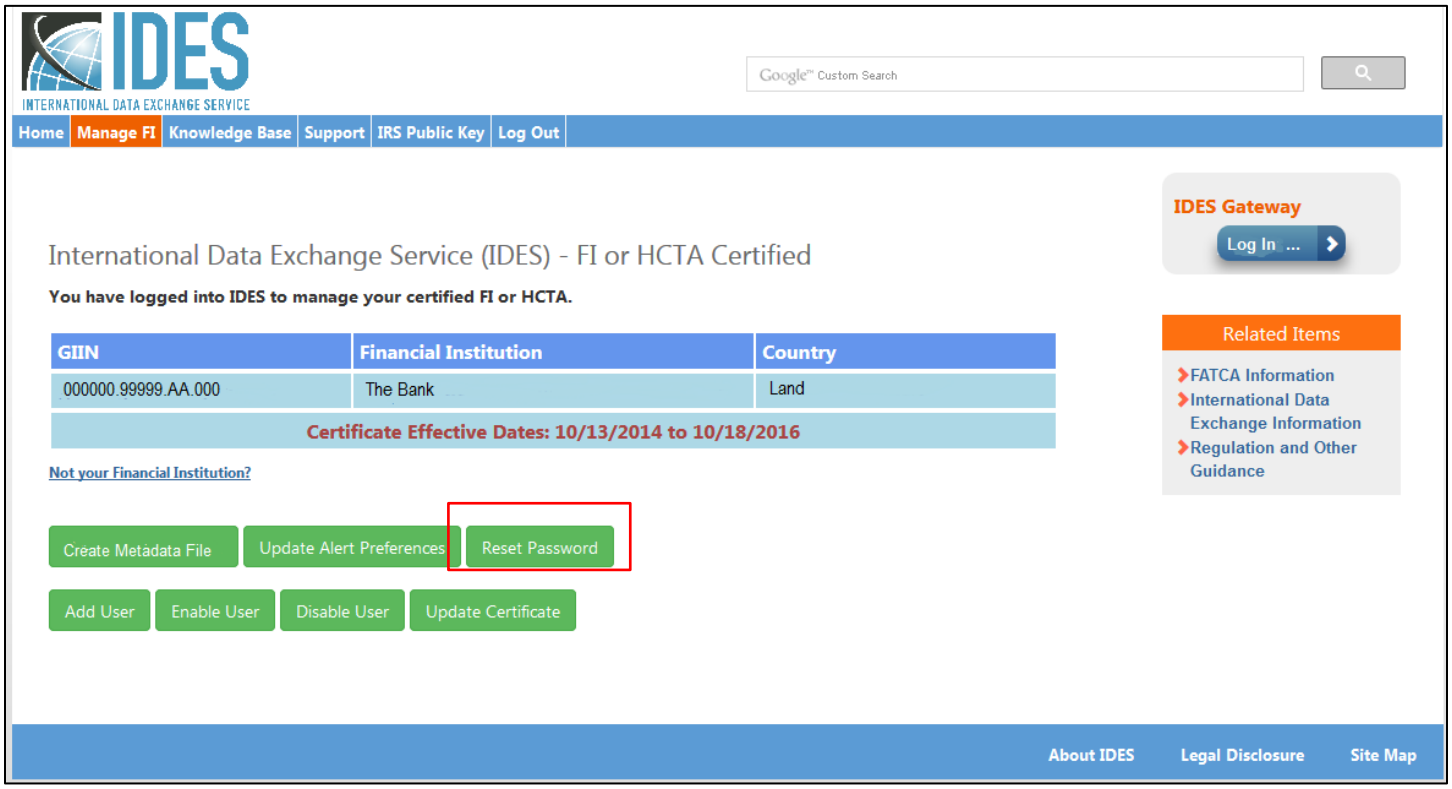


Figure 52 – Reset a password.

1. Click **Reset Password.**

.

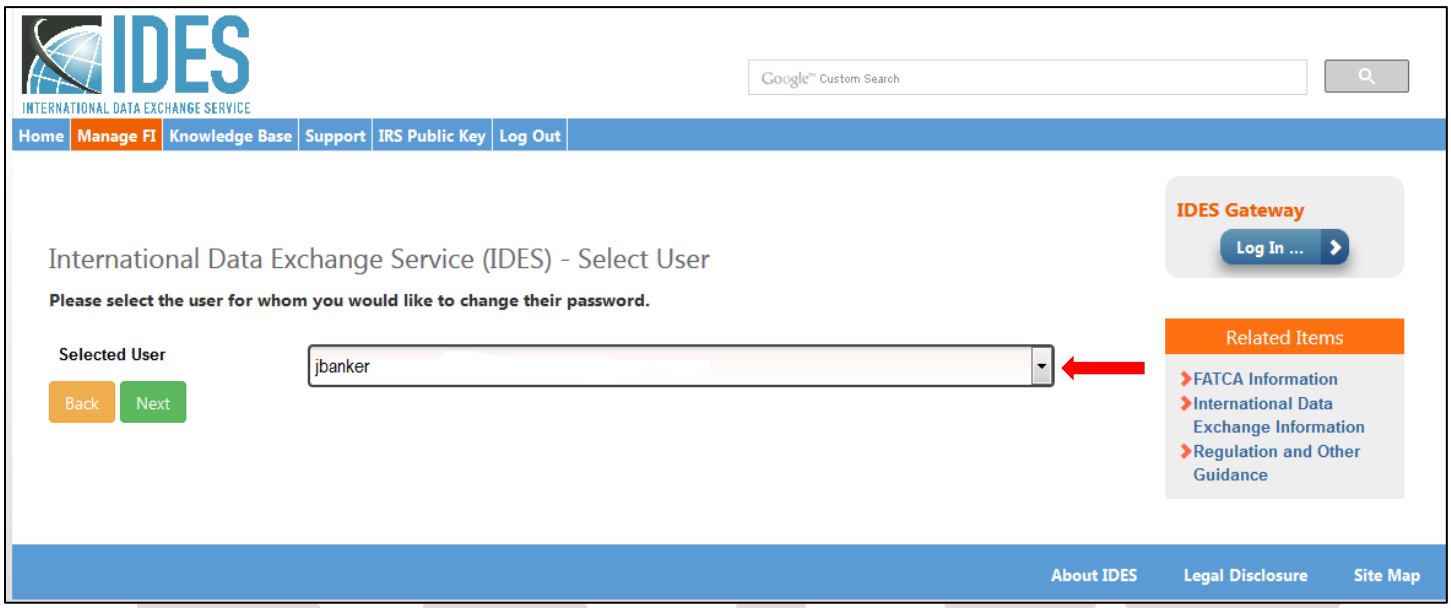


Figure 53 – Select the user to update.

2. **Select User** – Click on the drop down box to select the end user.
3. Click **Next**.

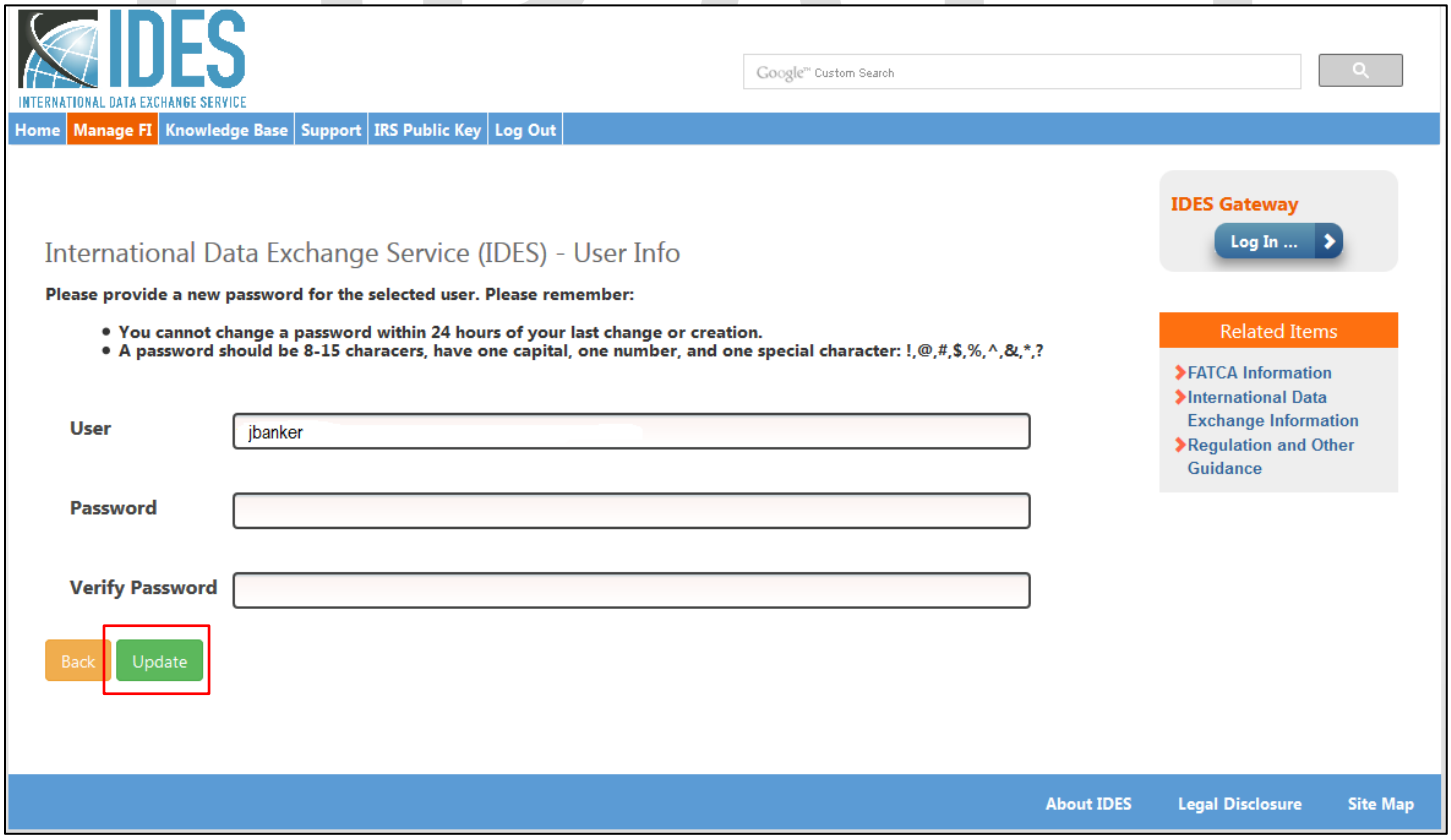


Figure 54 – Create a new password for the selected user.

4. **User** – Verify the correct user.
5. **Password** – Enter the new password.

DRAFT

a. Password Guidelines: The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .). If you enter a password that does not meet the guidelines, you will receive an error message.

6. **Verify Password** – Re-type your password (must match previous entry). If it does not match, you will receive an error message.
7. Click **Update** to complete password update.

7.8. Download the IRS Public Key

The IRS Public Key should be included in the transmission archive .zip file that is uploaded through the IDES Gateway.

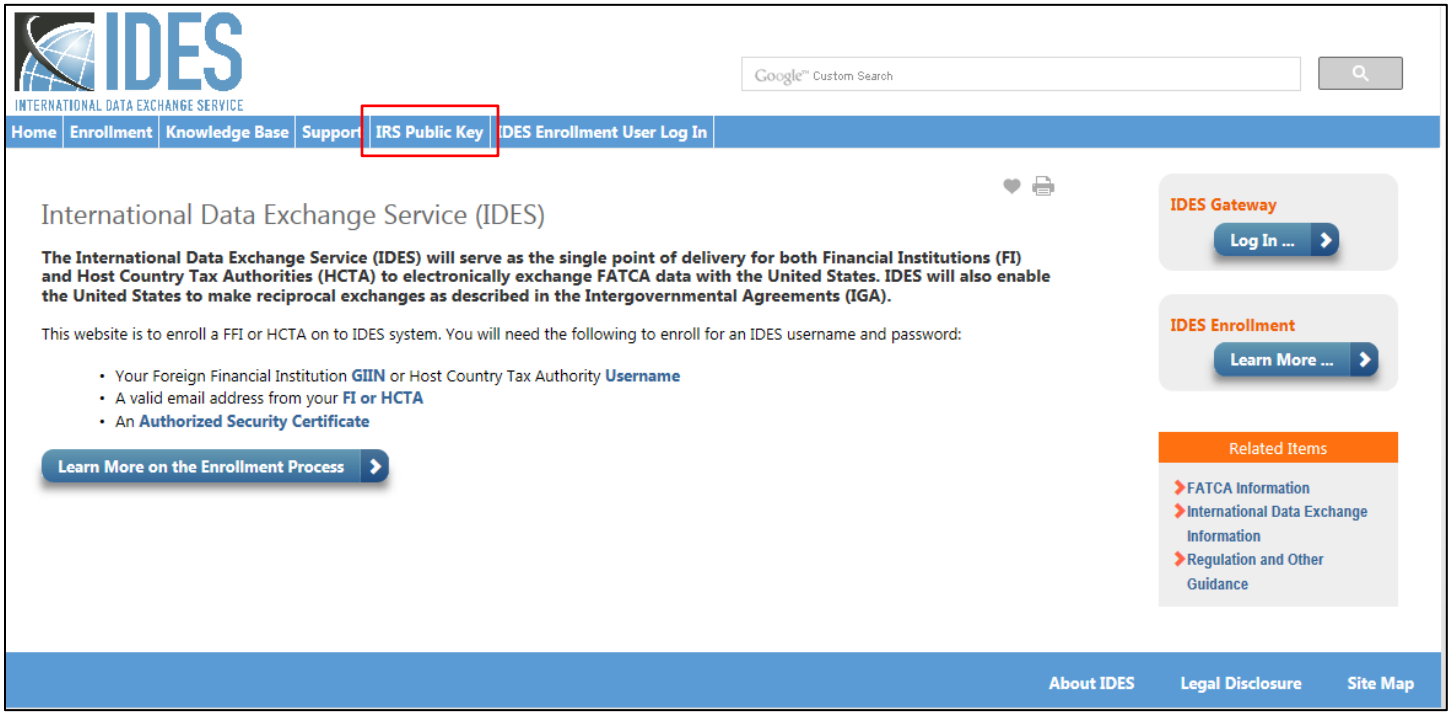


Figure 55 – Download the IRS public key

1. From the IDES Enrollment home page, click the **IRS Public Key** tab to begin download of the IRS Public Key Certificate to your computer.

Figure 56 – General certificate information.

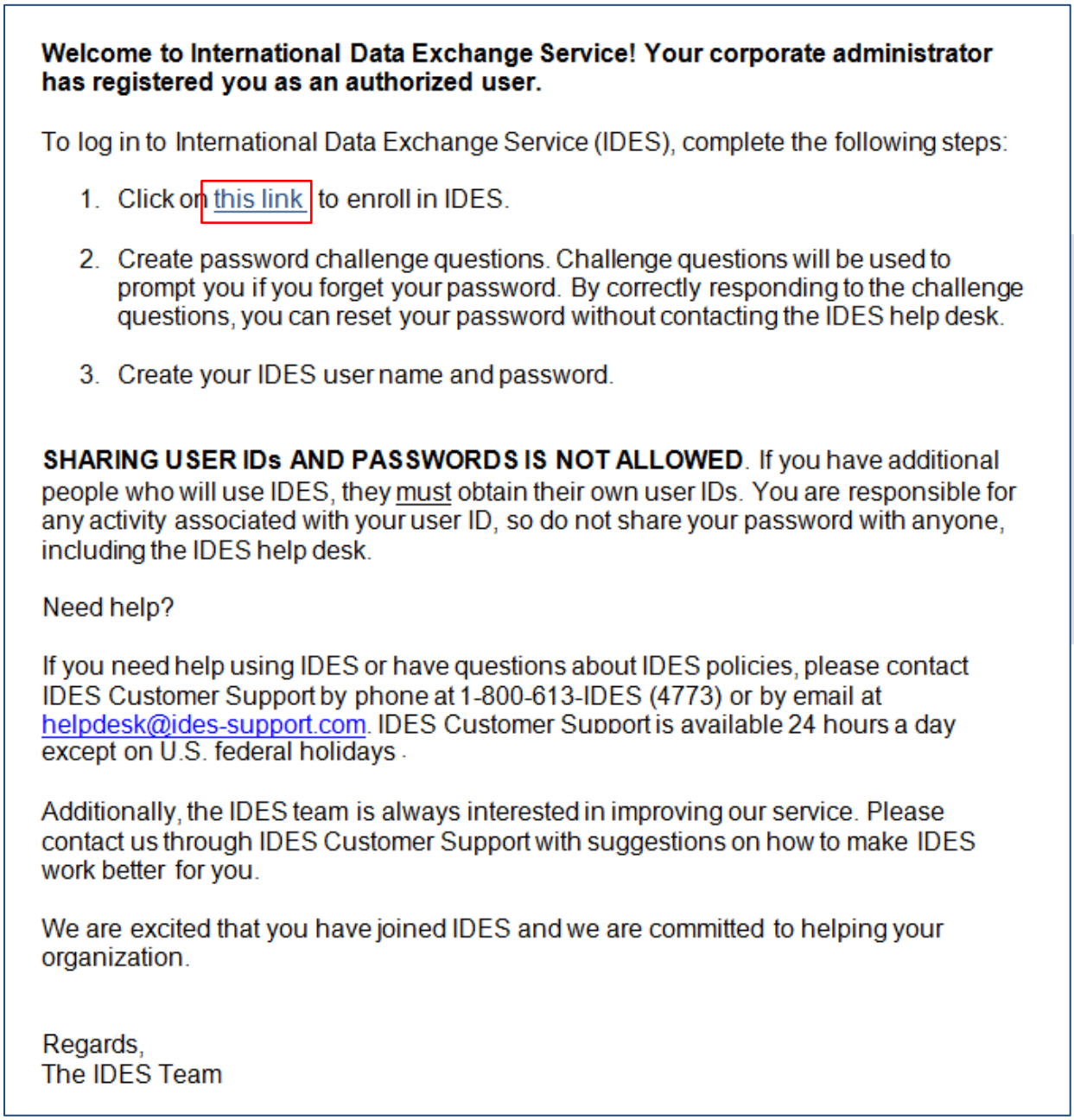
2. This certificate should be included in the FATCA reporting transmission archive you upload and transmit to the IRS via the IDES Gateway.

DRAFT

8. End Users

End users are added by the HCTA or FI Administrator. End users will receive an Email Registration Invitation from the IDES help desk in order to complete the IDES enrollment process. The link within the email is valid for 48 hours.

8.1. Create an Account



Welcome to International Data Exchange Service! Your corporate administrator has registered you as an authorized user.

To log in to International Data Exchange Service (IDES), complete the following steps:

1. Click on this link to enroll in IDES.
2. Create password challenge questions. Challenge questions will be used to prompt you if you forget your password. By correctly responding to the challenge questions, you can reset your password without contacting the IDES help desk.
3. Create your IDES user name and password.

SHARING USER IDs AND PASSWORDS IS NOT ALLOWED. If you have additional people who will use IDES, they must obtain their own user IDs. You are responsible for any activity associated with your user ID, so do not share your password with anyone, including the IDES help desk.

Need help?

If you need help using IDES or have questions about IDES policies, please contact IDES Customer Support by phone at 1-800-613-IDES (4773) or by email at helpdesk@ides-support.com. IDES Customer Support is available 24 hours a day except on U.S. federal holidays .

Additionally, the IDES team is always interested in improving our service. Please contact us through IDES Customer Support with suggestions on how to make IDES work better for you.

We are excited that you have joined IDES and we are committed to helping your organization.

Regards,
The IDES Team

Figure 57 – IDES new end user welcome email.

1. The new end user will receive a copy of the above email.
2. Users will click on **this link** within in the email to complete the IDES enrollment process.

8.2. Create Challenge Questions

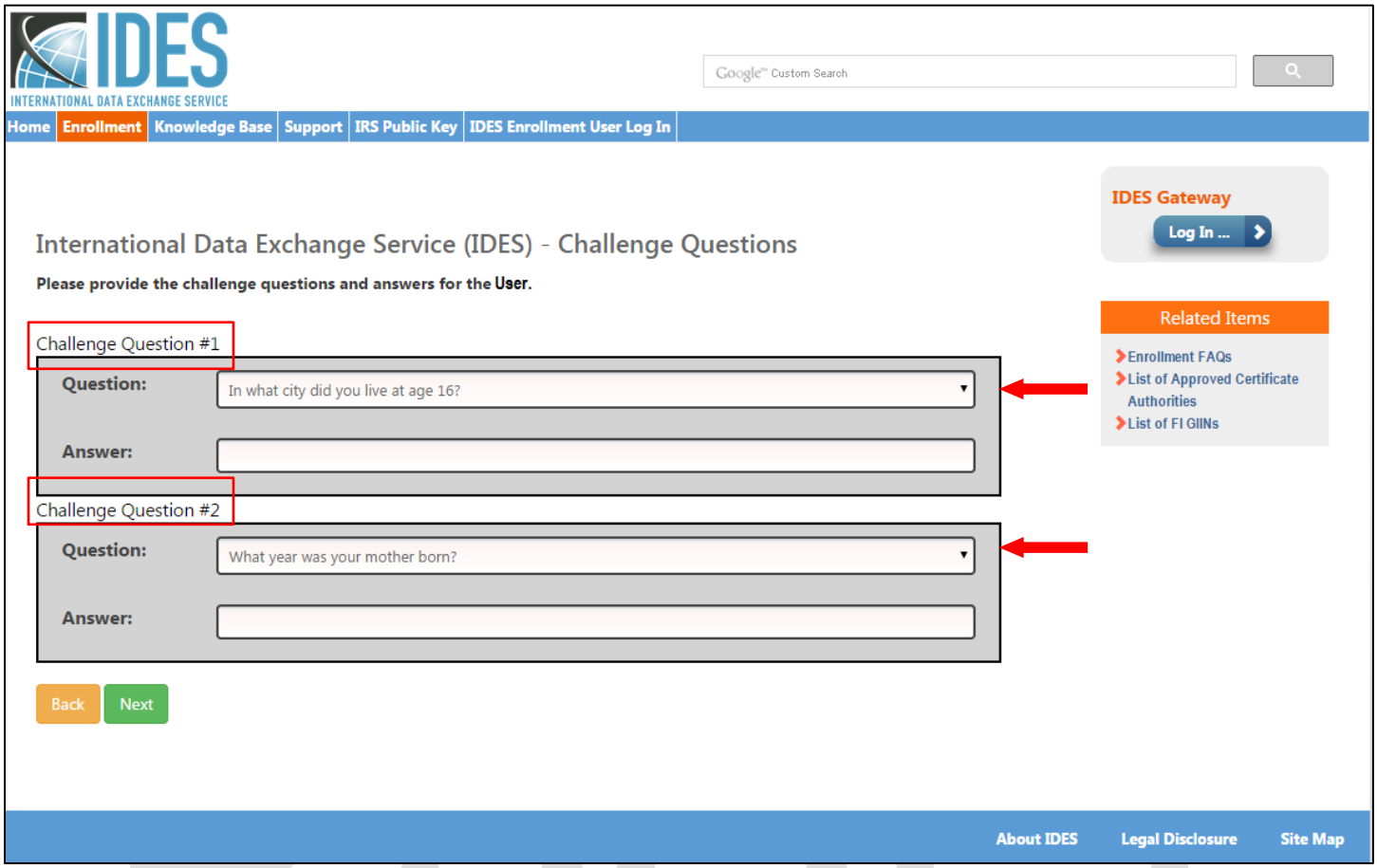


Figure 58 – Create IDES challenge questions.

1. **Challenge Question #1**
   c. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   d. Answer: Type a response to the challenge question.
2. **Challenge Question #2**
   c. Question: Select the drop-down arrow to view a list of questions. Select a challenge question.
   d. Answer: Type a response to the challenge question.
3. Click **Next** to continue and set up a **Username.**

IMPORTANT: Remember to document your answers to your challenge questions. Users will need these to reset password or to contact the IDES Help Desk. Note that challenge question responses must exactly match the responses as originally submitted.

.

8.3. Create User Profile

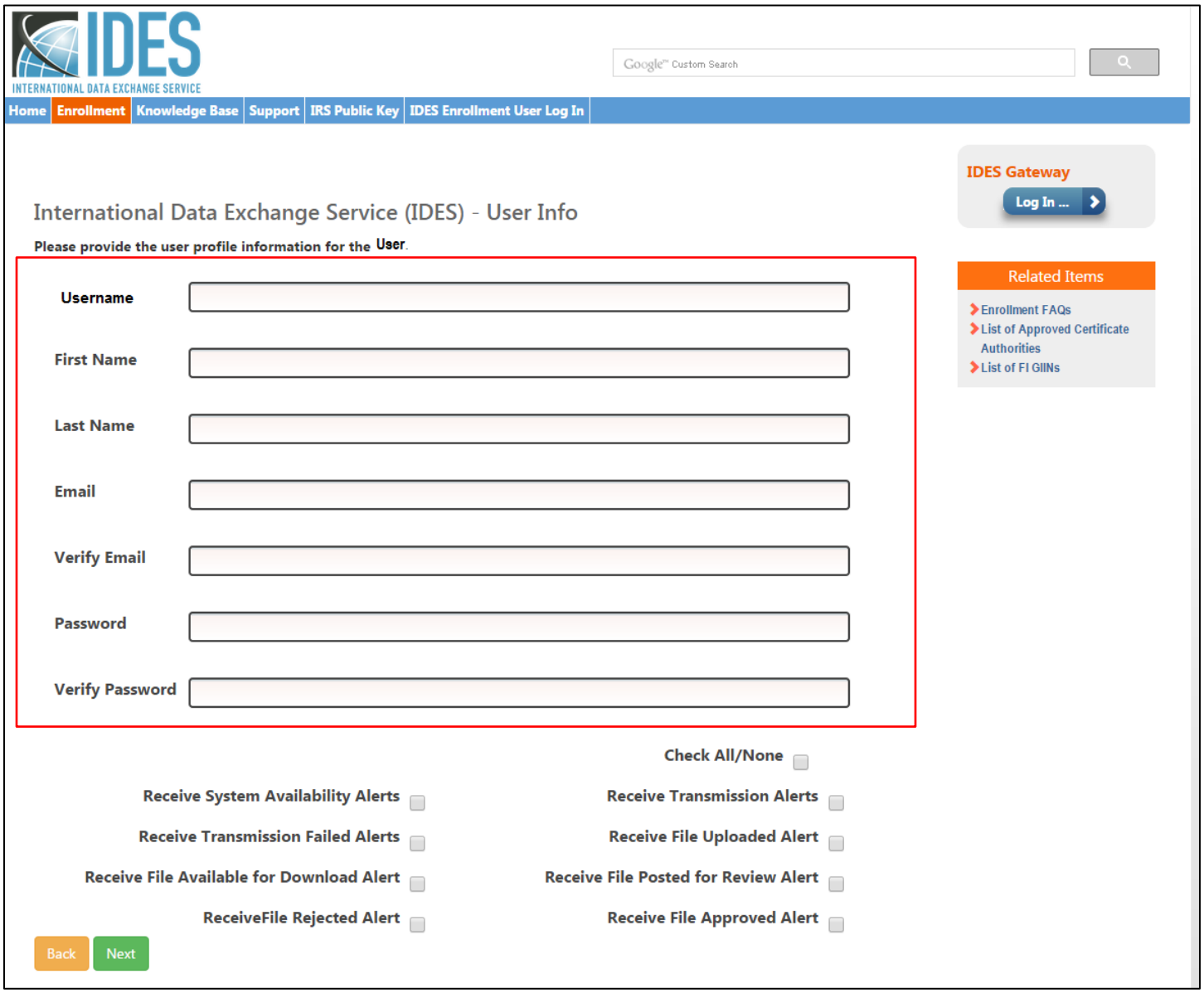


Figure 59 – Submit user profile information.

1. **Username** – Enter your new username. We recommend first initial and last name. If the username is already taken you will receive an error message.
2. **First Name** – Enter your first name.
3. **Last Name** – Enter your last name.
4. **Email** – Enter your email address.
    a. It is mandatory to use a unique email address for enrollment as the system will not allow for duplicate email addresses. The email address may be a personal email address or a shared mailbox address.
5. **Verify Email** – Enter your email address again (must match the previous entry). If it does not match, you will receive an error message.
6. **Password** – Create a valid password.

a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @ # % ^ * () ? , .).
b. If you enter a password that does not meet the guidelines, you will receive an error message.

7. **Verify Password** – Re-type your password (must match the previous entry). If it does not match, you will receive an error message.

8.4. Select Alert Preferences

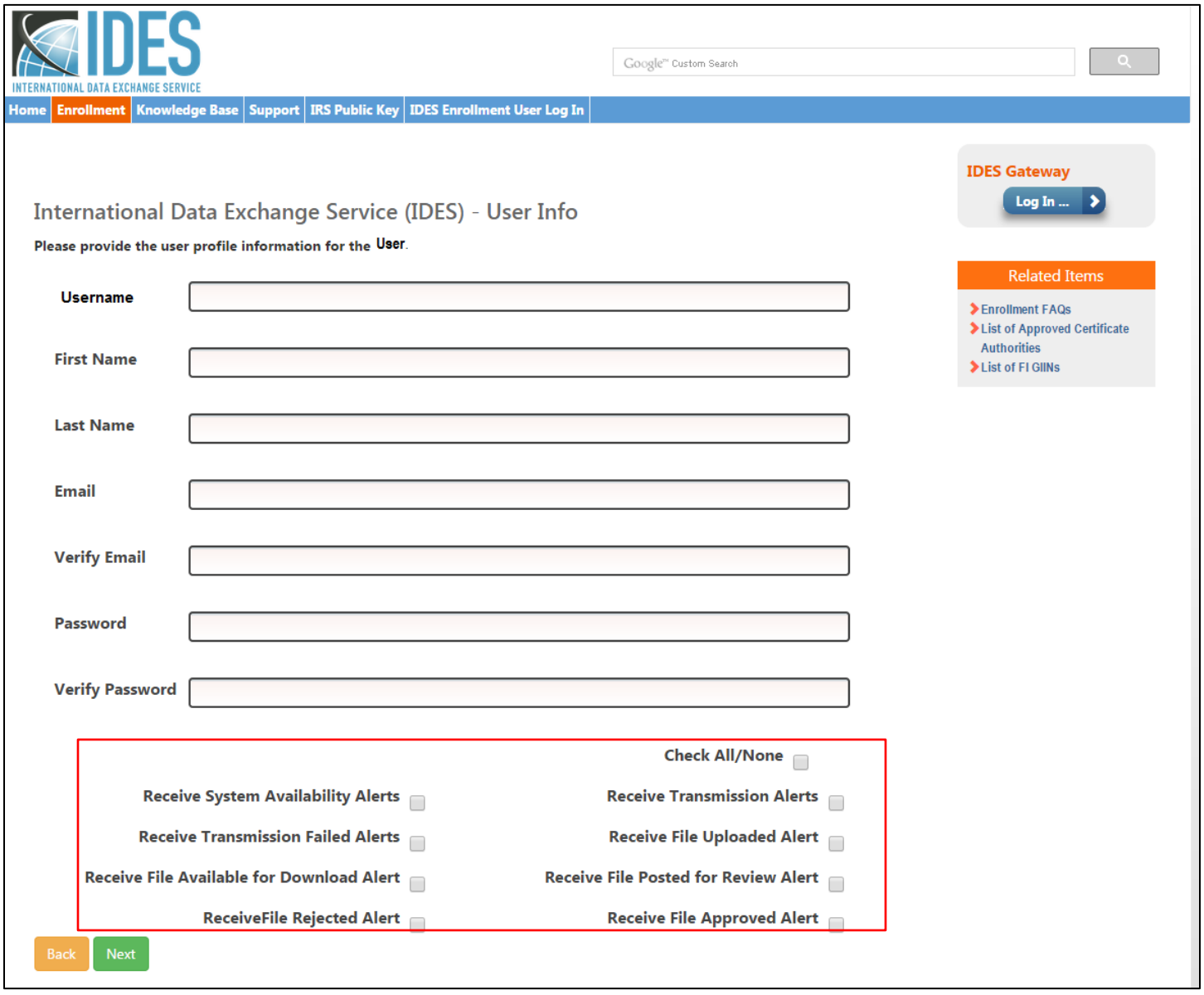


Figure 60 – Select IDES alert preferences.

1. Select Alert Preferences – Click on the box next to the alerts you wish to receive by email. You can click the Check All/None box to choose all alerts or to remove all alerts. You must select user preferences to receive alerts. There are eight Alert Preferences.

Alert Preference	Description
a. System Availability Alert	IDES Enrollment and/or IDES Gateway are unavailable.
b. Transmission Failed Alert	Transmission uploaded via the IDES Gateway failed for one of several reasons (e.g., virus, encryption validation, naming convention, package content). The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission failed.
c. File Available for Download Alert	The user has a file to download on the IDES Gateway. This is not functional at this time.
d. File Rejected Alert (for Model 1 Option 2 countries)	Transmission upload was rejected by the HCTA. The email will have an alert code that you will need to look up on the IDES Gateway to determine the reason the transmission was rejected.
e. Transmission Alert	Receive all IDES Alerts (See Alerts **b,c,d,f,g,h**).
f. File Uploaded Alert	Received transmission is uploaded to the IRS for review.
g. File Posted for Review Alert (for Model 1 Option 2 countries)	Sent to the HCTA when an FI uploads a report.
h. File Approved Alert (for Model 1 Option 2 countries)	Sent after the HCTA has approved the FI file.

Table 8 – IDES Alert Preferences

2. Click **Next** to continue to complete enrollment process.

DRAFT

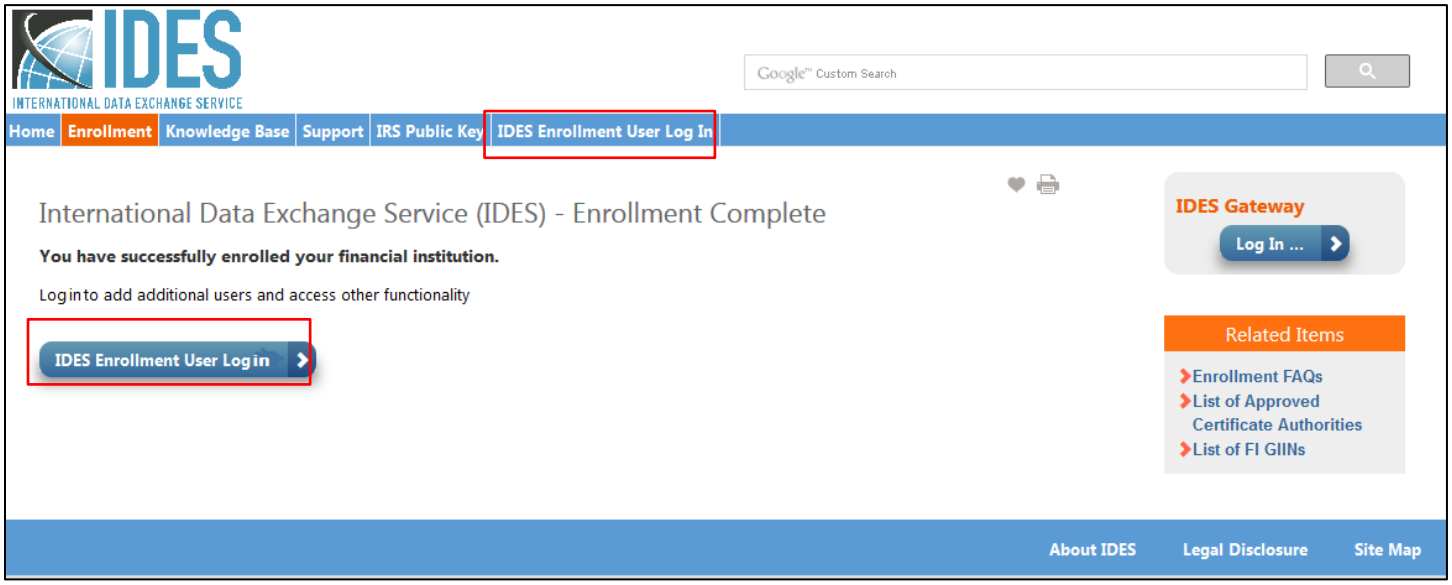


Figure 61 – Enrollment Confirmation.

DRAFT

3. You have completed the enrollment process as an end user. You will also receive an email from the IDES help desk that verifies your authorization to access the IDES Gateway.
4. Click **IDES Enrollment User Log In** to log in as an end user.

8.5. IDES Enrollment User Log In

1. Access the IDES Enrollment site at www.IDES-Support.com.

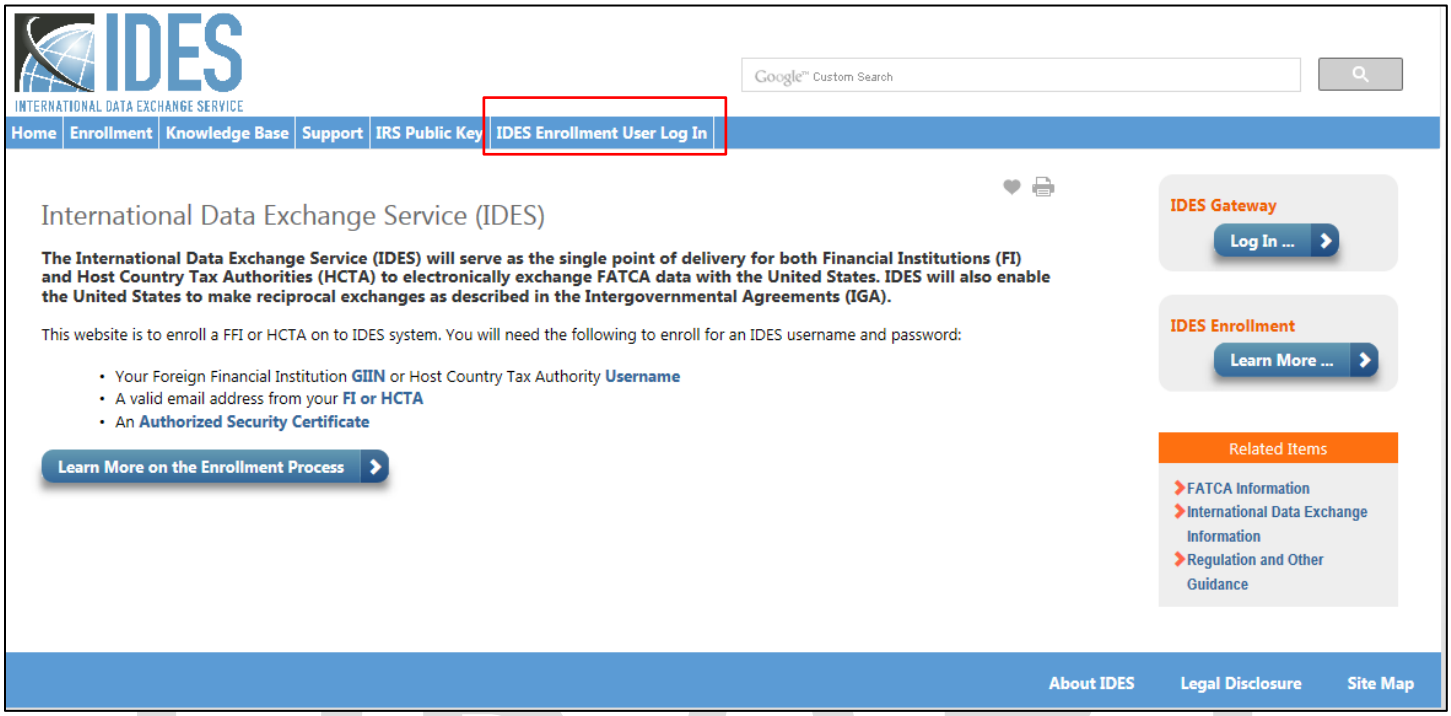


Figure 62 – IDES enrollment user log in page.

2. Click on the **IDES Enrollment User Log In** tab.

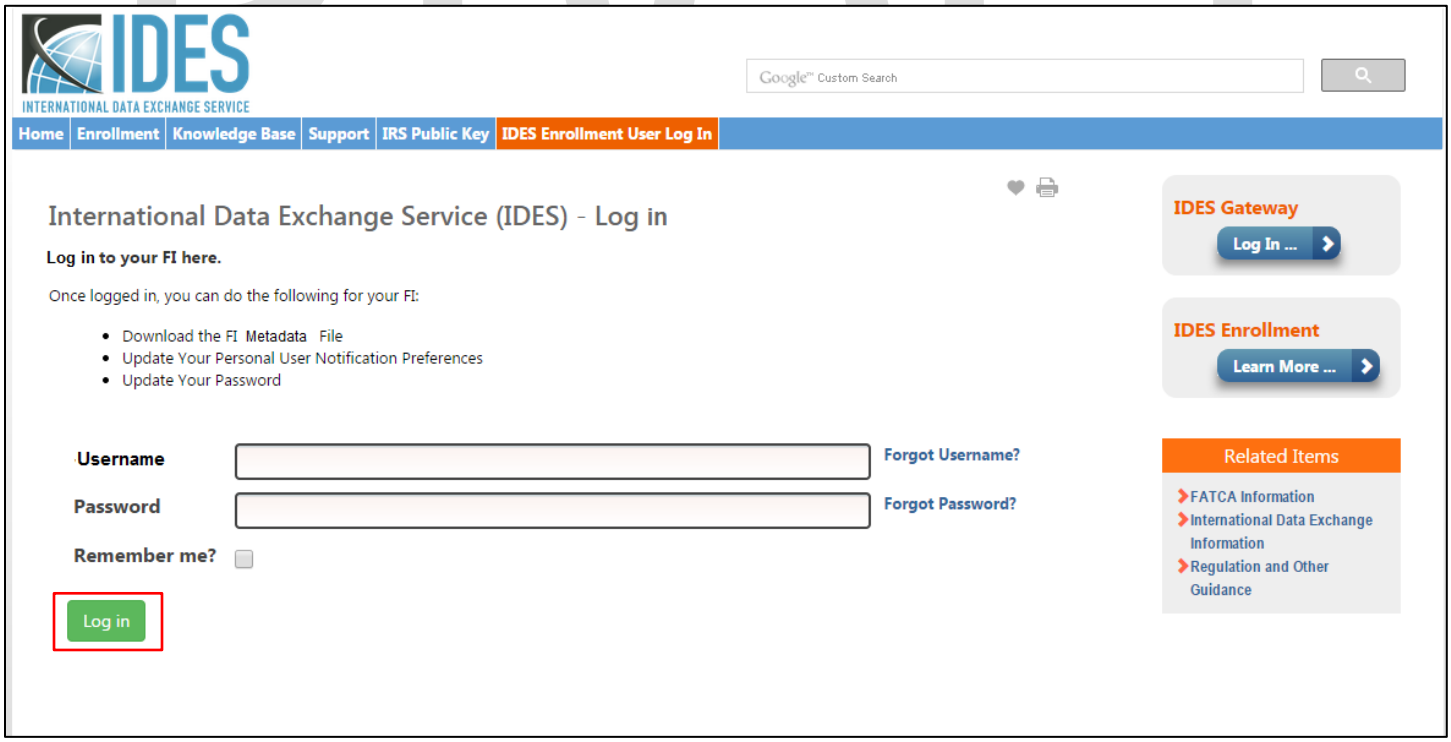


Figure 63 – Log in to the IDES enrollment site.

3. **Username** – Enter Username
4. **Password** – Enter Password
5. Click **Log in**.

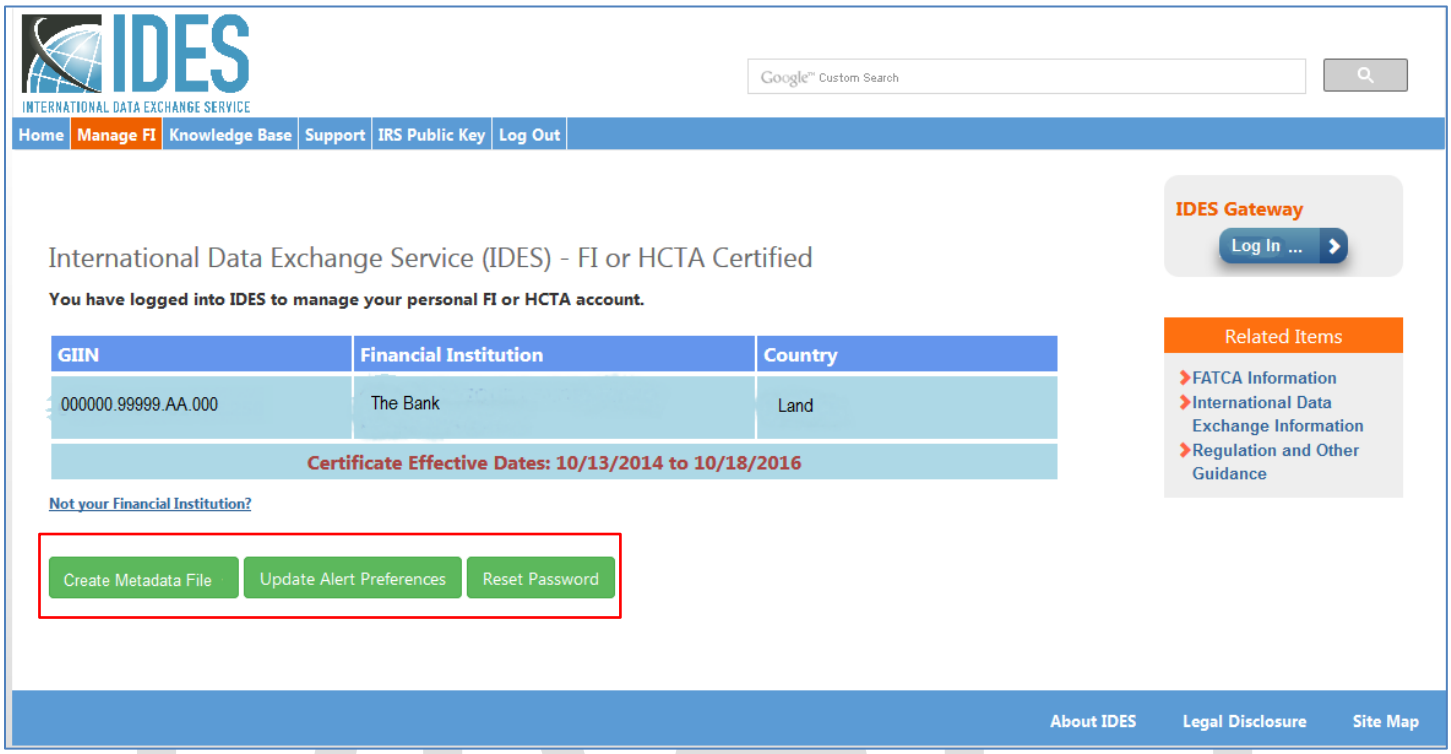


Figure 64 – Manage an IDES user account.

6. You are now signed in. You can perform three functions from this screen:
   a. **Create a Metadata File**.
   b. **Update Alert Preferences**.
   c. **Reset Password**.

8.6. Create a Metadata File

Metadata is a collection of data about the content and characteristics of the FATCA reporting files. It is used to ensure the transmission archives are correctly processed. The metadata file will be included in the transmission archive and may also be created during the data preparation phase. HCTAs and FIs should create and validate metadata files using the FATCA IDES Metadata XML Schema v1.0.

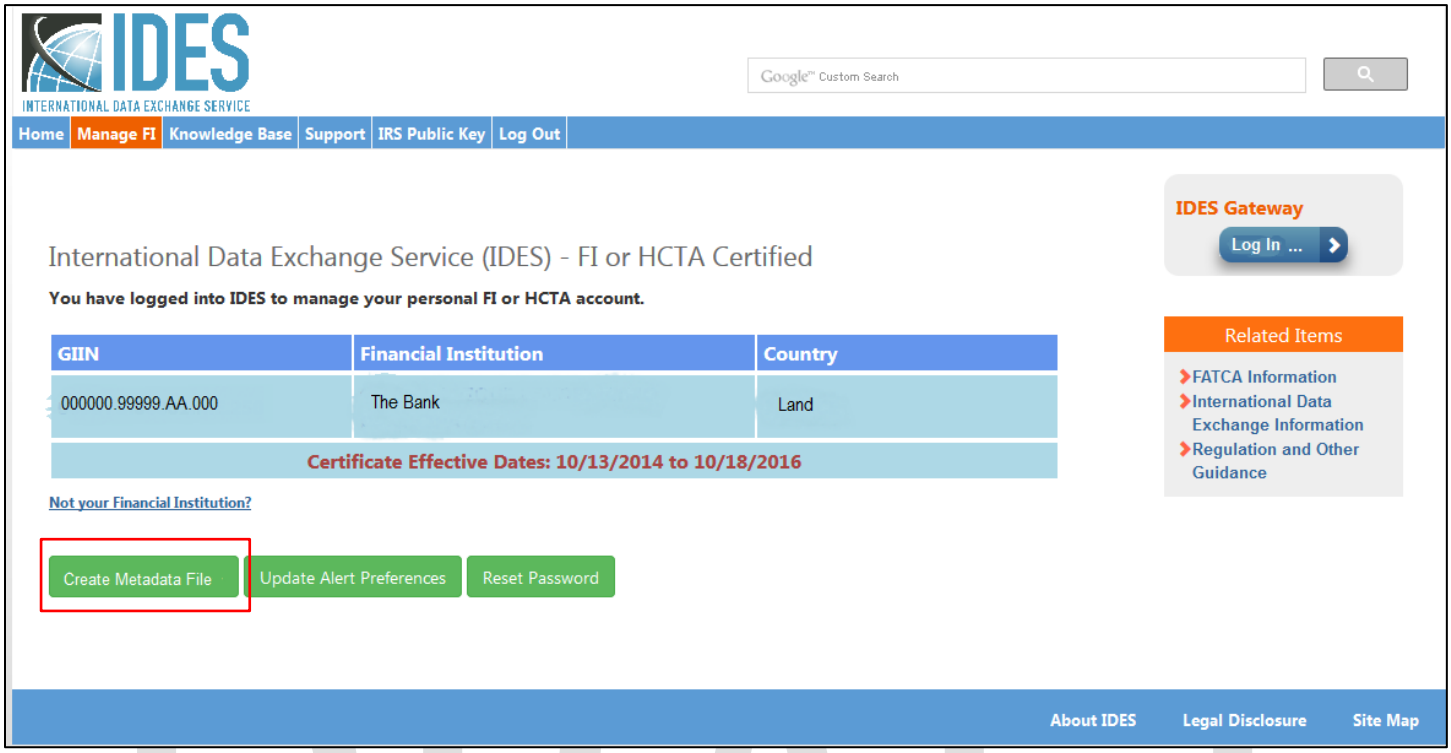


Figure 65 – Create a Metadata File.

1. From the **Manage FI** tab, click **Create Metadata File.**
2. Refer to Create a Metadata File for full instructions.

DRAFT

8.7. Update Alert Preferences

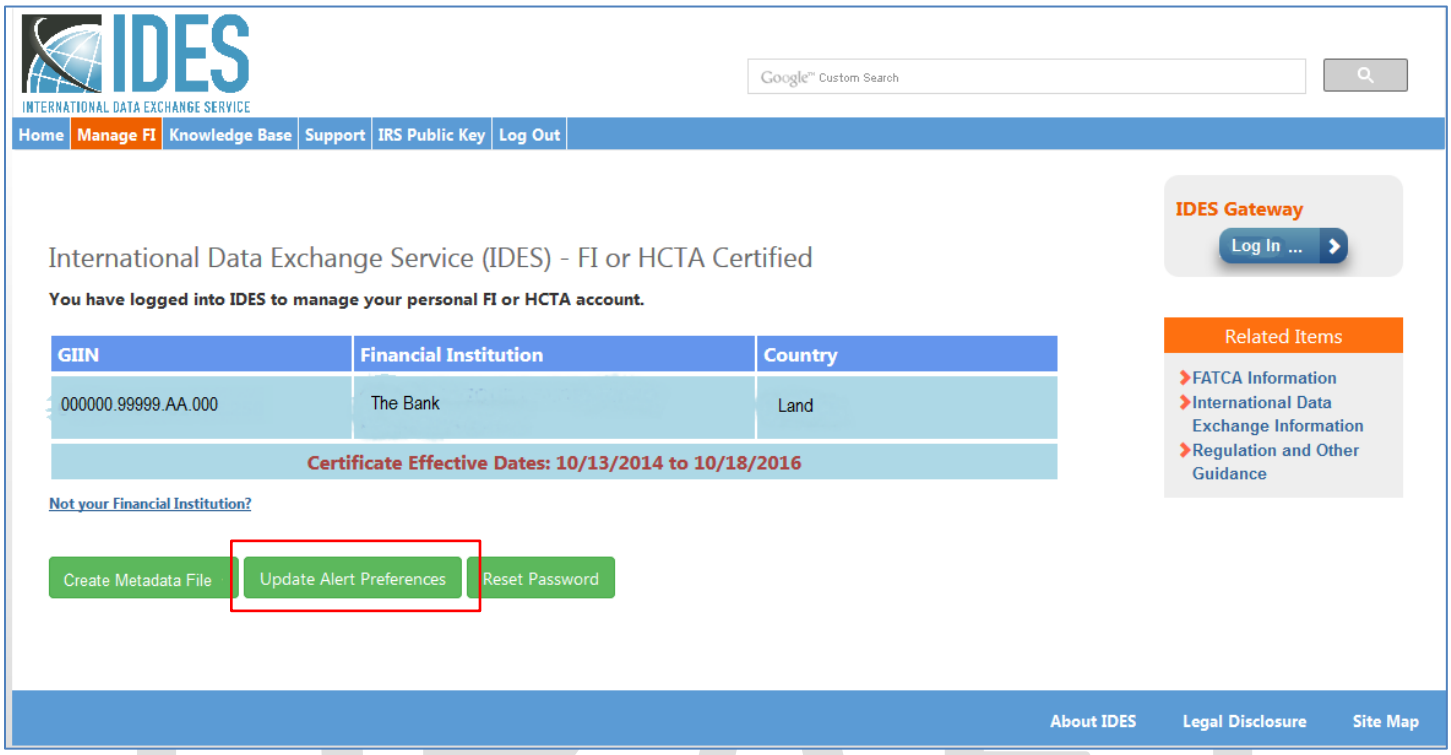


Figure 66 – Update IDES alert preferences.

1. From the **Manage FI** tab, click **Update Alert Preferences.**

DRAFT

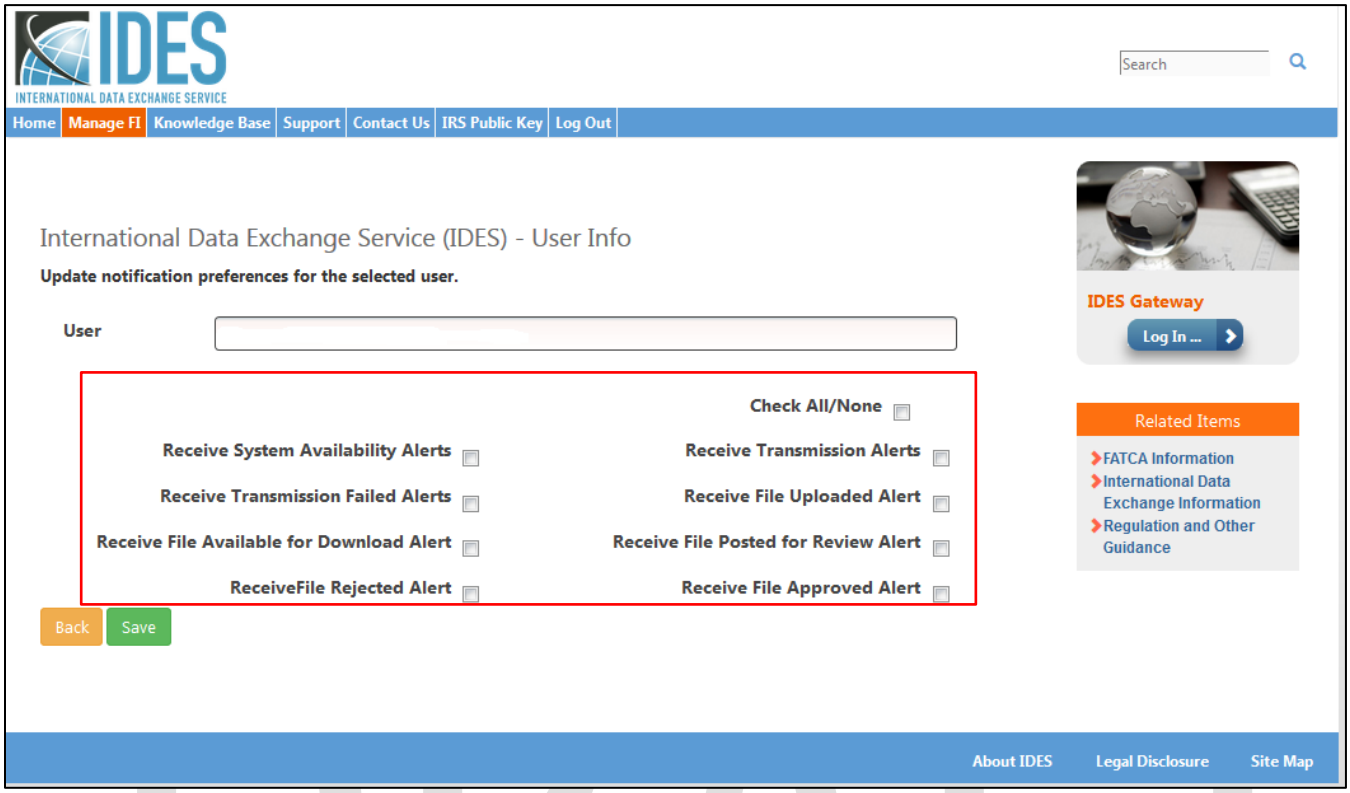


Figure 67 – Selecting new alert preferences.

2. Username will appear in the **User** field
3. Select the Alert(s) that you want to receive by email. If you want to receive all alerts click the **Check All/None** box. Clicking it again will remove all alerts. See Select Alert Preferences for full instructions.

DRAFT

8.8. Reset Password

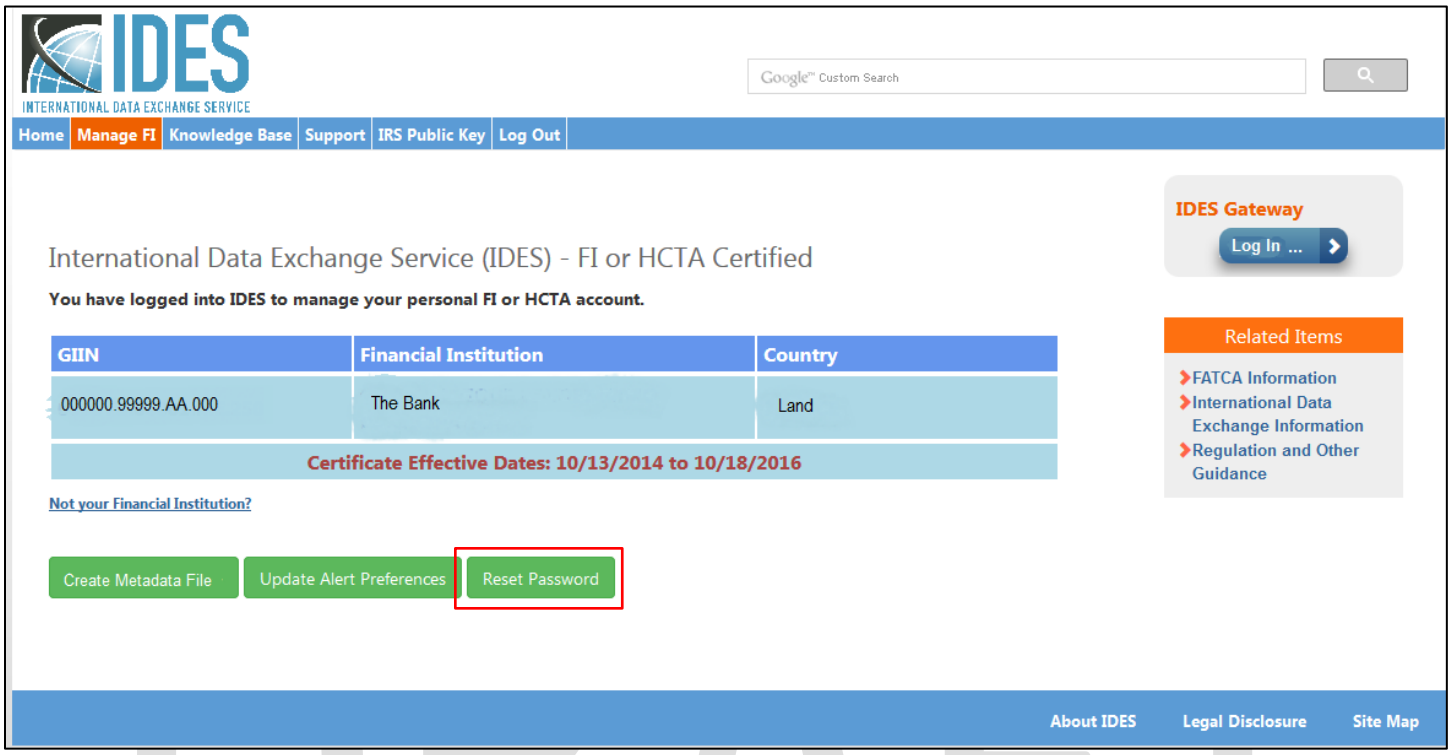


Figure 68 – Reset a password.

1. From the **Manage FI** tab, click **Reset Password.**

DRAFT

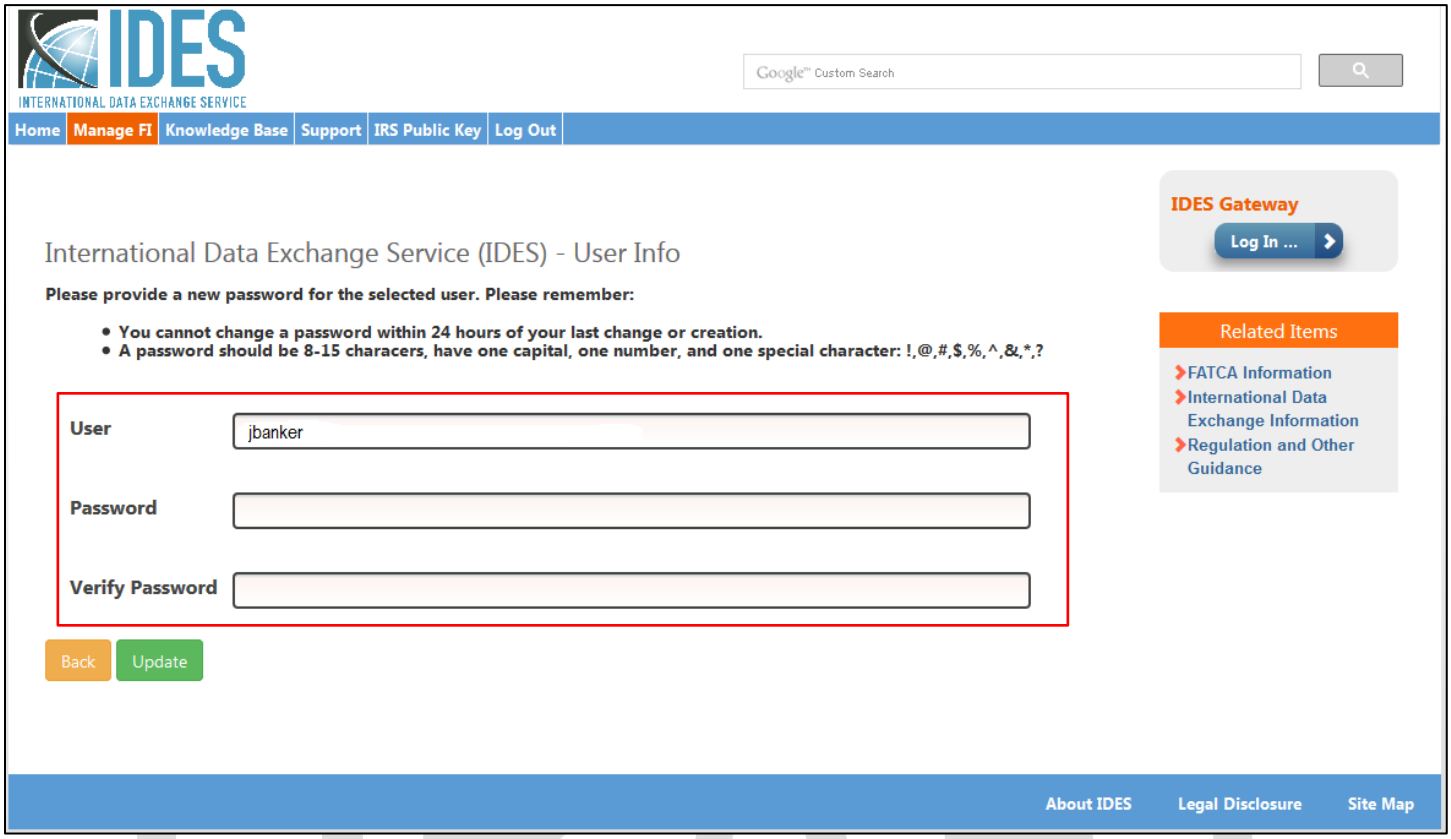


Figure 69 – Create a new password.

2. **User** - Verify your username.
3. **Password** – Enter a new password.
    a. The password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .). If you enter a password that does not meet the guidelines, you will receive an error message.
4. **Verify Password** - Re-type your password (must match previous entry). If it does not match, you will receive an error message.
5. Click **Update** to complete password update.

DRAFT

8.9. Forgot Username

If an end user forgets their username, they can request a Username reminder email.

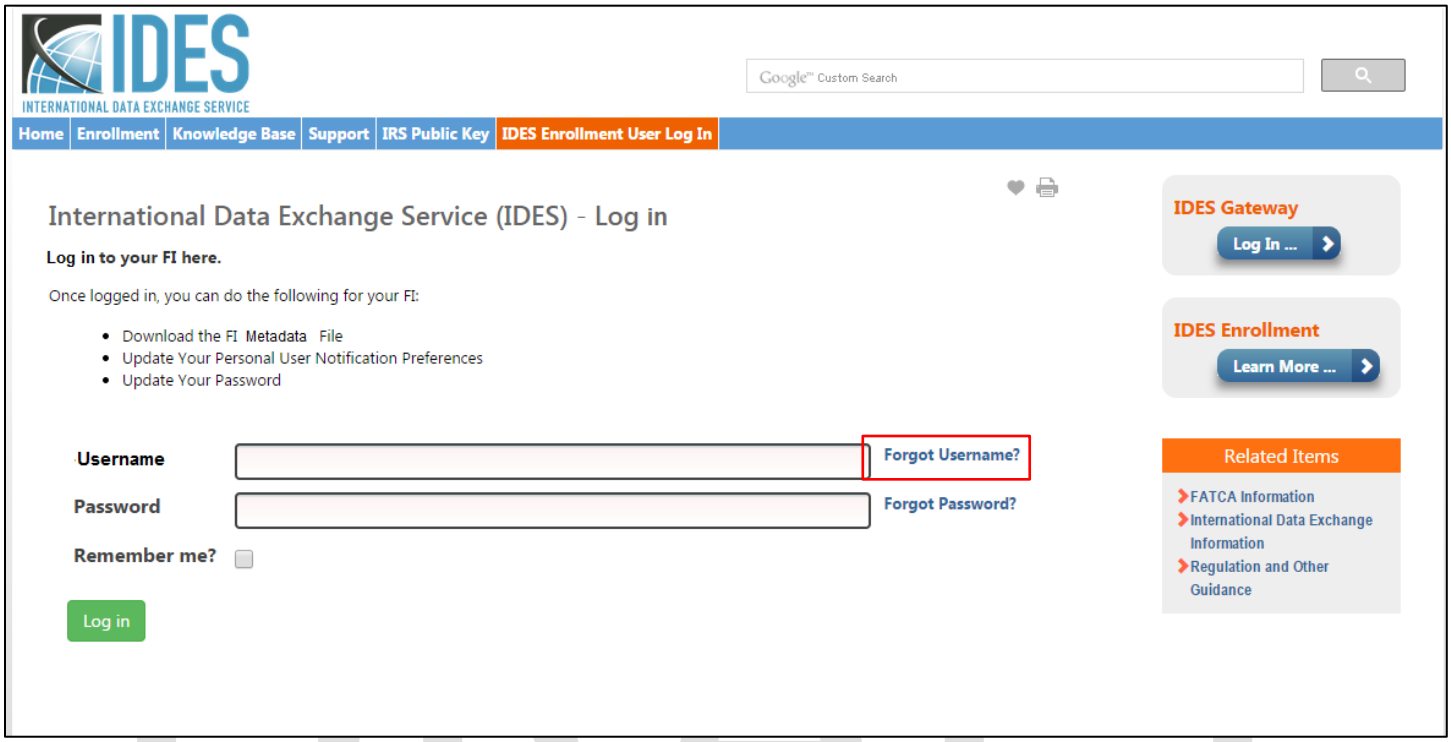


Figure 70 – Request a Username reminder email.

1. Select **IDES Enrollment User Log In** tab, click **Forgot Username?**

DRAFT

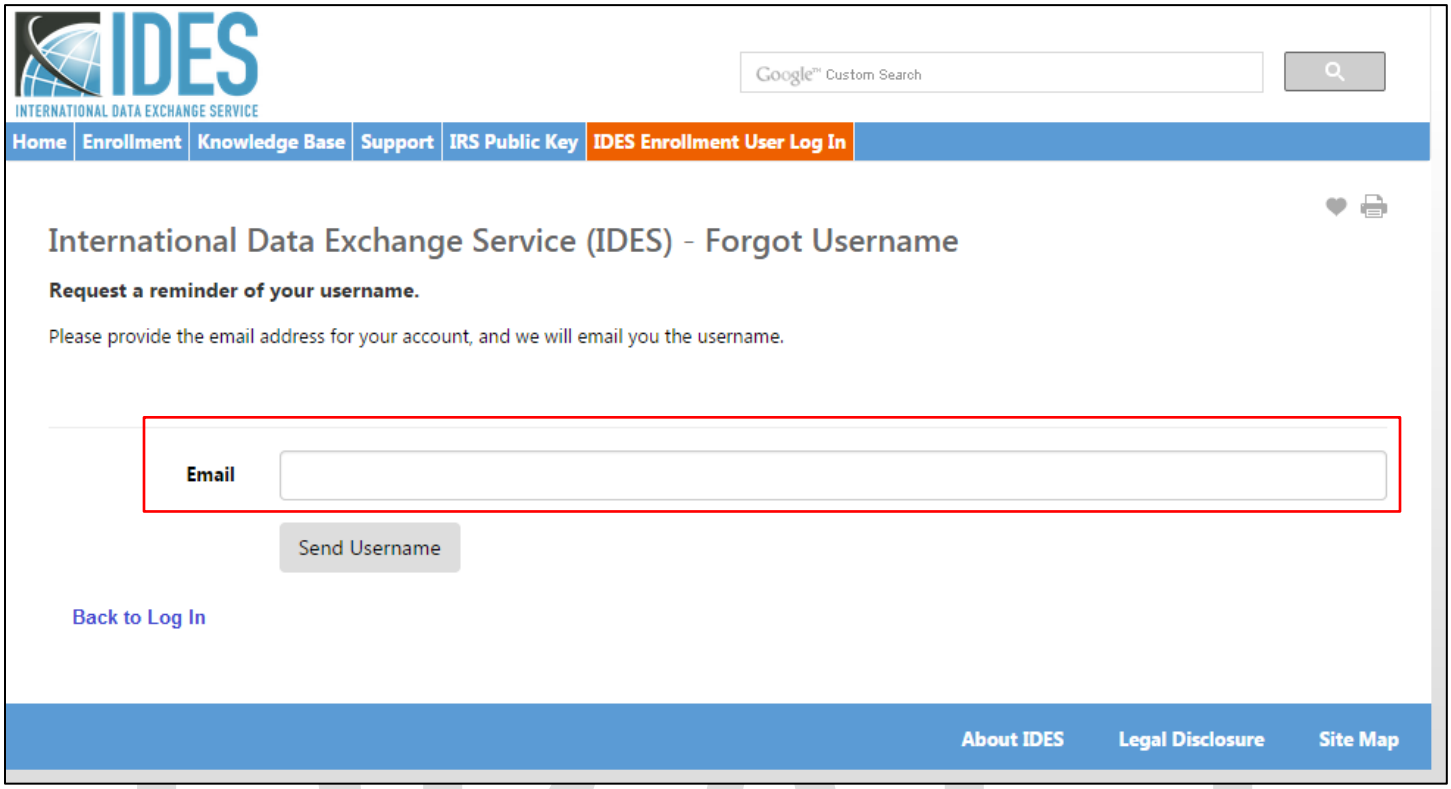


Figure 71 – Enter an email address for a username reminder message.

2. **Email** – Enter the email address used to register on the IDES enrollment site.
3. Click **Send Username**.

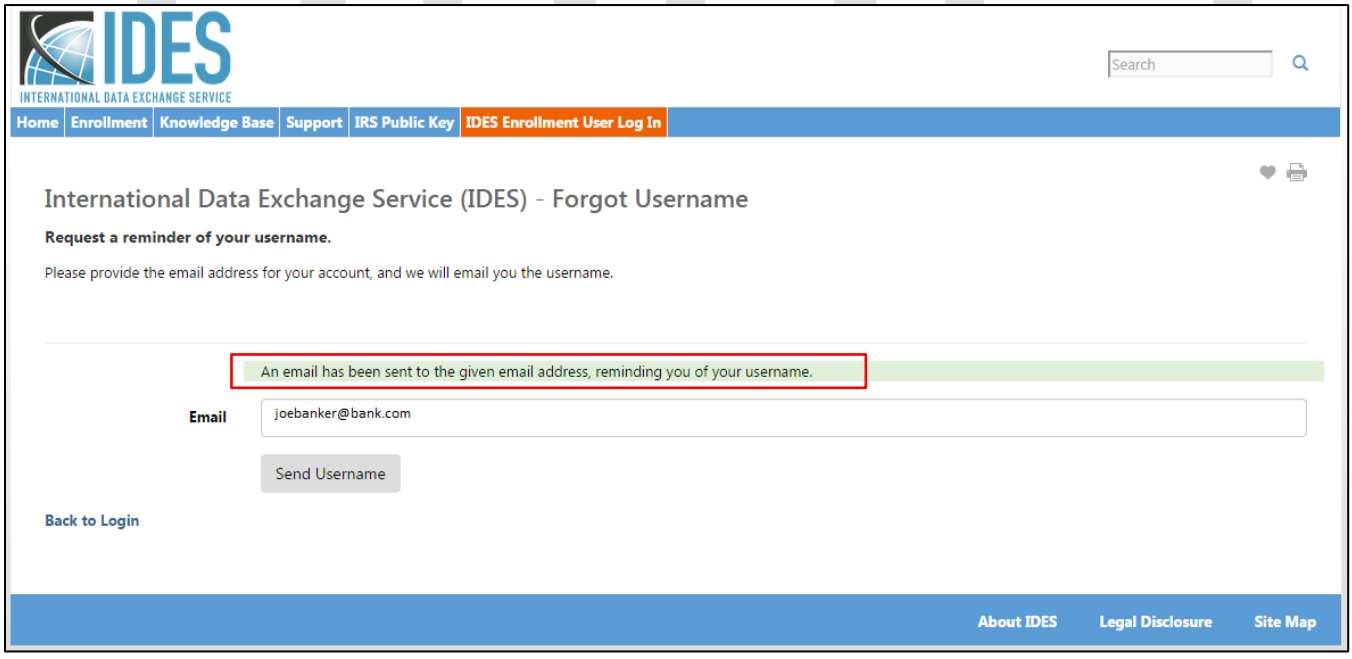


Figure 72 – Reminder email sent confirmation.

4. Confirmation page showing that username reminder email was sent.

DRAFT

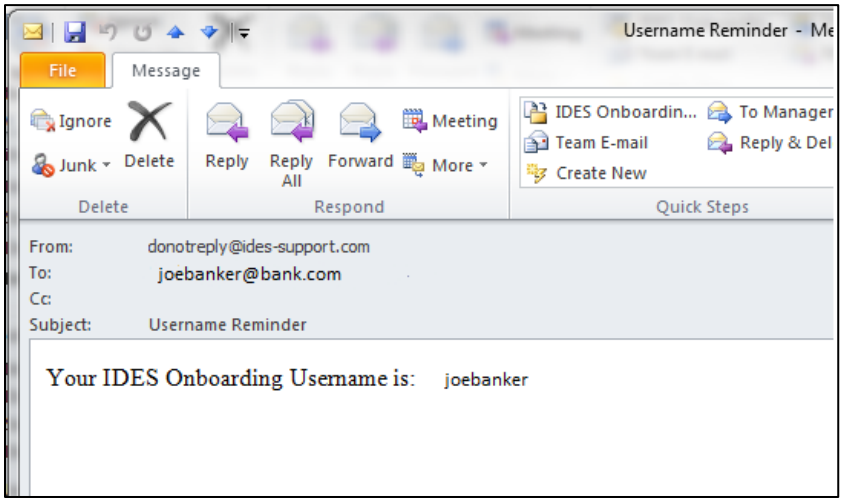


Figure 73 – IDES username reminder email.

5. Check your email for a copy of Username Reminder email. Return to the IDES enrollment home page and select the **IDES Enrollment User Log In** tab.

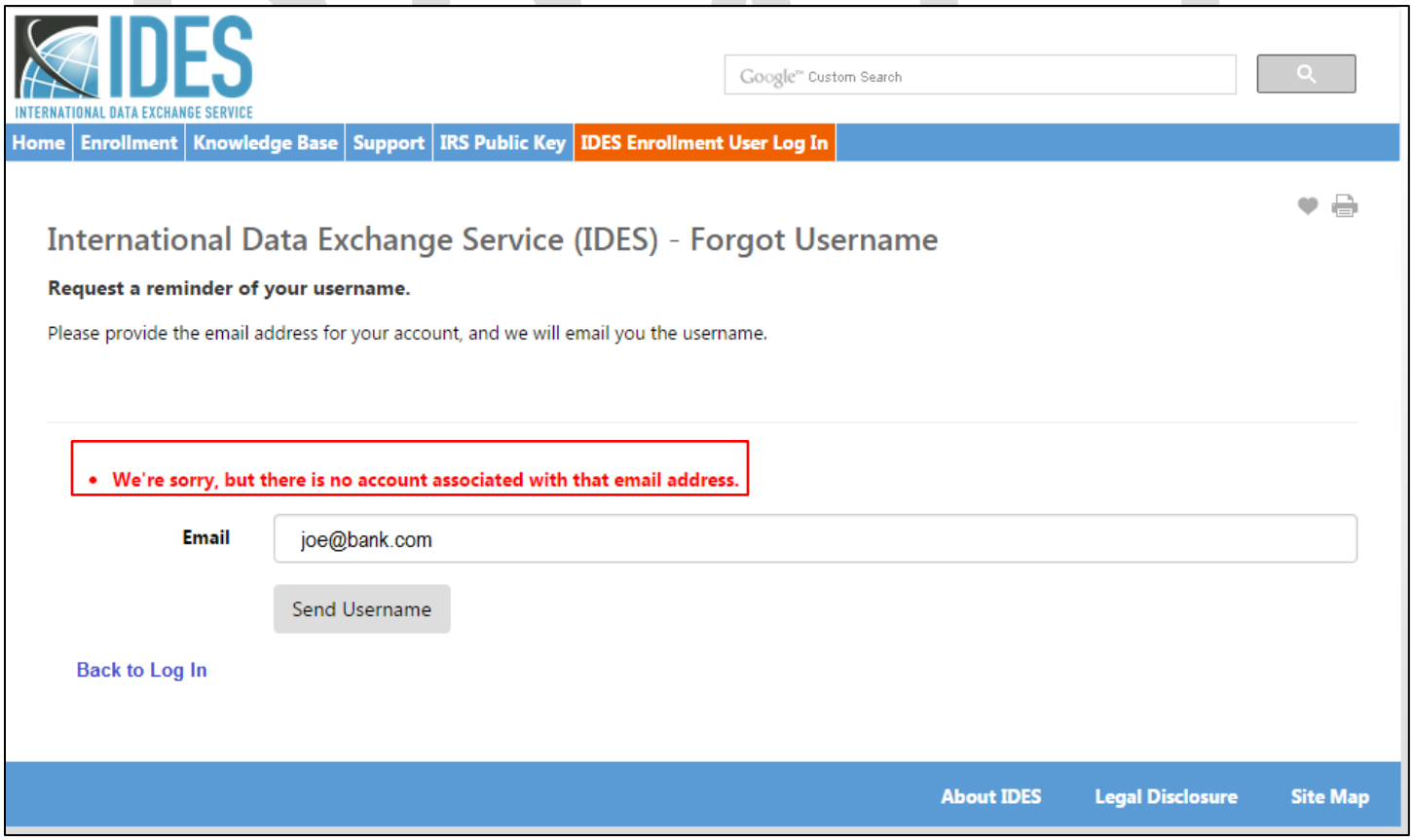


Figure 74 –User email address not recognized error message.

Note: If there is not an IDES account associated with the email address entered, you will receive an error message. Enter the same email that was used for enrollment. If you still receive the error after entering the correct email, contact the Help Desk.

8.10. Forgot Password

Passwords can be reset on the **IDES Enrollment User Log In** tab.

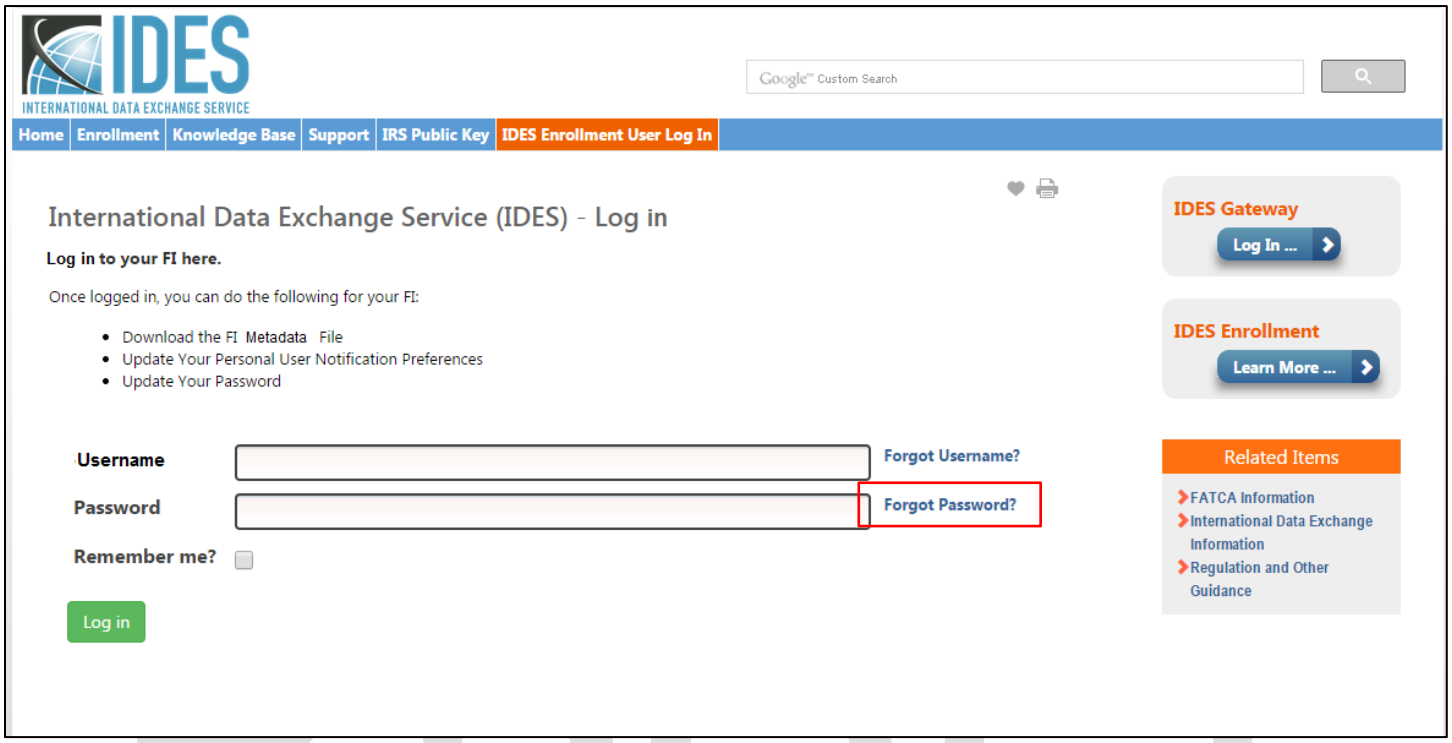


Figure 75 – Forgot Password reset page.

1. Select **IDES Enrollment User Log In** tab, click on **Forgot Password?**

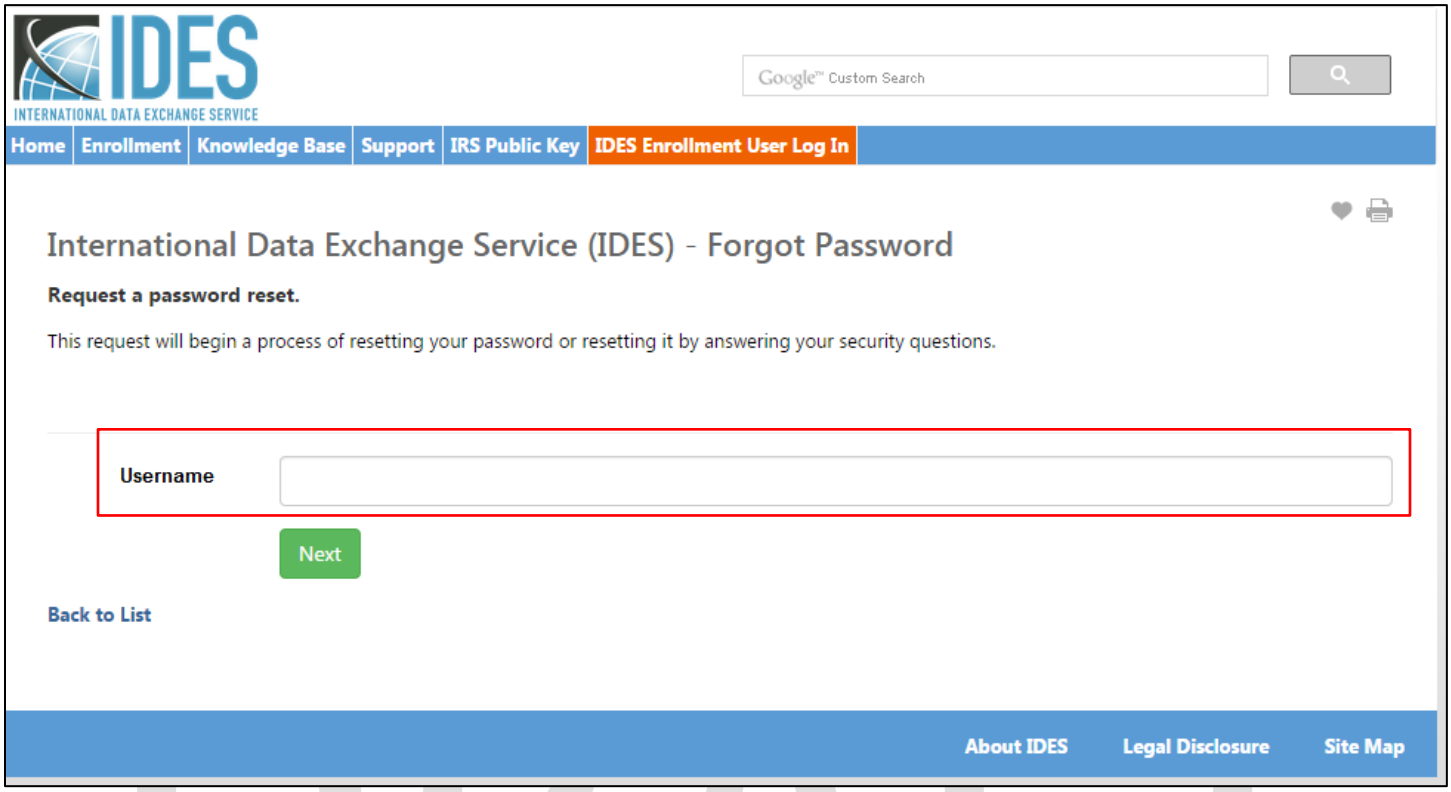


Figure 76 – Enter a username to reset a password.

2. **Username** – Enter your username.
3. Click **Next** to continue.

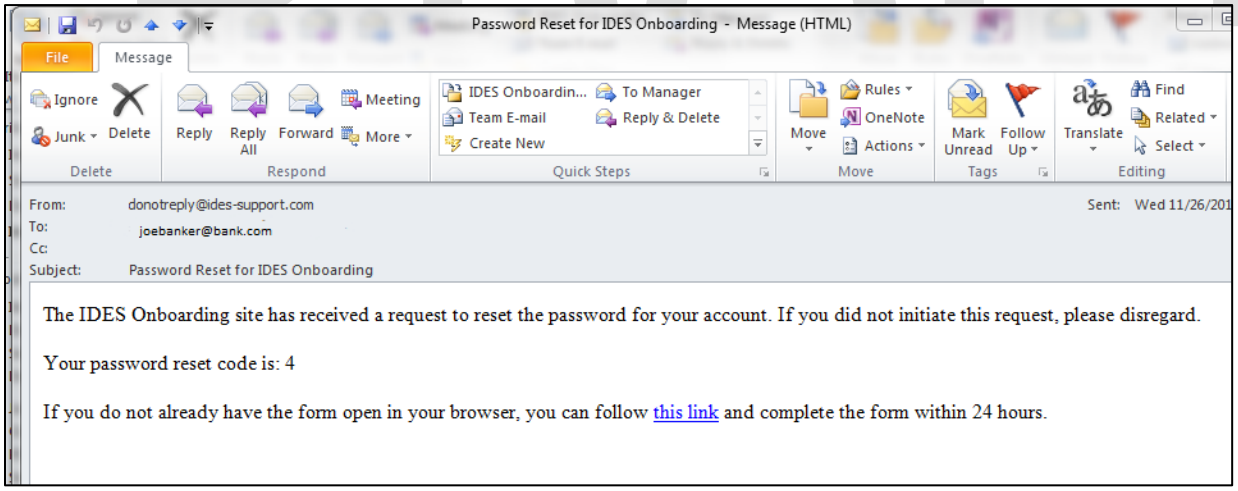


Figure 77 – Email sent to users to reset a password.

4. An email will be sent to the email address provided during enrollment. The email will contain a reset code needed to reset the user's password.

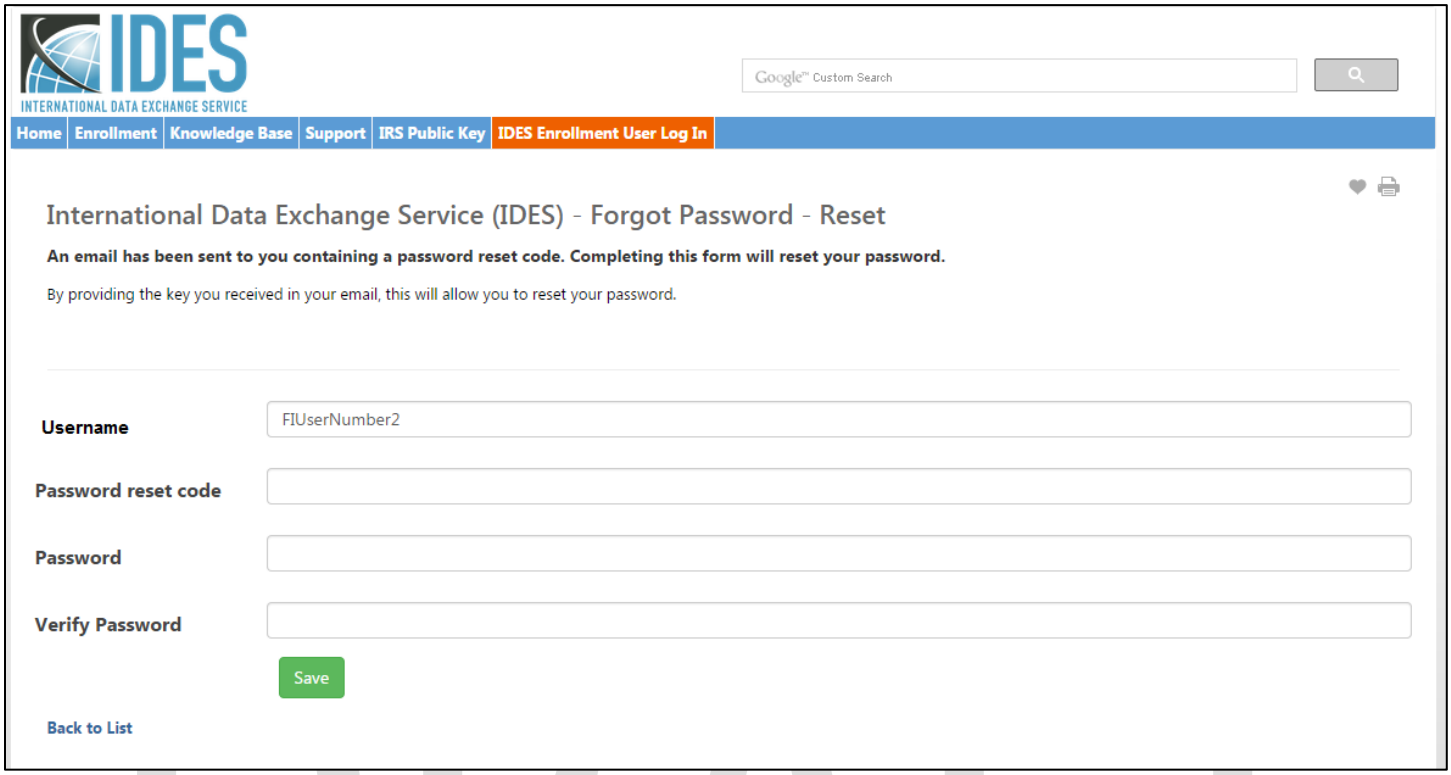


Figure 78 – Create a new password.

5. **Password Reset Code** – Enter the reset code you received in your email.
6. **Password** – Enter your new password.
   a. The Password must be 8-20 characters and include at least one uppercase and lowercase letter, one number, and one of the designated special characters (~ ! @# % ^ * () ? , .). If you enter a password that does not meet the guidelines, you will receive an error message.
7. **Verify Password** – Re-type your password (must match previous entry). If it does not match, you will receive an error message.
8. Click **Save** and return to the **IDES Enrollment User Log In** tab to log in with your new password.

DRAFT

9. Data Preparation for FATCA XML Report

9.1. Overview

This section describes how to prepare a FATCA data file. Before you begin, you must have a valid certificate from an IRS approved certificate authority.

9.2. Prepare the FATCA XML File

These instructions may change with maintenance updates to the system. IDES will only accept files in .zip format. Each archive will contain either three or four files depending on the IGA Model and the type of user. These archives will consist of the following files:

- FATCAEntitySenderId_Payload
- FATCAEntityReceiverId_Key
- HCTAFATCAEntityId_Key (Model 1, Option 2 only)
- FATCAEntitySenderId_Metadata.xml

Steps	Process	File Naming Convention
---	Obtain a digital certificate from an approved Certificate Authority (CA). See Section 3, Obtaining a Digital Certificate	Not applicable
1	Prepare and validate the FATCA XML file Digitally sign the file	FATCAEntitySenderId_Payload.xml
2	Compress the FATCA XML file with compatible zip utility	FATCAEntitySenderId_Payload.zip
3	Encrypt the FATCA XML file with AES-256 key	FATCAEntitySenderId_Payload
4	Encrypt AES key with public key of each recipient For Model 1, Option 2 (only). Encrypt AES key with public key of HCTA	FATCAEntityReceiverId_Key HCTAFATCAEntityId_Key
5	Create sender metadata	FATCAEntitySenderId_Metadata.xml
6	Create the transmission file	UTC_FATCAEntitySenderId.zip
7	Transmit the data packet to IDES and receive delivery confirmation	N/A

Table 9 – Overview process to prepare and send a file.

Note: The file name should be the same size and pattern as the standard data elements FATCAEntitySenderId, FATCAEntityReceiverId and HCTAFATCAEntityId and stated in a 19-character GIIN format, such as *000000.00000.TA.840_Payload.xml.*

DRAFT

Process to Prepare and Transmit XML File:

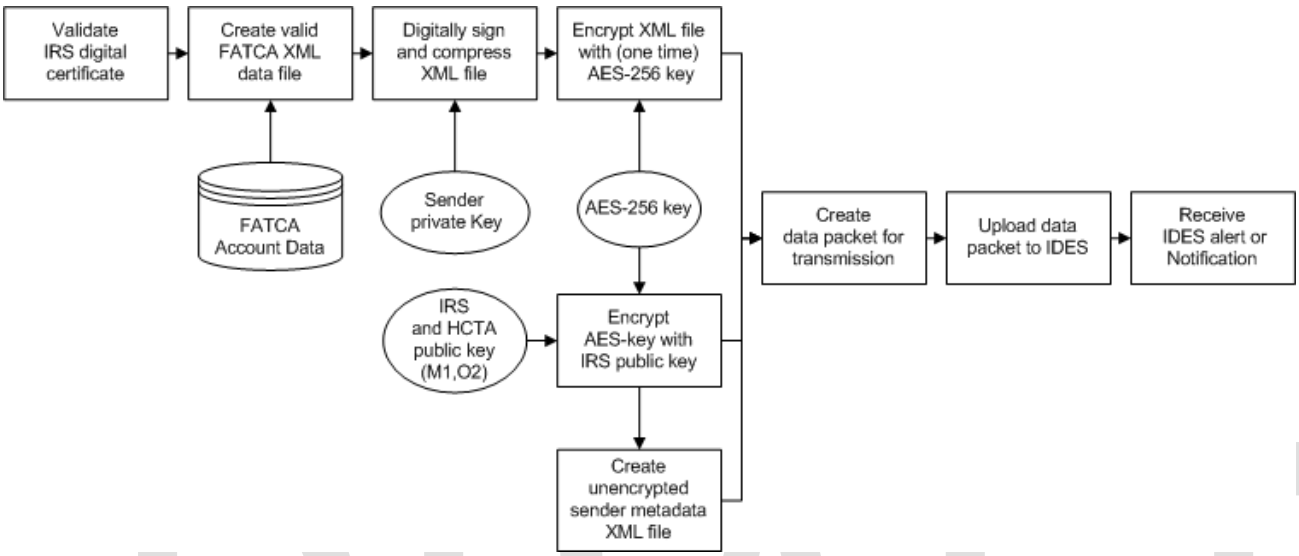


Figure 79 - Data preparation overview

Step 1 - Prepare and Validate the FATCA XML File

Step 1 explains how to create a sender payload file. Each FATCA XML file contains information about the accounts required to be reported under FATCA. Ensure that all XML elements have prefixes, do not use default namespaces. For information on the FATCA XML and related Form 8966 (FATCA Report), see FATCA XML Schemas and Business Rules for Form 8966.

Step 1a - Sign the XML File

Digital signatures are used to assure data integrity, which means that the messages are not altered in transmission. The receiver can verify that the received message is identical to the sent message. A sender uses its private key to digitally sign the message. Senders and recipients of FATCA files will ensure that the file was not corrupted during compression, encryption, and decryption, or altered during transmission to or from IDES.

DRAFT

Sign XML File:

Process	Description	File Naming Convention
Sign XML File	▪ Prepare the FATCA reporting data using XML element prefixes. Do not use the default namespaces. ▪ To generate the digital signature[1], the XML file is processed by a "one-way hashing" algorithm to generate a fixed length message digest. ▪ Depending on the tool used to perform the digital signature, a different type of canonicalization method may be required. The following methods are acceptable: ○ <Canonicalization Method Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/> ○ <Canonicalization Method Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/> ▪ IRS requires that the payload file be signed by first creating a SHA2-256[2] hash. The Sender will then create an RSA digital signature using the 2048-bit private key that corresponds to the public key found in the Sender's digital certificate on IDES. ▪ After validating the schema, digitally sign the FATCA XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition)[3] "*enveloping*" signature. ▪ Use the digital signature "*enveloping*" type. The "enveloped and detached" types will cause the transmission to fail. ▪ The file name is "FATCAEntitySenderId_Payload.xml". The file is case sensitive and any variation in file name or format will cause the transmission to fail.	FATCAEntitySenderId_Payload.xml

Table 10 – Process to digitally sign a file.

Step 2 - Compress the XML File

The XML file "FATCAEntitySenderId_Payload.xml" should be compressed using a compatible compression utility and the standard Deflate compression method.

---

[1] Digital Signature Standard (DSS) (FIPS 186-4), July 2013, nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[2] Secure Hash Standard (SHS) (FIPS 180-4), March 2012, csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[3] XML Signature Syntax and Processing (Second Edition), June 2008, http://www.w3.org/TR/xmldsig-core/

DRAFT

Tools	Version	Host System
WinZip	17.5	Windows
7-Zip	9.2	Windows or Linux
Windows built-in zip utility	N/A	Windows
Linux/Unix standard zip utility	N/A	Linux/Unix
Apple built-in archive utility	MAC OS X 10.3 and later	MAC

Table 11- Recommended compression tools based on compression testing and supported algorithms.

Compress XML File:

Process	Descriptions	File Naming Convention
Compress XML File	▪ The compressed file "zip" is the file extension used by the compression tool or library. ▪ Other tools may be used but the compression method must be recognized by one of the five tools or libraries for the file to be successfully processed.	FATCAEntitySenderId_Payload.zip
Summary	▪ If the file is not recognized or processing fails, the file will be rejected. The sending partner will receive a notification that explains the reason for the transmission failure and how to modify and resubmit the file. ▪ The file name is "FATCAEntitySenderId_Payload.zip". The file is case sensitive and any variation in file name or format will cause the transmission to fail. ▪ Note: The current supported compression is ZIP compression using the standard Deflate compression method.	N/A

Table 12 – Process to compress a file.

Step 3 - Encrypt the XML File with AES 256 Key

AES is one of the most secure encryption algorithms and the preferred encryption standard for IDES. The file is encrypted to protect FI and taxpayer sensitive information.

DRAFT

Encrypt XML File with AES Key:

Process	Descriptions	File Naming Convention
Encrypt XML File	▪ After compression, encrypt the file "FATCAEntitySenderId_ Payload.zip" using the AES-256 cipher with a randomly generated "one-time use" AES key. ▪ While performing AES encryption, there are several settings and options depending on the tool used to perform encryption. IRS recommended settings should be used to maintain compatibility: o Cipher Mode: ECB (Electronic Code Book). o Salt: No salt value o Initialization Vector: No Initialization Vector (IV). If an IV is present, set to all zeros to avoid affecting the encryption. o Key Size: 256 bits / 32 bytes – Key size should be verified and moving the key across operating systems can affect the key size. o Encoding: There can be no special encoding. The file will contain only the raw encrypted bytes. o Padding: PKCS#7 or PKCS#5 ▪ The AES encrypted file name is "FATCAEntitySenderId_Payload". The file is case sensitive and any variation in file name or format will cause the transmission to fail.	FATCAEntitySenderId_Payload

Table 13 – Process to encrypt an XML file with an AES key.

Additional information regarding the AES-256 encryption algorithm and keys can be found in:

1. NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revision 3)
2. Advanced Encryption Standard (FIPS 197), November 2001

Step 4 - Encrypt the AES Key with Public Key of Recipient

The next step is to encrypt the AES key with the public key of each recipient. The file is encrypted to protect the AES key. All FATCA partners must validate the recipient's X.509 Digital Certificate to an approved CA. An X.509 Digital Certificate contains the public key for each FATCA partner, including the IRS, and is retrieved from the IDES Enrollment site.

DRAFT

Encrypt AES Key with Public Key:

Process	Description	File Naming Convention
Validate Certificate	▪ To validate the certificate: 1. Verify the certificate chain; 2. Check the revocation status of the certificate chain. There are two methods: ▪ Retrieve a Certificate Revocation List (CRL) or ▪ Send an Online Certificate Status Protocol (OCSP) query to a CA designated responder	N/A
Encrypt the AES Key	▪ After validating the certificate, use the public key from the recipient's certificate to encrypt the AES 256 key. ▪ The public key encryption uses the standard RSA algorithm. While performing AES encryption, there are several settings and options depending on the tool used. IRS recommended settings should be used to maintain compatibility: ○ Padding: PKCS#1 v1.5 ○ Key Size: 2048 bits ▪ The encrypted file name is "FATCAEntityReceiverId_Key". "FATCAEntityReceiverId" is the 19-character of the recipient of this AES key	FATCAEntityReceiverId_Key
Summary	▪ FATCA reporting with one recipient will have two encrypted files. The files are case sensitive and any variation in file name or format will cause the transmission to fail: 1. Symmetric encryption - the AES 256 encrypted FATCA XML file name is "FATCAEntitySenderId_Payload" 2. Asymmetric encryption - the public key encrypted AES 256 key file name is "FATCAEntityReceiverId_Key"	N/A

Table 14 – Process to encrypt an AES key with a public key.

Note: For most FIs and HCTAs, (e.g., Model 1 (Non-Reciprocal), Model 2 and non-IGA) the IRS is the only recipient.

Step 5 - Encrypt the AES Key – Model 1, Option 2

Under IGA, Model 1, Option 2, an FI submits a FATCA XML file to IDES. The HCTA reviews and releases or denies the file to the IRS. The HCTA and the IRS will decrypt the same FATCA XML file. The FI creates a duplicate of the original AES 256 key. The duplicate AES 256 key is encrypted with the HCTA Public Key.

Encrypt AES Key – Model 1, Option 2:

Process	Description	File Naming Convention
Validate Certificate	▪ See Step 4 – Validate Certificate	
Encrypt the AES Key	▪ After validating the certificate, use the public key from the recipient's certificate to encrypt the AES 256 key. ▪ The encrypted file name should be "FATCAEntityReceiverId_Key". "FATCAEntityReceiverId" is the 19-character GIIN of the recipient of this AES key	FATCAEntityReceiverId_Key

Encrypt the AES Key	▪ Encrypt the AES key with the public key of the approving HCTA ▪ The encrypted file name is “HCTAFATCAEntityId_Key”, where “HCTAFATCAEntityId” is the GIIN of the HCTA recipient of this AES key	HCTAFATCAEntityId_Key
Summary	▪ FATCA reporting with two recipients should have three encrypted files. The files are case sensitive and any variation in file name or format will cause the transmission to fail: 1. Symmetric encryption - the AES 256 encrypted FATCA XML file name is “FATCAEntitySenderId_Payload” 2. Asymmetric encryption - the public key encrypted AES 256 key file name is “FATCAEntityReceiverId_Key” 3. Asymmetric encryption - the public key encrypted AES 256 key file name is “HCTAFATCAEntityId_Key”	N/A

Table 15 – Process for a Model 1 Option 2 FI to encrypt an AES key.

DRAFT

Step 6 - Create Sender Metadata File

Users can create a sender metadata file to ensure that recipients accurately process FATCA XML files and notifications. Notifications are responses sent by the IRS to an FI or HCTA and state whether the file was processed correctly or contained errors.

A template metadata file is available in XML format as part of the enrollment process. FIs and HCTAs can use the template to create a metadata file to attach to the payload before uploading to IDES.
The FATCA Sender Metadata XML file is created using the FATCA Metadata XML Schema v1.0 and the file name is “FATCAEntitySenderId_Metadata.xml.” All FATCA partners must provide the values for the elements in the sender metadata file. For more information, review the FATCA Metadata XML Schema v1.0 User Guide.

Elements	Length	Description
FATCAEntitySenderId	N/A	FATCA partner that submits data
FATCAEntityReceiverId	N/A	FATCA partner receives data
FATCAEntCommunicationTypeCd	N/A	Indicates the transmission type **RPT = FATCA Report communication** NTF = FATCA Notification communication
SenderFileId	200	References the user provided transmission filename
FileCreateTs	N/A	References timestamp created by the sender transmission
TaxYear	4	Indicates the tax year (YYYY format)
FileRevisionInd	1	Indicates if this is a revised transmission
OriginalIDESTransmissionId	32	IDES Transmission ID referencing an update to an

		earlier transmission Optional – Use only after IRS request
SenderContactEmailAddressTxt	N/A	Sender email address

Table 16 - Sender Metadata Schema summarizes each element.

Note: The sender metadata file is never encrypted because it is used to verify and route transmissions to the correct recipient.

DRAFT

Step 7 - Create a FATCA Data Packet

A file that is transmitted through IDES is known as a *FATCA data packet* or *data packet*. The data packet is an archive in .ZIP file format, and it should be created using one of the compatible data compression tools described in Table 3. IDES only supports data packets in a .ZIP file format with a .zip file extension. The files are case sensitive and any variation in the file name or format will cause the transmission to fail.

Data Packet File Archive:

Model 1, Option 2 (Only) Attach 4 Files	All Others Models (1 and 2) Attach 3 Files
▪ FATCAEntitySenderId_Metadata.xml	▪ FATCAEntitySenderId_Metadata.xml
▪ FATCAEntityReceiverId_Key	▪ FATCAEntityReceiverId_Key
▪ HCTAFATCAEntityId_Key	▪ FATCAEntitySenderId_Payload
▪ FATCAEntitySenderId_Payload	

Table 17 – Files contained in a transmission archive or data packet.

The file naming convention of data packet is composed of a Coordinated Universal Time (UTC) timestamp and the GIIN of the sender (FATCAEntitySenderId) as:

UTC_FATCAEntitySenderId.zip

The timestamp format of the UTC is YYYYMMDDTHHMMSSmsZ where:

YYYY = 4-digit year
MM = 2-digit month
DD = 2-digit day
HH = 24-hour
MM = 2-digit minutes
SS = 2-digit seconds
ms = 3-digit milliseconds

For example, a sender with a FATCAEntitySenderId of "000000.00000.TA.<ISO>" that transmits a data packet on January 15, 2015 at 16:30:45 can create a data packet named as:

20150115T163045123Z_000000.00000.TA.840.zip

Step 8 - Transmit Data Packet using IDES

After the archive is uploaded and transmitted, IDES sends an alert to the authorized user via email. The message provides status information about the file upload. If the upload and IDES file checks are successful, IDES assigns a unique "TransmissionID" in the email. If there is an error, the IDES alert provides an appropriate error code in the email message.

DRAFT

9.3. Receive an IRS Notification

A notification is a transmission archive or data packet that contains encrypted documents sent from the IRS to an FI or HCTA. When the IRS sends a notification, IDES sends an email to the authorized user stating that a file is ready for download. Generally, a file will be available for 7 days. See Section 2.6 File Retention Policy for more information. The email correspondence includes the file name of the "TransmissionID" in the original file. Notifications are prepared using the same process and file components used to prepare the FATCA XML.

Users will need to download and unzip the notification message archive. IDES assigns each notification message a file name similar to the FATCA data report, such as UTC_FATCAEntitySenderId.zip. Users can also process the elements contained in the IRS notification.

Note: In a Notification Message, the FATCAEntitySenderId is the IRS and FATCAEntityReceiverId is either the HCTA or FI.

Steps	Process	File Naming Convention
1.	Validate the sender metadata file using the IRS Sender Metadata schema.	FATCAEntitySenderId_Metadata.xml
2.	Use your private key to decrypt the FATCAEntityReceiverId_Key file	FATCAEntityReceiverId_Key HCTAFATCAEntityId_Key
3.	Use the revealed AES key to decrypt the FATCAEntitySenderId_Payload.	FATCAEntitySenderId_Payload
4.	Decompress the FATCAEntitySenderId_Payload.zip	FATCAEntitySenderId_Payload.zip FATCAEntitySenderId_Payload.xml
5.	Validate "Enveloping" Digital Signature of the Notification XML file (the Payload).	N/A
6.	Validate the Notification XML file using the IRS notification schema.	N/A

Table 18- Process to open a notification message archive.

DRAFT

10. Access the IDES Gateway

10.1. Overview

The IDES Gateway is a web application that allows enrolled HCTAs and FIs to securely upload and download FATCA data over the Internet using three methods:

- A manual process through a secure web browser at https://www.idesgateway.com.
- An automated process through SFTP for scheduled bulk file transmissions. See Section 11.7, Transmit a File Using SFTP.
- A link on the IDES Enrollment home page.

1. Connect to IDES using https://www.idesgateway.com

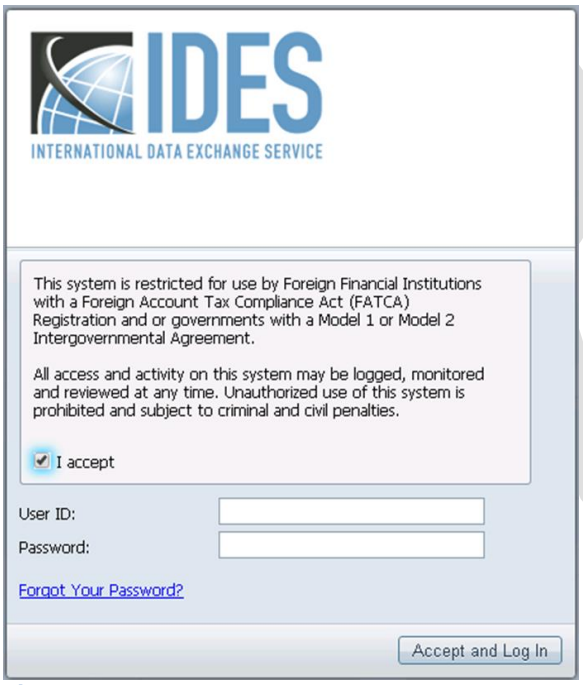


Figure 80 - IDES Gateway Log In Screen.

2. The URL directs you to the **IDES Log in** screen. An authorized session begins.

   Note: Only users that completed the enrollment process are authorized to access the system. For information on enrollment, see IDES Enrollment section.

3. Select the **I accept** box.
4. In **User ID**, enter the username selected during the enrollment process.
   a. If you are an HCTA, type the user name provided by the IRS or contact your local Competent Authority for more information.
5. In **Password** field, enter the password and click **Accept and Log In** to continue.

   Note: The system automatically locks the IDES account after three unsuccessful login attempts.

DRAFT

10.2. Reset Password

1. If the login is unsuccessful after three attempts or you have forgotten your password, you may be required to reset your password.
2. On the **Log in** screen, click **Forgot Your Password?** to go to IDES help desk support. If you fail to change your password within 90 days, your account will be automatically deactivated.

10.3. Session Timeout

An IDES Gateway session will time out after 15 minutes of inactivity. Users will need to return to the Login Page to begin a new session.

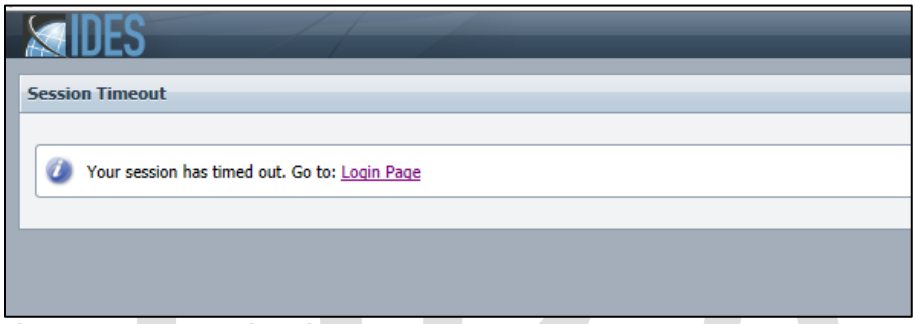


Figure 81 - IDES Session Timeout message.

1. Select **Login Page** to enter a user name and password.

10.4. User Interface Overview

The following links and features make it easy to navigate the IDES Gateway. User access levels and allowable transaction types will depend on IGA Model and the type of user. IDES automatically associates a user type and IGA Model.

DRAFT

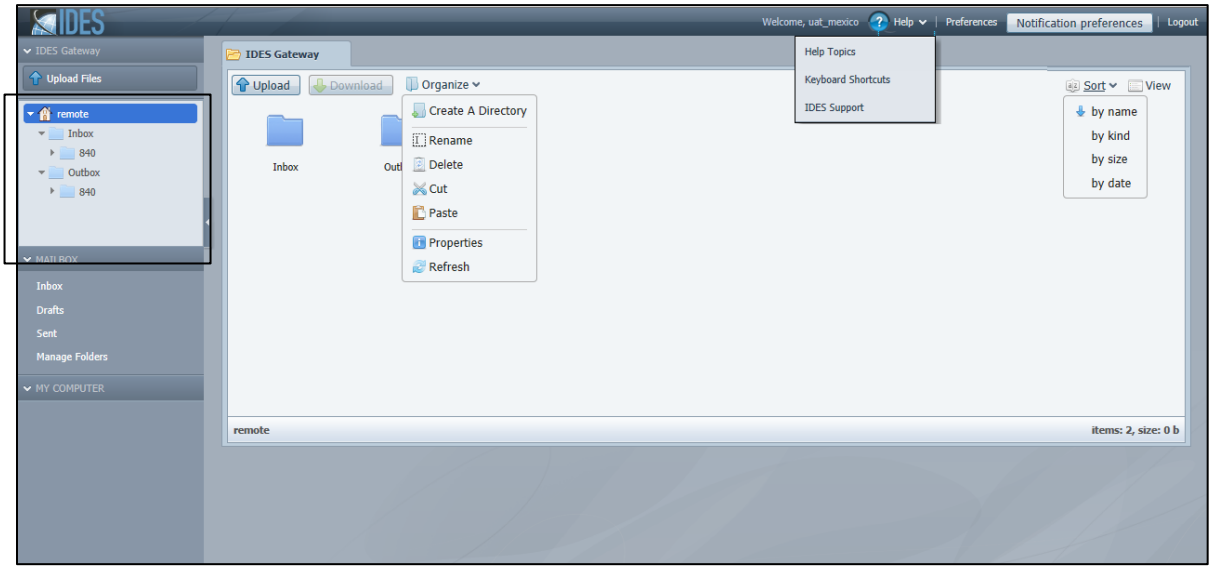


Figure 82 - IDES Gateway home screen.

DRAFT

User Interface	Description
Upload Files/Remote:	
▪ Inbox	Download files and notifications from IDES. Data packets can be downloaded and saved to your computer hard drive.
▪ Outbox	Upload a transmission archive or data packet to IDES. IDES only accepts transmission archives with .zip extension.
▪ Pending	Applies to countries under IGA Model 1, Option 2 HCTA only.
Upload Button	Transmits files from the Outbox to the receiver. For example, select **Upload** to move files from the Outbox to the receiver (U.S.). Note: For Model 1, Option 2, **Upload** is disabled.
Download Button	Transmits files from the Inbox to the user's computer. For example, select **Download** to move files from the Inbox to your computer.
Mailbox:	
▪ Inbox	Messages are received and stored.
▪ Drafts	Messages that have not yet been sent.
▪ Sent	Messages that have been sent.
▪ Manage Folders	Displays all mailbox options in the workspace.
My Computer	Provides access to your computer hard drive.
Workspace	View files and transmission status.
Organize Button	Functions such as cut, delete, and properties, which enable file navigation and commands.
Help Menu	Access to online help, shortcuts, and the IDES help desk.
Accessibility (not shown)	View transmission transfer history through IDES Sentinel Reporting.

Preferences	Change a password and/or select the file transfer mode (Binary or ASCII).
Alert Preferences	Select alerts and specify maximum number of alerts per day. The default is all alerts.
Sort	Sort files by name, kind, size, and date.
View	View files by folder icons or by list.
Logout	End the IDES Gateway session.

Table 19- IDES User Interface Overview.

DRAFT

10.5. Global Preferences

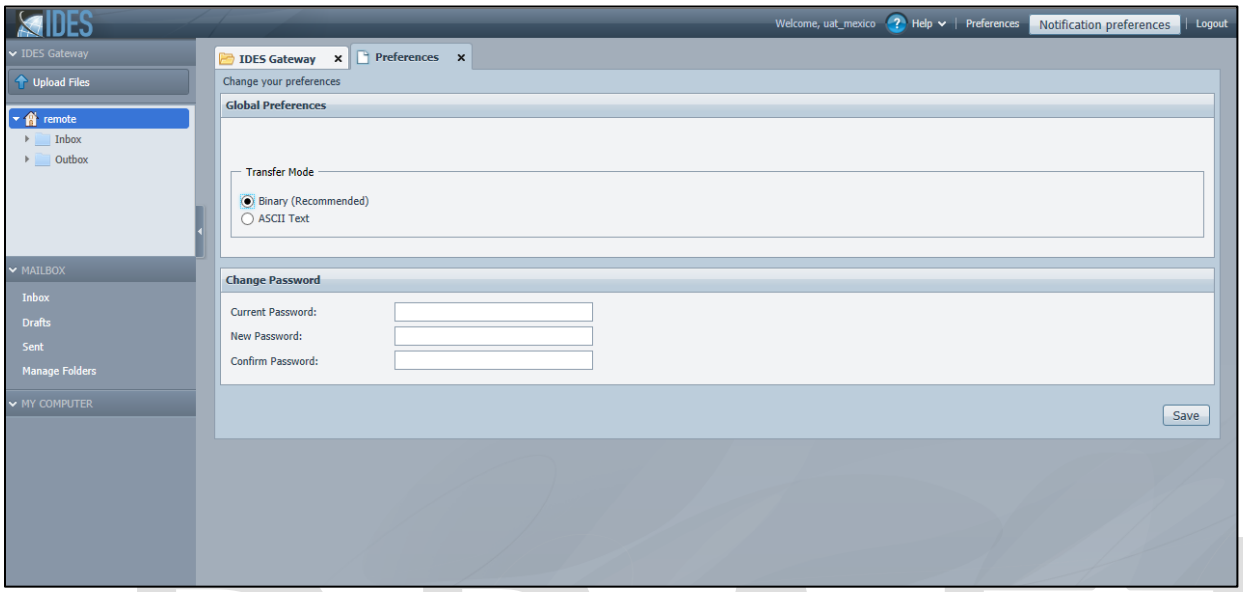


Figure 83 – Select global preferences.

1. On **IDES Gateway** home screen, select **Preferences**.
2. Under **Transfer Mode**, select **Binary** or **ASCII Text.**

Note: Binary mode is the recommend default.

To Change Password:

1. In **Current Password**, enter the current password.
2. In **New Password**, enter the new password and in **Confirm Password**, re-enter the new password.
3. Select **Save.**

Note: The same password will apply to both the enrollment site and IDES Gateway. Any changes to a user password will automatically apply to both sites.

Expired Passwords: Use the **Change Password** option to update passwords. The IDES account will expire if you fail to change the password every 90 days. The **Change Password** option cannot be used if the password has expired. To update an expired password, go to the IDES Enrollment site or contact the IDES help desk. Note that users will use the same password to access both the enrollment site and the IDES Gateway.

DRAFT

10.6. Alert Preferences

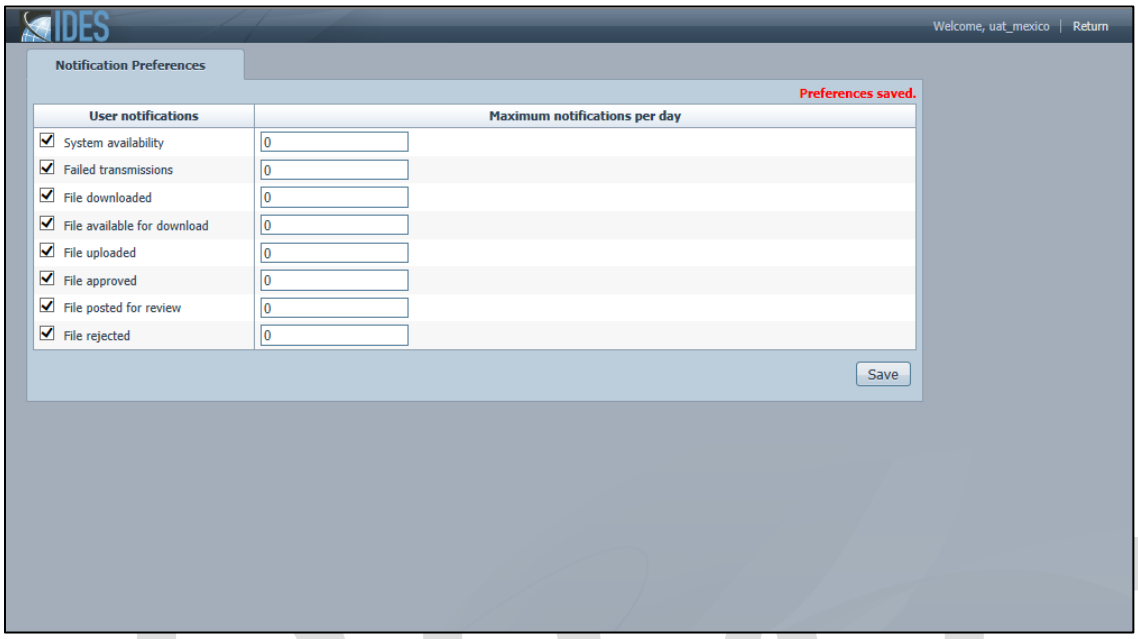


Figure 84 – Set alert preferences

1. In **User alerts**, select or deselect the appropriate box.
2. In **Maximum alerts per day**, enter the maximum number of alerts to be received each day. If left blank, you will receive all alerts.
3. Select **Save, Preferences saved** appears.
4. Select **Return**.

Note: Modifications to alert preferences will supersede alert preferences set during enrollment

11. Transmit a FATCA Report

11.1. IDES Transmission Archive

IDES only accepts transmission archives or data packets with the .zip extension. Most archives will contain a minimum of 3 or 4 files. Data packets that are not in .zip format will be automatically deleted. The sender will receive an alert that the file has been deleted. Note that this alert, as well as other transmission-related alerts will be sent directly to the user that transmitted the data, and will not be sent to all users enrolled under the FI or HCTA. Alert details will be stored and may be viewed by all authorized users via IDES Sentinel Reporting.

An FI under a Model 1, Option 2 IGA does not transmit FATCA reporting data directly to IRS. The FI uploads and transmits files to their HCTA. The HCTA will download the files and approve or reject the transmission to the IRS. An HCTA can only approve or reject files located in the pending folders, and cannot make any changes to the files. An HCTA must upload files with a .zip and '*accepted'* or '*rejected'* extension. Any data packets that do not adhere to the file format will be automatically deleted.

DRAFT

11.2. IDES Transmission ID

An IDES Transmission ID is created when a data packet is transmitted to the IRS. The transmission ID is a unique 32 character-length number that identifies the transmission. This transmission ID will be included in both IDES system alerts and notifications generated by the IRS. File transmission IDs for all transmissions can also be viewed through the IDES Sentinel Web Monitoring (Sentinel) platform. The original transmission ID is an element in the metadata schema and can help to monitor and track a specific message. For example: <ISO>F-weXu2uKAh-UjuL8V6QPEN2IlJgX, represents the ID for a file sent by an HCTA.

11.3. Retransmissions

Retransmissions are FATCA reports that have been revised and re-sent. The FATCA metadata file identifies the revision with the <FileRevisionInd> element and recognizes the original transmission using the <OriginalIDESTransmissionId> element. The <OriginalIDESTransmissionId> element helps IDES link the new transmission to the original transmission.

11.4. Folder Structure

The IDES folder directory structure is based on the ISO-3166 standard three-digit country code. Sub-directories are automatically created based on the entity GIIN and/or ISO country code. FI and HCTA administrators and end users have the same access to the home directory and other folders. Each HCTA will have sub-folders under its country code folder. For Model 1 Option 2, each FI under the HCTA will be listed as a sub-folder under the country code folder.

Example: After HCTA login, the IDES Gateway home page shows access to two folders and subdirectories:

Inbox/840 (US)	Files from the U.S./recipient available for download
Outbox/840 (US)	Files to the U.S. or recipient available for upload
Pending/HCTA (ISO)* Model 1, Option 2	Files from FI are pending approval or rejection
	If approved, then files are routed to the U.S.
	If rejected, then files are automatically deleted

Table 20 – IDES Gateway folders and subdirectories.

Note: All users of the same entity (FI or HCTA) will have the same access rights, and can see transmissions made by other users of the same FI or HCTA. There are no shared folders between all IDES users, and no controls to stop users from uploading files from the same entity.

DRAFT

11.5. Transmit a File Using Web UI

11.5.1. Upload a File

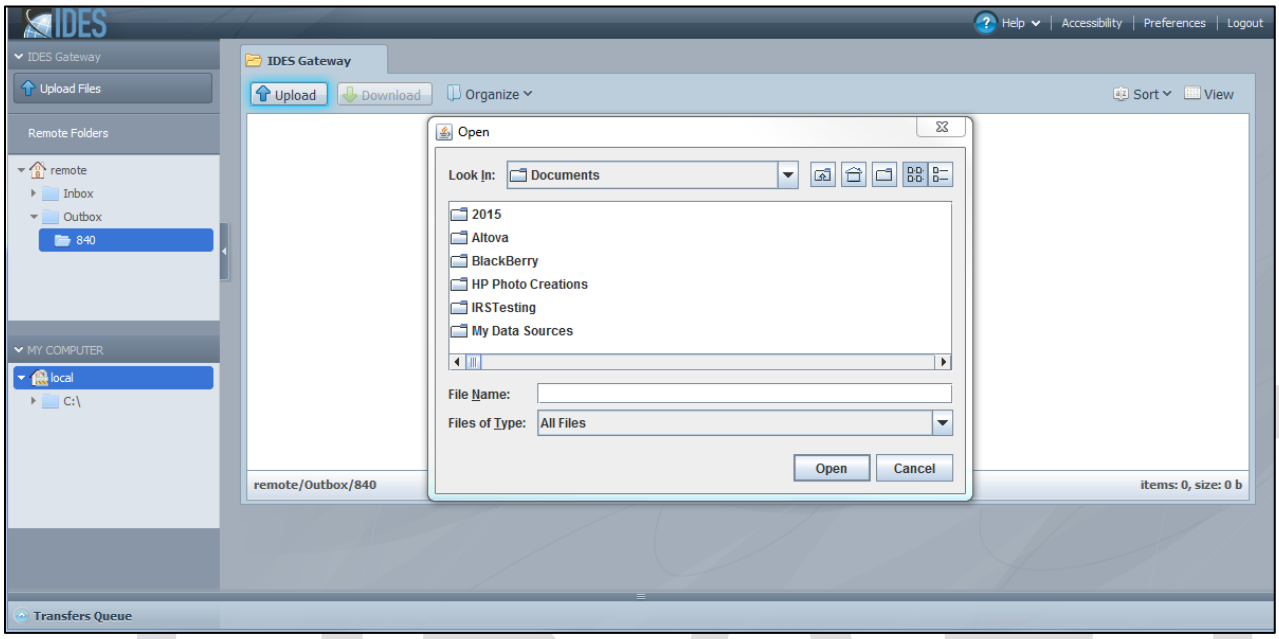


Figure 85 - Select and upload files.

1. On the **IDES Gateway** home page, select the **Outbox** and click on folder **840**.
2. Click **Upload** and a dialog box appears that allows you to select files.
3. Select the file(s) and click **Open**. The file transfer process begins.
4. View the **Transfers Queue** at the bottom of the screen. The files are then moved from the sender **Outbox** to the receiver.

DRAFT

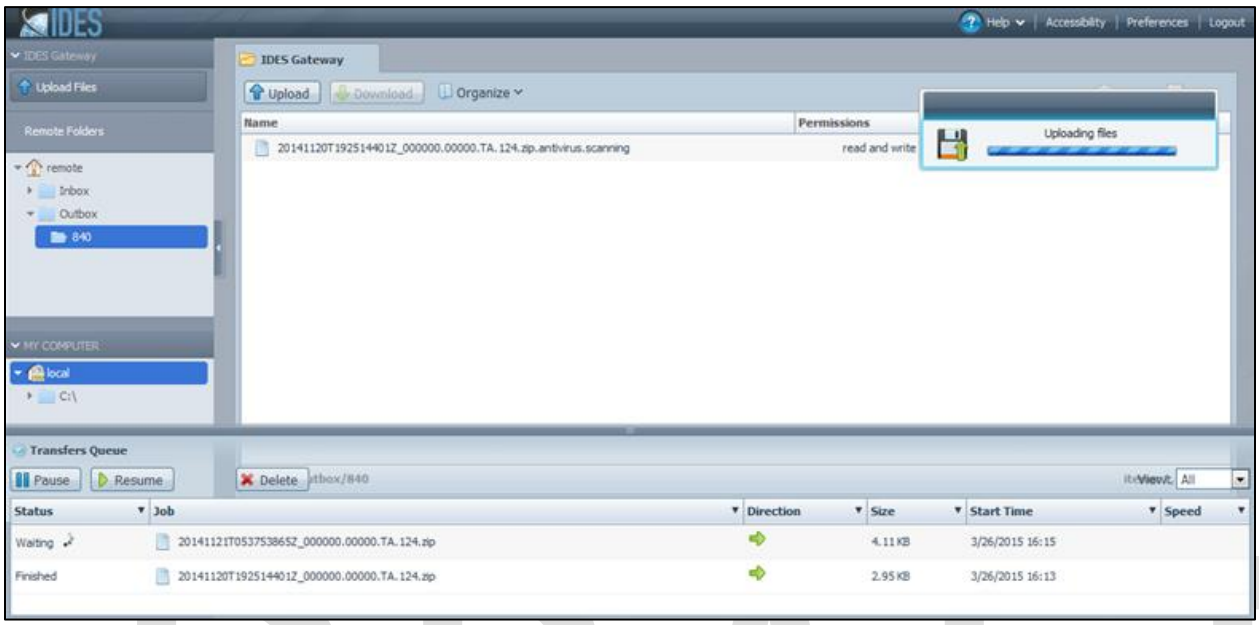


Figure 86 - View file transfer status in Transfers Queue.

5. After the uploaded files are transmitted from the **Outbox,** the status appears at the bottom of the screen in the **Transfers Queue.**

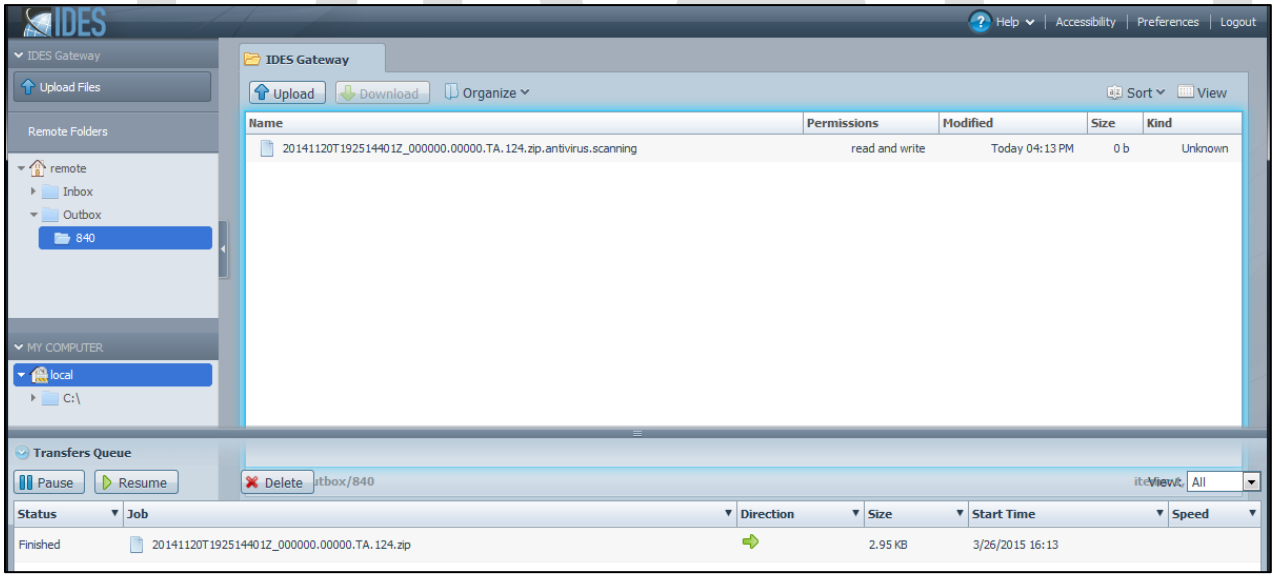


Figure 87 - Temporary file and transfer status

6. In addition to the transfer queue status, a temporary file displays to confirm successful transfer. Uploads are transmitted to the receiver.
7. The files are routed based on the sender and recipient elements defined in the unencrypted FATCA Metadata XML file or file name<Sender>GIIN_Metdata.xml. The elements in the metadata schema <FATCAEntitySenderId> and <FATCAReceiverId> identify the sender and receiver. See Create Sender Metadata File for more information.

11.5.2. Download a File

Recipients will receive an email alert when files are available to download. To select Alert Preferences settings, see Chapter 10. Global Preferences.

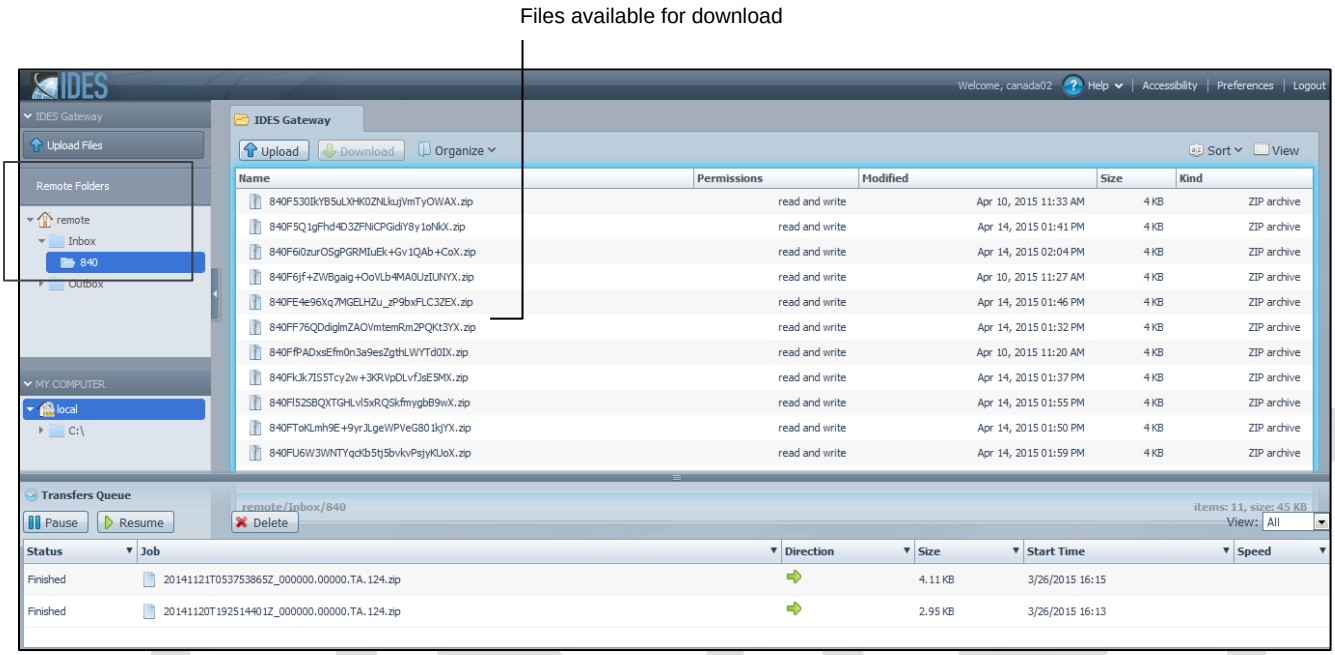


Figure 88- IDES file download screen.

1. On the **IDES Gateway** main page, navigate to **Inbox** and click on **840 (United States)** to view files available for download.

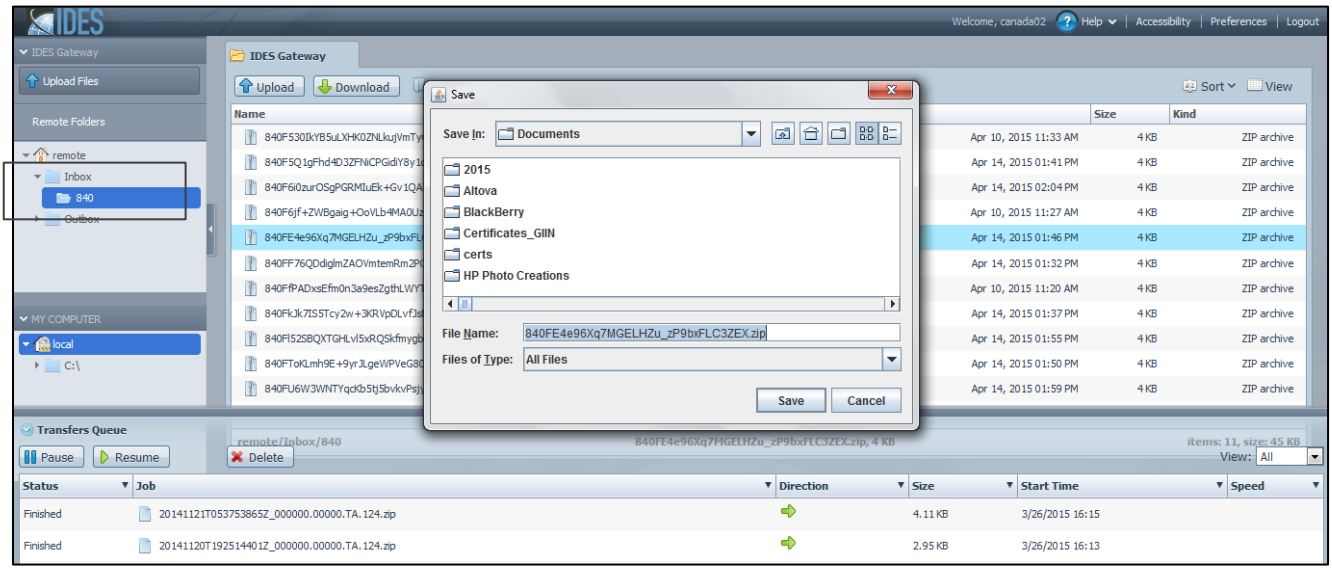


Figure 89 – Save a file.

2. Select the file and click **Download**.
3. Drag and drop the file to hard drives listed under the **My Computer** section, or right click the filename and select **Save As.**
4. View **Transfers Queue** at the bottom of the screen to show the file status. The files have been moved from the **Inbox** to the hard drive.

11.6. Model 1, Option 2 HCTA

FIs under Model 1, Option 2 may only transmit files to their HCTA. After logging in, the FI should follow normal procedures to upload and transmit files to their HCTA. Once a file is transmitted, the HCTA will receive an IDES alert indicating that files are available in the HCTA's Pending folder for download and review. Once reviewed, HCTAs should rename the files as either ".accepted" or ".rejected" and upload the files to the US.

FI upload a file:

1. On the **IDES Gateway** home page, select the **Outbox** and click on folder **840**.
2. Click **Upload** and a dialog box appears that allows you to select one or many files.
3. Select the file(s) and click **Open**. The file transfer process begins.
4. View the **Transfers Queue** at the bottom of the screen. The files are then moved from the sender **Outbox** to the pending folder for retrieval by the HCTA.

HCTA download and verify a file:

1. On the **IDES Gateway** home page, select the **Inbox** and click on folder **Pending**. The folder displays a list of files available for download.
2. The HCTA file transfer screen displays three folders and subdirectories:
   a. **Inbox:** Files from the US are available for download
   b. **Outbox:** Files to the US (840) may be uploaded
   c. **Pending:** Files from an FI are available for download. An HCTA cannot upload files to the Pending folder. Files from the Pending folder are renamed with the file extension of ".accepted" or ".rejected".

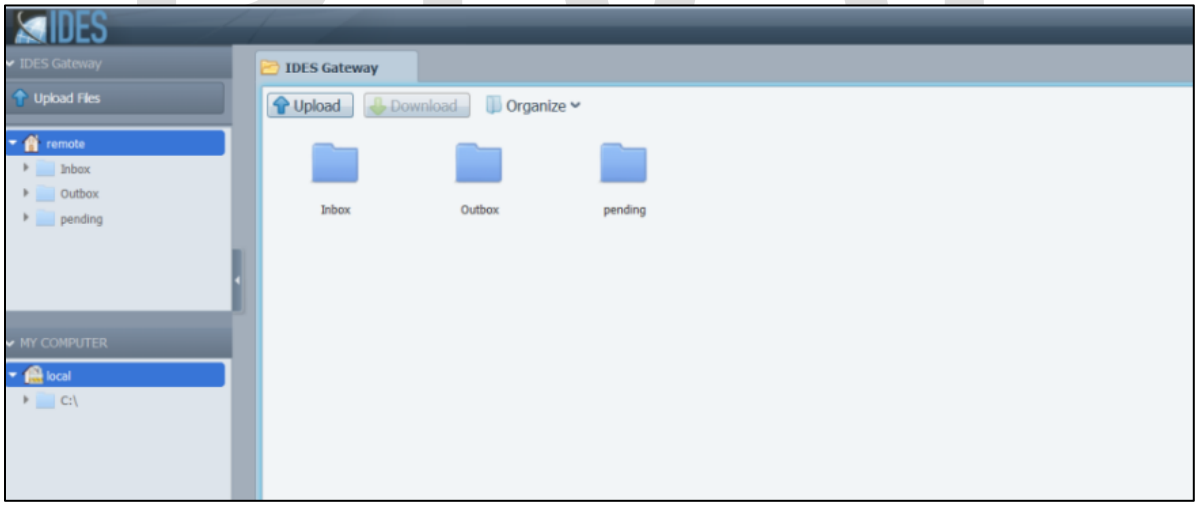


Figure 90 - Model 1 Option 2 Folder Structure

DRAFT

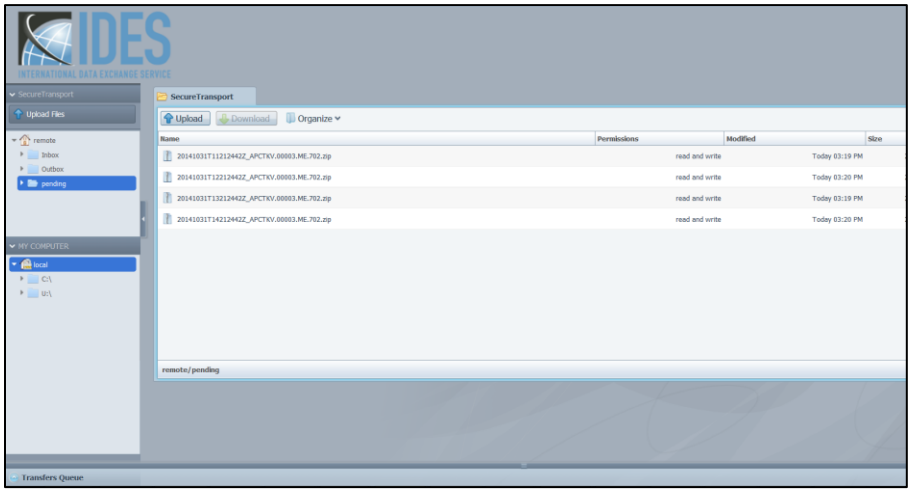


Figure 91 - IDES Pending status folder.

3. Select a file and click **Download** or drag and drop the file to your computer. The HCTA will review the files to determine whether to approve or reject.

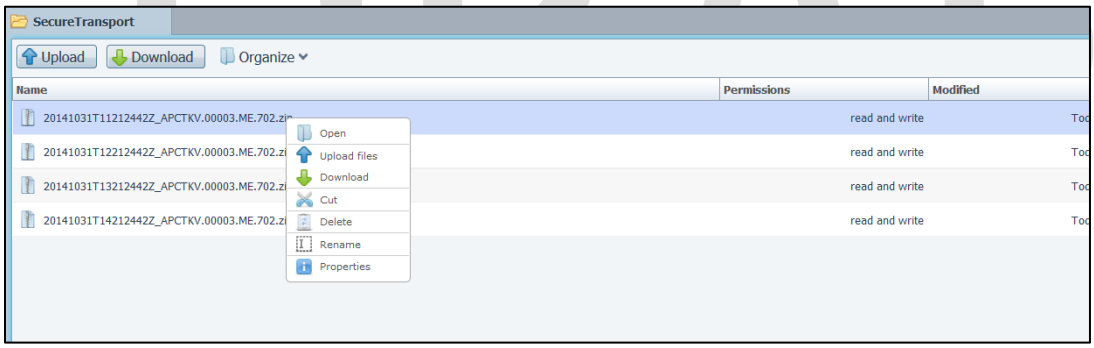


Figure 92 – IDES file options.

4. After the files are reviewed, select the file and right click, then select **Rename**. An HCTA may only rename and transmit an archive or data packet. An HCTA cannot upload files to the **Pending** folder.
5. Rename a file as either filename.zip.accepted or filename.zip.rejected. The filenames are case sensitive and any variation in name, extension or format may cause a transmission failure.

   After a file is renamed:
   - If the file is approved, the file is routed to the US (840) and alerts/notifications are distributed
   - If the file is rejected, the file is automatically deleted and alerts/notification are distributed

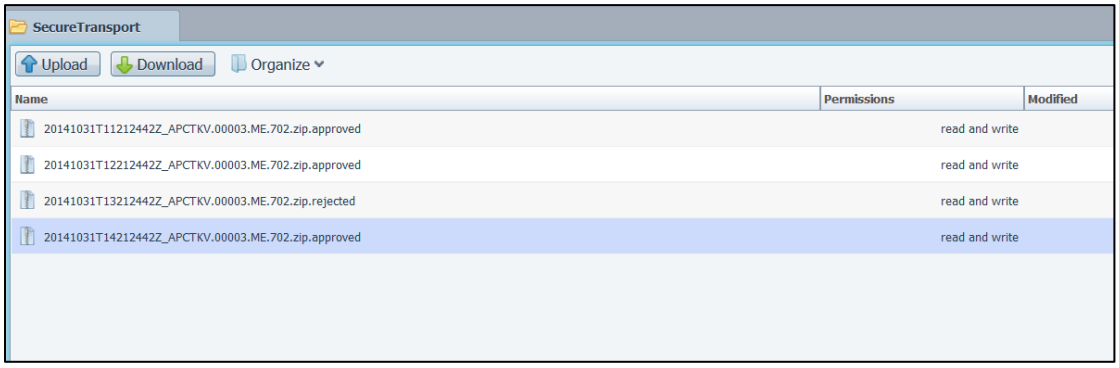


Figure 93 - IDES rename file options.

9. Approved files should be sent to the IRS and rejected files are automatically deleted.

Note: IDES only accepts .zip files with .accepted or .rejected file extensions. Files in pending status after seven (7) days will be automatically rejected and/or deleted.

Step	Description
1.	User connects to IDES and uploads a .zip transmission archive or data packet into the Outbox 840 or 702.
2.	The transmission is routed to a **«Pending»** folder in the HCTA account based on the HCTA IGA Model and data elements in the unencrypted FATCA metadata. The transmission is renamed using the IDES unique Transmission ID as the file name.
3.	An approver (HCTA user account) downloads the file from the **«Pending»** folder and reviews the file. The HCTA has 7 days to review the files. All files in the Pending folder exceeding 7 days will be deleted.
4.	The approver (HCTA user account) renames the file to either ***<filename>*.approved** or ***<filename>*.rejected**. IDES files that do not match the format will be automatically rejected and deleted from the system.
5.	The files matching pattern ***.rejected** are pulled from the system and deleted.
6.	The files matching the ***.approved** are routed according to their destination to the US. (3 first characters of the file name).
7.	If a file remains in the **«Pending»** folder and is not renamed either to **<filename>.approved** or **<filename>.rejected** for 7 days, it will be automatically rejected. IDES runs a scheduled process to automatically rename such files to ***<filename>*.rejected**

Table 21 – Summary description of IDES reporting process for Model 1 Option 2 HCTAs.

DRAFT

11.7. Transmit a File Using SFTP

The IDES SFTP Server provides users with secure access to manage and transfer files between hosts over a network. IDES SFTP authenticates using your username and password. The DNS name must be used for the connection.

The SFTP connection methods shown provide a general overview of the process. You may have a different SFTP configuration and operating system. Please use one of the recommended SSH Client tools. Depending on the configuration, your organization may need to adjust network confirmation (firewall) settings to provide connectivity. Contact your information technology specialist for assistance with accessing IDES using SFTP.

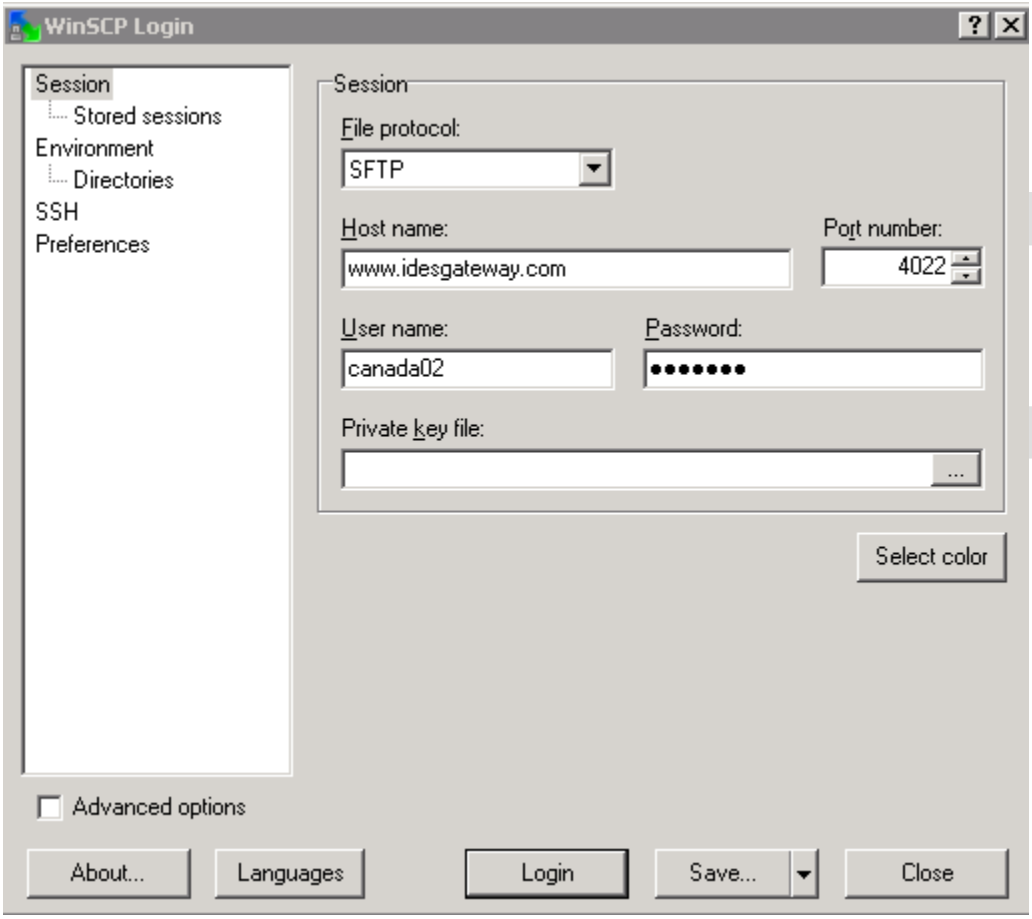


Figure 94 - Sample SFTP connection.

11.8. Connect to IDES SFTP using Windows Secure Copy (WinSCP):

1. Open your SFTP client. Your SFTP client may have different settings than the one shown as an example.
2. In SFTP **Host name**, enter https://www.idesgateway.com. The following IP addresses should be exposed (no firewall restrictions) to send and receive files.
    a. Port: 4022
    b. External IP address:
        - 54.172.126.52
        - 54.172.215.70

3. When you connect using SSH, you may see an authentication screen. Click **Continue.**

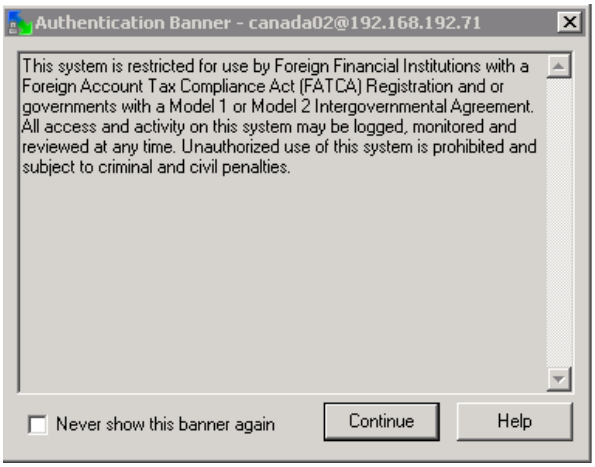


Figure 95 - SSH Authentication Disclaimer.

4. In **User name**, enter the user name selected during the enrollment process.
    a. If HCTA, type the user name provided by the IRS or contact your local Competent Authority for more information.

5. In **Password**, enter your password and click **Login**.

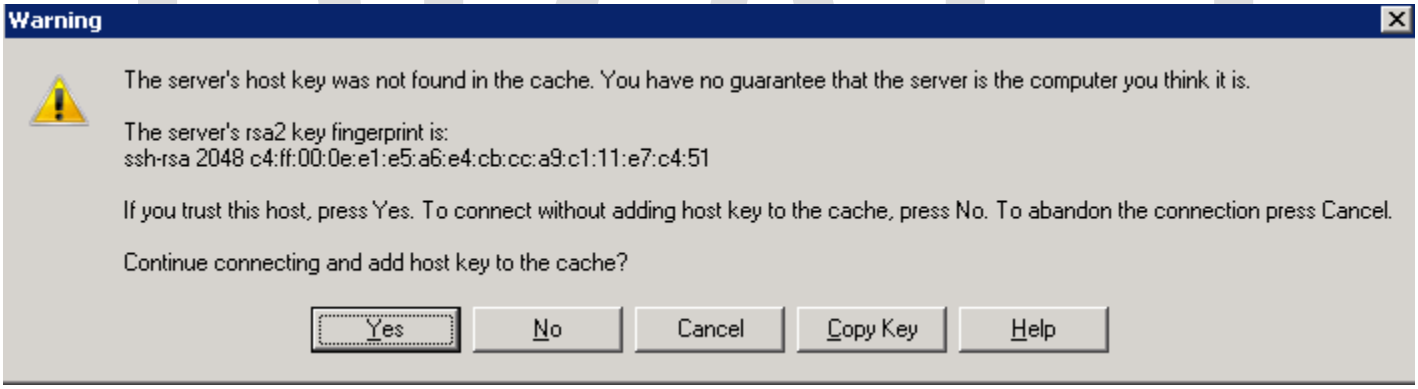


Figure 96- SFTP Warning Dialog.

6. You may be prompted with a **Warning** message about the server's secure key.
7. Click **Yes** to accept the key and continue.

DRAFT

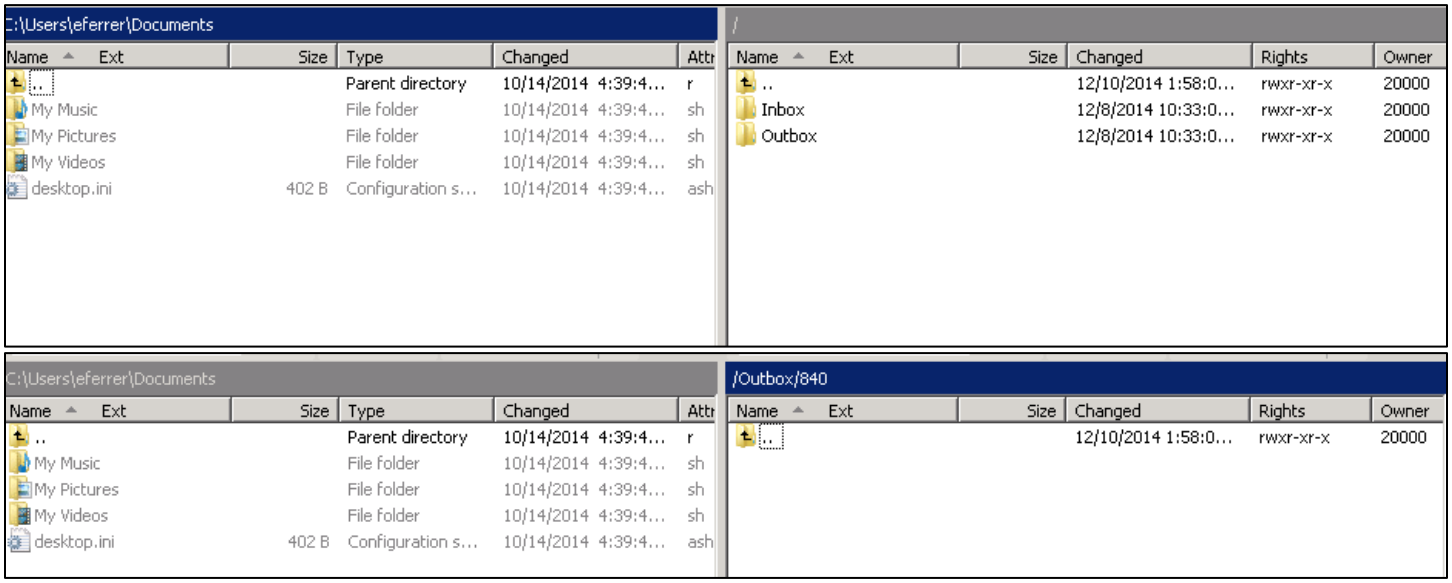


Figure 97 – SFTP Connection.

DRAFT

8. You will see your local computer directories on the left pane and the IDES home folders and subfolders in the right pane. See Folder Structure, for more information.
   - Navigate to Inbox/840 to download files from the US.
   - Navigate to Outbox/840 to upload files to the US.

9. SSH transfers: Do not attempt to upload a file using a temporary file name and then rename the file. Some tools attempt to rename files automatically.
   a. If using WinSCP: Uploads will fail if WinSCP is configured to upload files such as *<filename>.filepart*. This configuration option should be disabled via the following steps:
      - Navigate to WinSCP > Preferences > Endurance -> "Enable transfer resume / transfer to temporary filename for"
      - Disable the above option

Note: IDES SFTP supports password authentication. You will generate a SSH key pair, install the private key in the client software certificate store, and upload the public key to a special folder in your SFTP utility user account. The IDES account will expire if you fail to change the password every 90 days. To update an expired password, go to the IDES Enrollment site or contact IDES help desk support.

12. Alerts

12.1. Overview

IDES issues email alerts via unsecured, plain-text email to all users based on user preference settings. The IDES Alert contains information about the transmission processing and does not contain any personally identifiable information. IDES Alerts are sent to both the sender and receiver immediately after the transmission is processed in IDES. All transmissions are scanned for virus, encryption, and mandatory elements in the metadata XML file. If a transmission fails the validation checks, the transmission will be deleted. The sender receives an IDES Alert email and is required to resubmit the

transmission for processing. The history of all alerts is available online in Sentinel and can be viewed through a secure web browser.

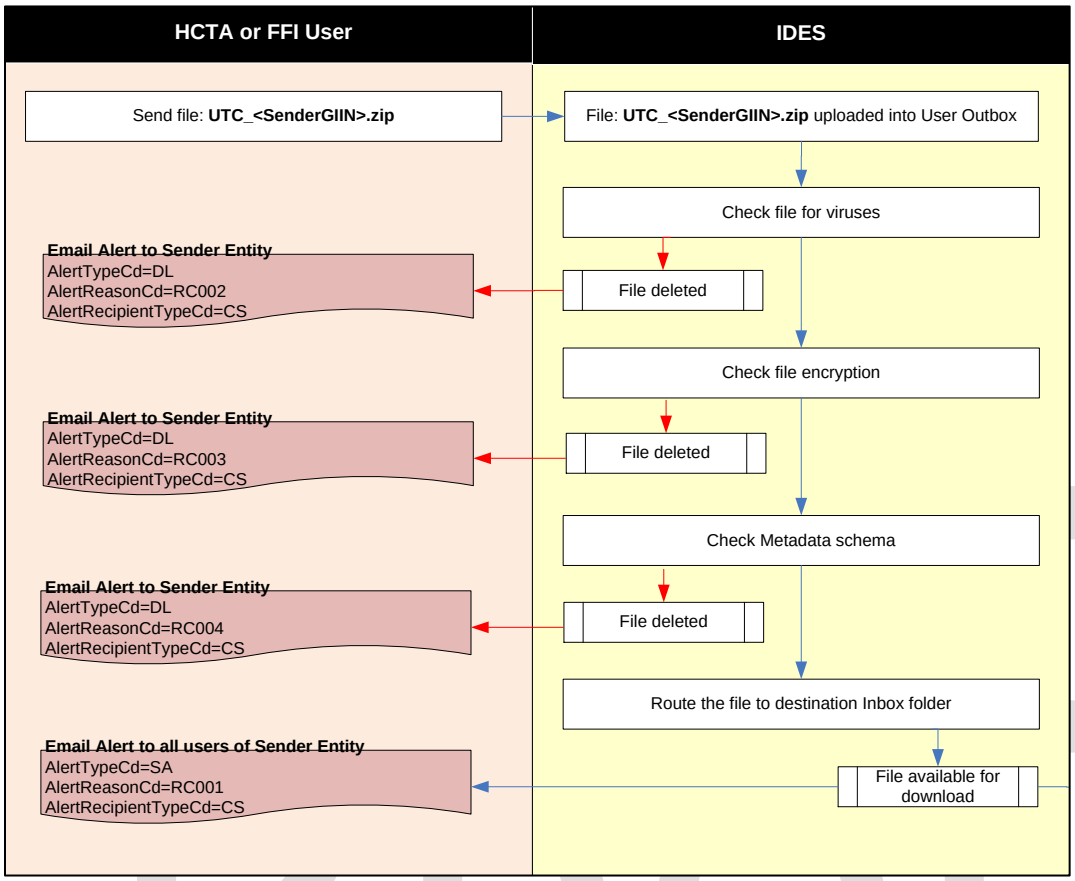


Figure 98 – IDES Alert flow chart for transmission uploads.

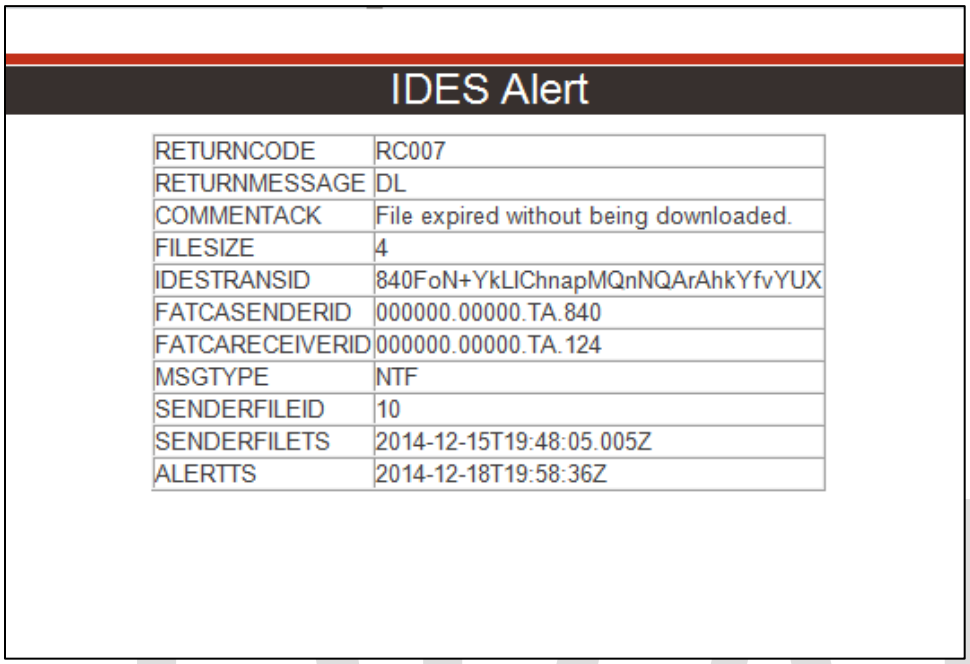
12.2. Receive Alerts

See Alert Preferences, for more information on configuring IDES Alerts.

The IDES Alert email message will come from a unique address: alerts@idesgateway.com. The message contains the following:

- IDES unique transmission ID
- User-specified file name/ID
- User-specified sending application timestamp
- From (Sender)
- To (Receiver)
- Message Type (payload type)
- Sending Date/Time Timestamp
- Alert Date/Time Timestamp
- Alert Code (transmission status)

From: alerts@idesgateway.com
To: Receiver email address
Subject: IDES – Alert for a Transmission



IDES Alert

RETURNCODE	RC007
RETURNMESSAGE	DL
COMMENTACK	File expired without being downloaded.
FILESIZE	4
IDESTRANSID	840FoN+YkLIChnapMQnNQArAhkYfvYUX
FATCASENDERID	000000.00000.TA.840
FATCARECEIVERID	000000.00000.TA.124
MSGTYPE	NTF
SENDERFILEID	10
SENDERFILETS	2014-12-15T19:48:05.005Z
ALERTTS	2014-12-18T19:58:36Z

Figure 99 - Sample IDES Alert e-mail message.

Note: If a transmission fails processing, it will be automatically deleted. When a transmission fails to upload, only partial elements are available in the alert message because the metadata file could not be processed. The transmission archive must be corrected and resubmitted.

DRAFT

13. IDES Reports

13.1. IDES Sentinel Web Monitoring

IDES Sentinel Web Monitoring provides monitoring and reporting for all transmissions on a record-by-record basis. Sentinel will correlate the events and store multiple data records that describe the end-to-end flow of every file transferred using IDES. Users can query the system for all events and search, filter and view the transmission history. Sentinel's monitoring features allow the user to:

- Execute and filter predefined queries to analyze the data in the repository based on specific parameters.
- Retrieve historical information about alerts and notifications.

Note: All users enrolled with IDES can access Sentinel through IDES Gateway or IDES Sentinel Web Monitoring. FI and HCTA users can view the alert and transfer history of all uploaded files and notifications that pertain to their entity only.

13.1. System Timeout

A session expires after 15 minutes of inactivity. When a session expires, the login window will appear.

13.2. Accessibility

To connect to Sentinel through IDES Gateway:

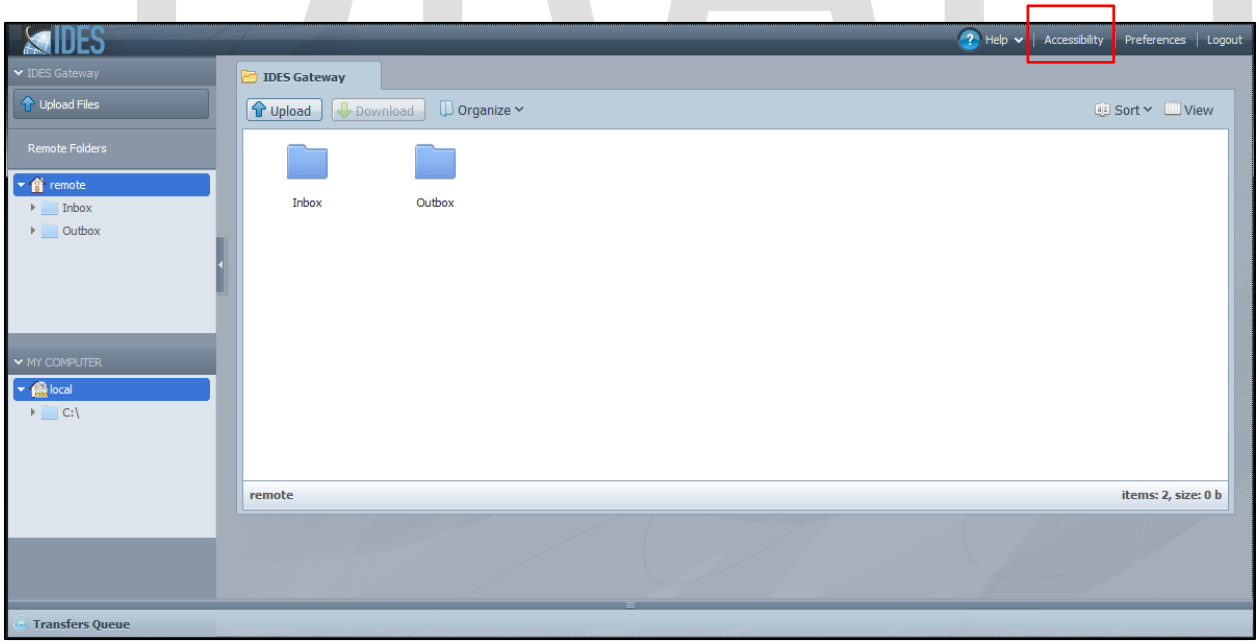


Figure 100 - IDES home page

DRAFT

1. From the **IDES Home Page**, select **Accessibility** to view keyboard shortcut options. Use the following keyboard shortcuts to access your transmission history.

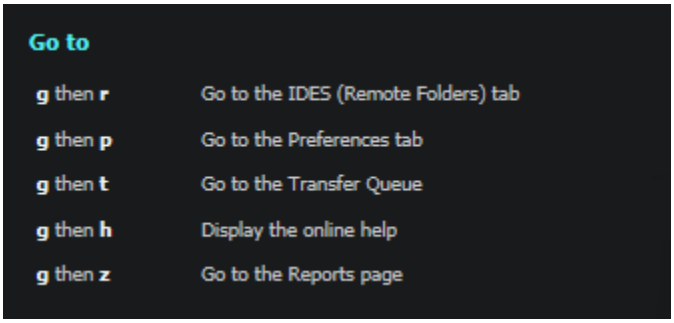


Figure 101 - Accessibility keyboard shortcuts

2. You are re-directed to [https://visibility.idesgateway.com.](https://visibility.idesgateway.com)
3. On the **Search** tab, select the **Status** and/or **Time Period** drop down menu to filter and retrieve the transmission transfer history for your entity.

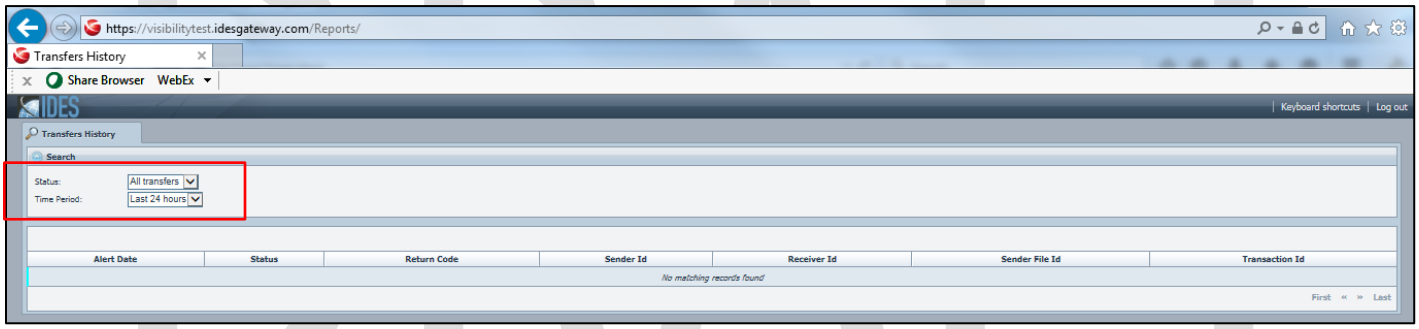


Figure 102 - IDES Accessibility Home Page

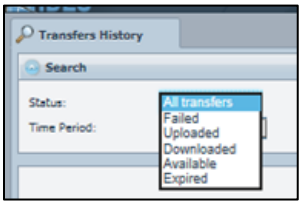
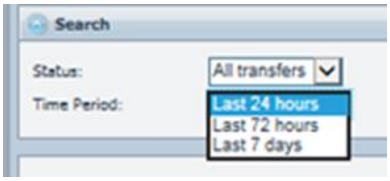


Figure 103 - IDES transfer history Search options



DRAFT

Status:	Time Period:
▪ Failed transmissions	▪ Last 24 hours
▪ Uploaded	▪ Last 72 hours
▪ Downloaded	▪ Last 7 days
▪ Available	
▪ Expired	

4. View the report **Results**. The transfer history is read only and the report may not be saved or exported. Refer to Section 13.8. Save Report, to view how to save reports in other formats.

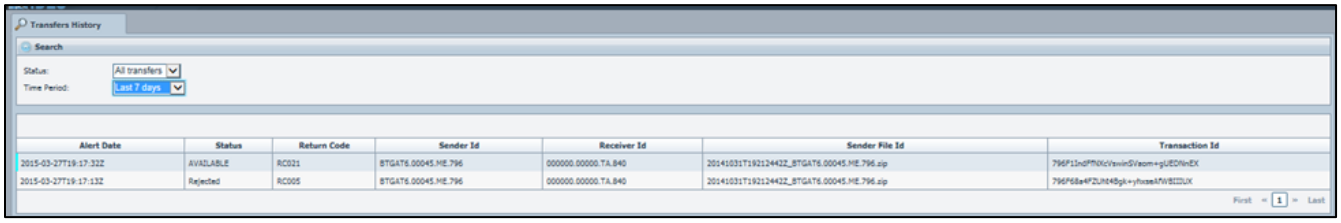


Figure 104 - IDES Accessibility transfer history results

DRAFT

13.5 Connect to IDES Sentinel Monitoring using web browser

To connect to Sentinel Monitoring, use your web client and enter the URL in a standard browser.

1. Open browser
2. Go to the Sentinel URL: https://visibility.idesgateway.com.
3. The Disclaimer screen displays. Click **OK** to continue.

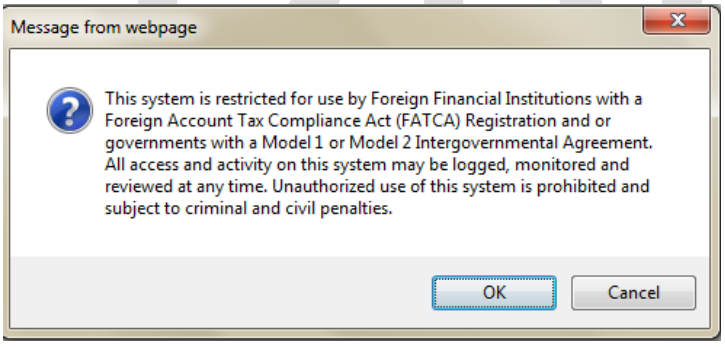


Figure 105 - Disclaimer Screen.

4. If you select **Cancel,** you are redirected to the IDES Enrollment site. **Note**: Only users that have completed the enrollment process are authorized to access the system.

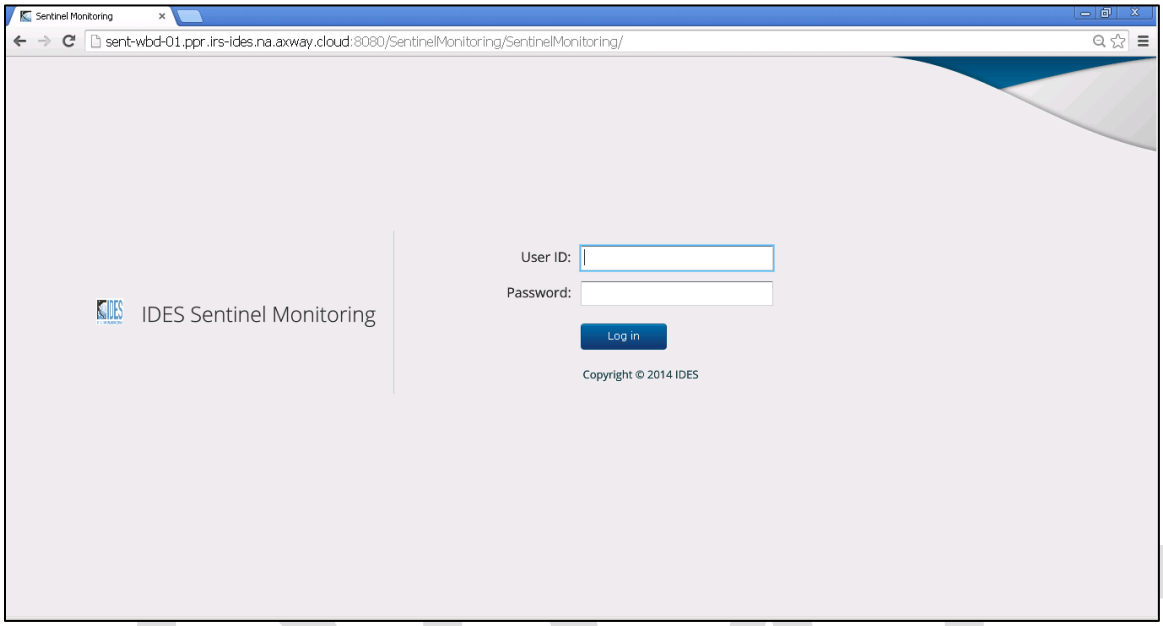


Figure 106 - IDES Sentinel Login Screen.

5. In **User ID**, enter your IDES user name.
6. In **Password**, enter the password and click **Log In** to continue to the **IDES Sentinel Monitoring** home page. IDES Sentinel is user name and password authenticated and only authorized users may access the system.

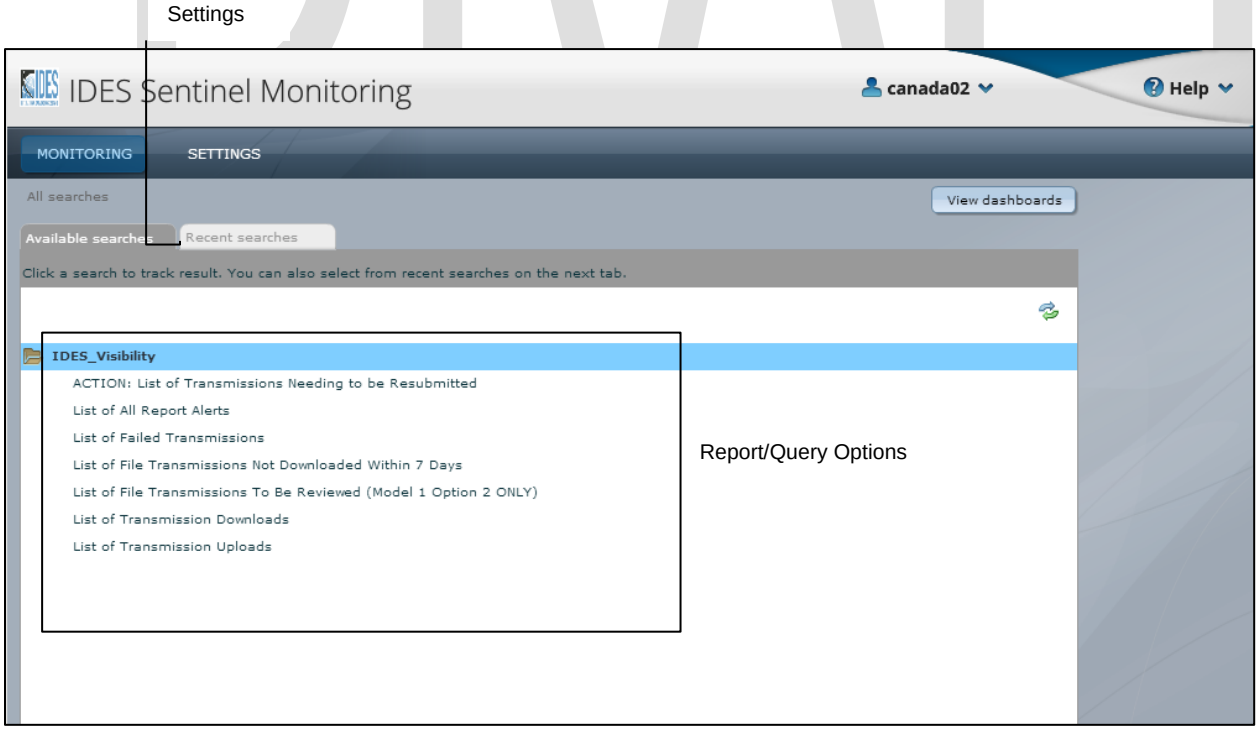


Figure 107 – IDES Sentinel Monitoring home screen

The Sentinel Monitoring home page provides a list of available reports and allows you to filter based on search parameters.

13.5 Search Options and Report Summary

IDES Sentinel Monitoring will include a set of predefined reports that will be available to all authorized users of a given FI or HCTA.

Report / Query	Description
List of Transmission to be Resubmitted	Shows all transmissions that need additional investigation. Users may be contacted by the IDES Helpdesk to retransmit
List of All Report Alerts	Shows all alerts for the FI or HCTA.
List of Failed Transmissions	Shows all failed uploads and downloads for the FI or HCTA.
List of File Transmission Not Downloaded Within 7 Days	Shows all expired notification files that were created by the IRS and made available to the FI or HCTA, but were not downloaded in the 7 day window.
List of File Transmissions To Be Reviewed (Model 1 Option 2 only)	Shows all file uploads by the FI that are waiting for the HCTA to review.
List of Transmission Downloads	Lists all successful downloads for the FI or HCTA.
List of Transmission Uploads	Lists all successful uploads for the FI or HCTA.

Table 22 - Summary of available reports

DRAFT

13.6 Search Transmission and Alert History

On a monthly basis, alerts, notifications, and reports will be stored in an electronic file format such as CSV or PDF. Alerts will be available online for 90 days and then archived. An FFI or HCTA with various end users can only view the alert history of files and notifications that pertain to their entity. If you need assistance retrieving historical account information, contact IDES help desk support.

An advanced filter will be available only to search the alerts based on the following attributes and parameters.

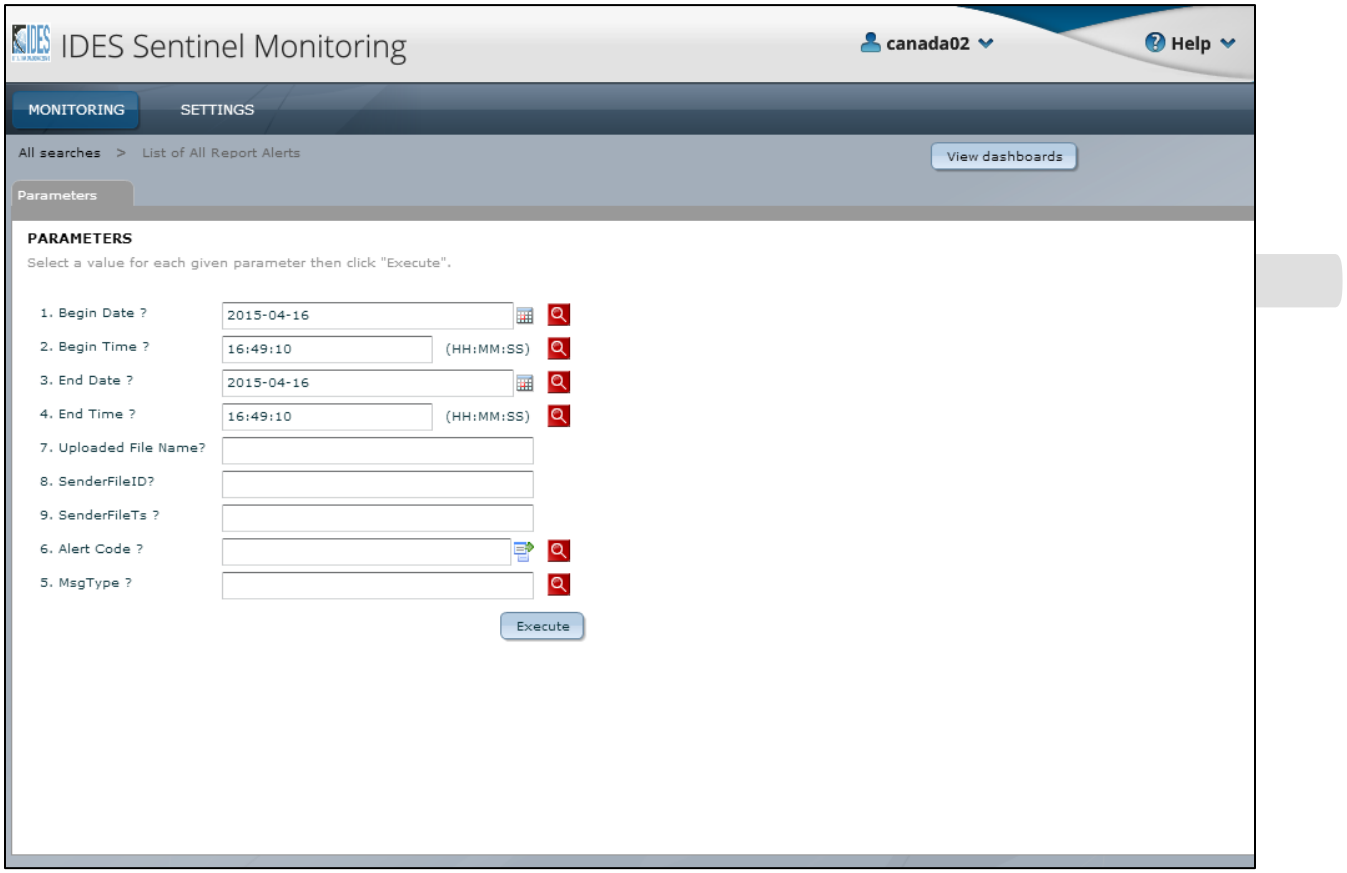


Figure 108 - IDES Sentinel search parameters.

To search:

1. Click the **Monitoring** button, select from the tab of **Available** searches (default) or **Recent Searches**. Double click on an item from the list of available reports shown in **Figure 107**.
2. The **Parameters** tab appears and displays several selections. Place your cursor over the item to show additional descriptions.
   - Transmission date and time
   - Uploaded file name
   - Sender file ID (as set in the metadata file)
   - Sender file TimeStamp (as set in the metadata file)
   - Transmission message type
   - Alert code

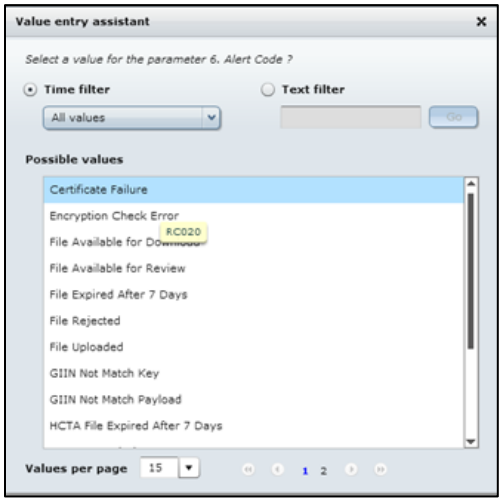


Figure 109 - Search parameter for alert codes

3. Enter a value for one or many parameters, or leave the fields blank to see all records.
4. Click to browse the list of possible values.
5. Click **Execute** to begin the search.

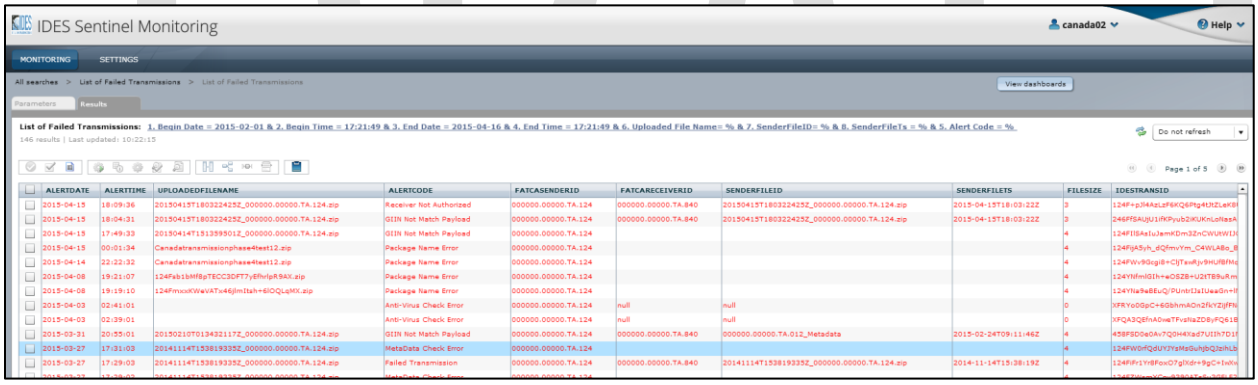


Figure 110 - IDES Sentinel search results.

6. The query results may extend over more than one page and returns a table with the following attributes:

- IDES alert Date/Time: The UTC timestamp.
- Uploaded file name
- Alert code: The reason for the alert or notification.
- Sender and Receiver ID
- File size
- Alert message: The IDES Alert message code. See Appendix E: Types of Alerts for more information.
- IDES Transmission ID: May be used to retransmit a message.

13.7 View Search Results

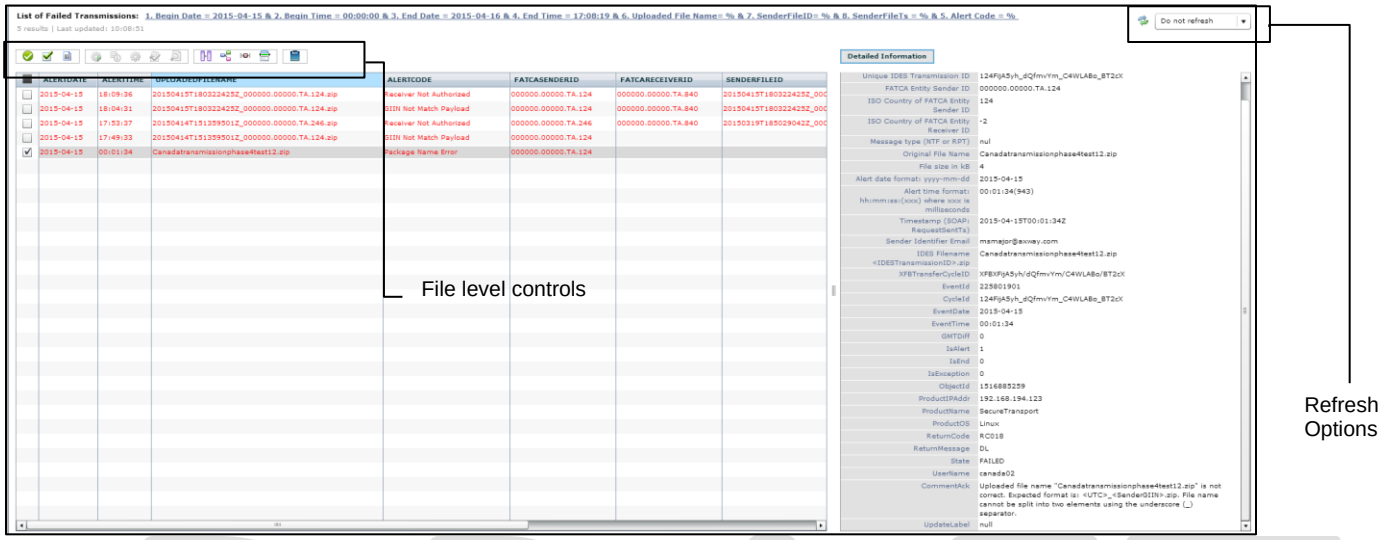


Figure 111 - IDES Sentinel search results screen

1. In the **Results** tab, select a search result and click the icon to view details.
2. The detailed information appears on the right of the search results table.
3. To return to the search results without displaying the detailed information, unselect the current search result.
4. If the search results extend over more than one page, use the following navigation features:

To display the next page

To display the previous page

To display the last page

To display the first page

5. Select the **checkbox** for each file to display a **Detailed Information** dialog box. At the bottom of the details box, you can view, more information under **"CommentAck".**

ReturnCode	RC018
ReturnMessage	DL
State	FAILED
UserName	canada02
CommentAck	Uploaded file name "Canadatransmissionphase4test12.zip" is not correct. Expected format is: <UTC>_<SenderGIIN>.zip. File name cannot be split into two elements using the underscore (_) separator.

e

Figure 112 - Detailed information dialog box

6. Deselect the **checkbox** to return to the search results.

DRAFT

13.8 Save Search Reports

IDES Sentinel Reports can be saved in many formats. The report generation will help users organize and monitor transmissions. For security reasons, a session expires by default after 15 minutes of inactivity.

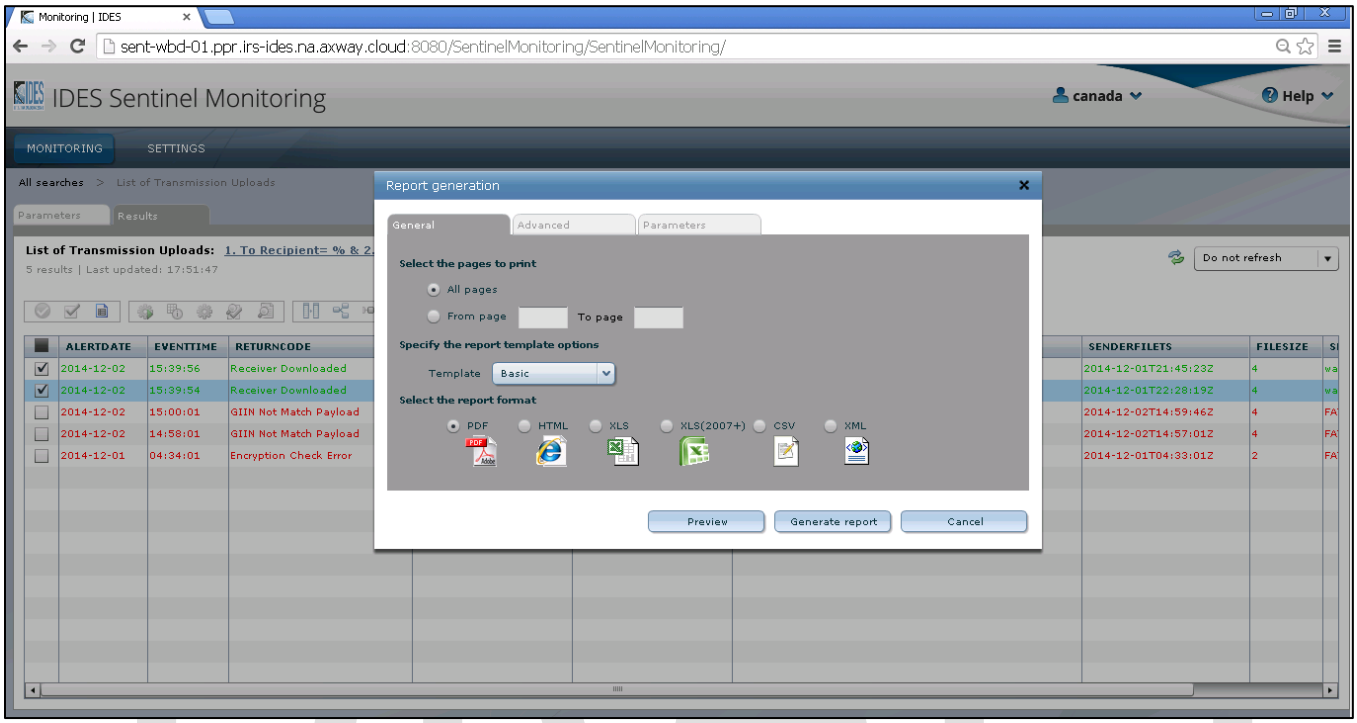


Figure 113 - IDES Sentinel Report Generator.

1. Select the report to save and click the box to the left of the **Report Name**.
2. Click the **Generate Report** icon.
3. A **Report generation** dialog box appears. The dialog box has three tabs, **General, Advanced,** and **Parameters**.
4. On the **General Tab**, select the following:
    a. **Pages to print:** Select radio button for all pages or enter the page range.
    b. **Report template options:** Click dropdown box and select Basic or Advanced.
    c. **Report format:** Select radio button for PDF, HTML, XLS, CSV or XML.
5. Click one of the following options:
    a. **Preview: Preview the report in** the selected report format.
    b. **Generate Report: Create a report and save it anywhere you choose**
    c. **Cancel: Cancel your selections**.

Appendix A: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
FATCA	Foreign Account Tax Compliance Act
FCPA	Federal Common Policy Root CA
FFI	Foreign Financial Institution
FI	Financial Institution
FTP	File Transfer Protocol
GIIN	Global Intermediary Identification Number
HCTA	Host Country Tax Authority
HTTPS	Hypertext Transfer Protocol Secure
IDES	International Data Exchange Service
IGA	Intergovernmental Agreement
IRS	Internal Revenue Service
NFFE	Non-Financial Foreign Entity
NTF	Notification Communication
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced eMail
PKI	Public Key Infrastructure
PMO	Project Management Office
RPT	FATCA Report Communication
RSA	Rivest, Shamir and Adleman

DRAFT

SFTP	Secure File Transfer Protocol
SSH	Secure Shell
TFI	Territory Financial Institution
TIEA	Tax Information Exchange Agreement
TLS	Transport Layer Security
USWA	United States Withholding Agents
UTC	Coordinated Universal Time
XML	Extensible Markup Language

Table 23 – Table of acronyms used in this document.

DRAFT

Appendix B: File Naming Convention

File Name	Description	Associated IGA Group
FATCAEntitySenderId_Payload	Encrypted payload using a randomly generated one-time use key (preference: AES-256)	All
FATCAEntityReceiverId_Key	Key encrypted using the receiver public key	All
HCTAFATCAEntityId_Key	Key encrypted using HCTA public key	Model1 Option 2
FATCAEntitySenderId_Metadata.xml	FATCA Metadata to ensure that recipients properly process FATCA XML reports. FATCA Metadata XSD will be published on the IRS website Note: A text version of the FATCA metadata SenderGIIN_Metadata.txt will be accepted for partners not familiar with xml.	N/A
UTC_FATCAEntitySenderId.zip	N/A	N/A

Table 24 – IDES file naming conventions.

DRAFT

Appendix C: Certificate Upload Error Messages

Status	Description
CtlNotSignatureValid	Specifies that the certificate trust list (CTL) contains an invalid signature.
CtlNotTimeValid	Specifies that the certificate trust list (CTL) is not valid because of an invalid time value, such as one that indicates that the CTL has expired.
CtlNotValidForUsage	Specifies that the certificate trust list (CTL) is not valid for this use.
Cyclic	Specifies that the X509 chain could not be built.
HasExcludedNameConstraint	Specifies that the X509 chain is invalid because a certificate has excluded a name constraint.
HasNotDefinedNameConstraint	Specifies that the certificate has an undefined name constraint.
HasNotPermittedNameConstraint	Specifies that the certificate has an impermissible name constraint.
HasNotSupportedNameConstraint	Specifies that the certificate does not have a supported name constraint or has a name constraint that is unsupported.
InvalidBasicConstraints	Specifies that the X509 chain is invalid due to invalid basic constraints.
InvalidExtension	Specifies that the X509 chain is invalid due to an invalid extension.
InvalidNameConstraints	Specifies that the X509 chain is invalid due to invalid name constraints.
InvalidPolicyConstraints	Specifies that the X509 chain is invalid due to invalid policy constraints.
NoError	Specifies that the X509 chain has no errors.
NoIssuanceChainPolicy	Specifies that there is no certificate policy extension in the certificate. This error would occur if a group policy has specified that all certificates must have a certificate policy.
NotSignatureValid	Specifies that the X509 chain is invalid due to an invalid certificate signature.
NotTimeNested	Deprecated. Specifies that the CA (certificate authority) certificate and the issued certificate have validity periods that are not nested. For example, the CA cert can be valid from January 1 to December 1 and the issued certificate from January 2 to December 2, which would mean the validity periods are not nested.
NotTimeValid	Specifies that the X509 chain is not valid due to an invalid time value, such as a value that indicates an expired certificate.

DRAFT

NotValidForUsage	Specifies that the key usage is not valid.
OfflineRevocation	Specifies that the online certificate revocation list (CRL) the X509 chain relies on is currently offline.
PartialChain	Specifies that the X509 chain could not be built up to the root certificate.
RevocationStatusUnknown	Specifies that it is not possible to determine whether the certificate has been revoked. This can be due to the certificate revocation list (CRL) being offline or unavailable.
Revoked	Specifies that the X509 chain is invalid due to a revoked certificate.
UntrustedRoot	Specifies that the X509 chain is invalid due to an untrusted root certificate.

Table 25 – IDES Certificate Upload Error Messages.

.

DRAFT

Appendix D: HCTA FATCA Entity ID Composition

A Global Intermediary Identification Number or GIIN is issued to FIs and direct reporting NFFEs to identify themselves to withholding agents and tax administrations for FATCA reporting.

The GIIN is a 19-character identification number that is a composite of several other identifiers.

In lieu of a GIIN, HCTAs will be issued an HCTA FATCA Entity ID. The HCTA FATCA Entity ID represents each country under an IGA and contains the following identifiers:

Format: **000000.00000.TA.<ISO>**

Characters	Position	Description
000000	1-6	N/a
Separator 1	7	Period =.
00000	8-12	N/A
Separator 2	13	Period =.
TA Category Code	14-15	HCTA = Tax Authority
Separator 3	16	Period =.
XXX Country Identifier	17-19	Numeric ISO 3166-1 numeric standard country code of the Tax Authority

Table 26 – IDES HCTA FATCA Entity ID composition.

DRAFT

Appendix E: Types of Alerts

Note: The list provides an overview of the IDES alert codes you may receive after submitting a transmission archive using IDES. If a transmission is deleted, then the data packet was not transmitted. Review the alert code, correct the transmission archive, and retransmit. If you need assistance, refer to the IDES User Guide, IDES web pages or contact IDES Customer Support.

Code	Reason	Description / Action	To Sender	To Receiver (IRS)	To Reviewer (HCTA)
Type: SA: - Transmission uploaded successfully					
RC001	Successful upload (including all IDES validation checks)	The data packet passed IDES validation and is now available for download by the receiver. No action is required from the sender.	X		
RC029	Successful upload (including all IDES validation checks), waiting for HCTA approval (Model 1 Option 2)	The data packet passed IDES validation checks and is now available for download and approval by the Model 1 Option 2 HCTA. No action is required from the sender.	X		
RC023	Successful upload and approval by the HCTA (Model 1 Option 2)	The data packet passed IDES validation checks and has been approved by the Model 1 Option 2 HCTA. It is now available for download by the receiver. No action is required from the sender.	X		
Type: DL - Transmission deleted					
RC002	Failed virus check in IDES	The data packet failed IDES validation. One or more files in the data packet are infected with malware. If the files are properly encrypted, this likely indicates that the metadata file is the infected file. The sender must perform a complete anti-virus check to clean the data packet and retransmit.	X		
RC003	Failed encryption check in IDES	The data packet failed IDES validation. One or more files in the data packet are not encrypted as required. The sender must encrypt the FATCA XML document and the AES key as required in the data packet and retransmit.	X		

DRAFT

RC004	Failed FATCA Metadata schema check in IDES	The data packet failed IDES validation. The metadata XML document did not validate against the metadata XML schema. The sender must include a valid metadata XML document in the data packet and retransmit.	X		
RC005	Transmission was rejected by the sender's HCTA (Model 1 Option 2)	The data packet passed IDES validation but it was rejected by the Model 1 Option 2 HCTA. The sender must contact the corresponding HCTA directly to address any concerns and retransmit.	X	X	X
RC006	No actions taken by the sender's HCTA (Model 1 Option 2); transmission expired after 7 days	The data packet passed IDES validation but it was not approved by the Model 1 Option 2 HCTA during the 7 day approval window and it has expired. The sender must contact the corresponding HCTA directly to address any concerns and retransmit.	X	X	X
RC007	Transmission ready for receiver to download, but expired after seven (7) days	The data packet passed IDES validation but it was not downloaded by the receiver during the 7 day window and it has expired. The sender should review the FAQs on IRS website or contact the IDES help desk for additional support to address any concerns and retransmit.	X	X	
RC008	Invalid FATCAEntitySenderID or GIIN	The data packet failed IDES validation. The file name of the data packet does not contain a valid FATCAEntitySenderID that is in the correct format. The sender must include a valid FATCAEntitySenderID in the correct format as part of the data packet file name and retransmit.	X		
RC009	Invalid Receiver GIIN	Not used	X		
RC010	Sender not authorized for the Receiver	Not used	X		
RC011	Receiver not authorized for the Sender	Not used	X		

DRAFT

RC012	FATCAEntitySenderID or GIIN does not match the payload or metadata	The data packet failed IDES validation. The FATCAEntitySenderID in the data packet file name does not match the FATCAEntitySenderID in the payload file name and/or metadata file name. The sender must include the same FATCAEntitySenderID across the data packet as required and retransmit.	X		
RC013	Receiver GIIN does not match the key	The data packet failed IDES validation. The data packet contains an invalid receiver key file. The sender must include a valid receiver key file in the data packet as required and retransmit.	X		
RC014	Payload missing	The data packet failed IDES validation. The data packet does not contain a payload file. The sender must include a payload file in the data packet as required and retransmit.	X		
RC015	Key missing	The data packet failed IDES validation. The data packet does not contain an AES key. The sender must include an AES key in the data packet as required and retransmit.	X		
RC016	Approving HCTA key missing (Model 1 Option 2)	The data packet failed IDES validation. The data packet does not contain the Model 1 Option 2 HCTA key. The sender must include the Model 1 Option 2 HCTA key in the data packet as required and retransmit.	X		
RC018	Package filename error	The data packet failed IDES validation. The file name of the data packet does not contain an underscore. The sender must set an underscore as the data packet file name separator and retransmit.	X		
RC019	Metadata missing	The data packet failed IDES validation. The data packet does not contain a metadata file. The sender must include a valid metadata XML document as required and retransmit.	X		

DRAFT

RC020	Invalid certificate	The data packet failed IDES validation. The digital certificate in the data packet is expired, revoked, or invalid. The sender must include a valid certificate from an approved certificate authority as required in the data packet and retransmit.	X		
RC025	Invalid zip package file	The data packet failed IDES validation. The data packet was not archived as required. The sender needs to archive the data packet using a compatible Zip compression tool as required and retransmit.	X		
RC026	Too many files in package	The data packet failed IDES validation. One or more extra files are included in the data packet. The data packet should contain only 3 files (or 4 files in the case of a sender in a Model 1 Option 2 jurisdiction). The sender must include only the required files in the data packet and retransmit.	X		
RC027	Zip package contains a folder	The data packet failed IDES validation. A folder is included in the data packet. The sender must delete the folder and all its contents from the data packet and retransmit.	X		
RC028	Invalid approving HCTA key name (Model 1 Option 2)	The data packet failed IDES validation. The data packet contains an invalid Model 1 Option 2 HCTA key. The sender must include a valid Model 1 Option 2 HCTA key in the data packet as required and retransmit.	X		
Type: RD - Transmission available for download					
RC021	Available for receiver to download (Model 1 Option 2)	The data packet passed IDES validation and is now available for download by the receiver. No action is required from the sender.		X	

DRAFT

RC022	Available for HCTA review (Model 1 Option 2)	The data packet passed IDES validation and is now available for download by the Model 1 Option 2 HCTA for review. No action is required from the sender. The Model 1 Option 2 may download and review the data packet from the Pending folder.	X		X
Type: SA - Transmission downloaded					
RC024	Downloaded by the receiver	The data packet passed IDES validation and was downloaded by the receiver. No action is required from the sender.		X	

Table 27- Types of IDES Alerts

DRAFT

Appendix F: Data Preparation User Tips

Due to the implementation of highly secured data transmissions, sometimes it can be challenging to trace the source of a data transmission problem. In response to user questions and common user errors demonstrated during the 2015 IDES testing windows, the IRS has compiled a list of tips to assist users with the data preparation and transmission processes.

If you identify any issues that are not covered here, please forward comments to lbi.fatca.ides@irs.gov. Due to the volume of questions received, responses to these issues will be addressed through future updates to this document or in IDES FAQs rather than via personalized responses

The suggestions below represent the most common solutions. The solutions are grouped into four categories:

Data Package
Payload file
Key file
Metadata file

All validation checks apply to the production and test environments. Certain critical errors will cause the immediate rejection of a transmission, and additional error checks will not be performed. Be aware that even if you correct the initial error, your transmission package may be rejected again if additional errors are found.

Overall Package

1. The transmission packet is in an incorrect format (not ZIP).

   The file extension must be .ZIP.

2. The file was compressed with an incorrect compression algorithm.

   All files must be compressed using the standard Deflate algorithm and common ZIP tools such as WinZip, 7Zip, etc. More information can be found at http://www.irs.gov/Businesses/Corporations/Compression-tools.

3. The data packet has an incorrect file name.

   The data packet filename must be in the format UTC_FATCAEntitySenderId.zip, where UTC represents a timestamp including milliseconds.

   For example, the filename 20150115163045 32Z_000000.00000.TA.124.zip represents a file submitted by the Host Country Tax Authority (HCTA) for Canada created at 2015 January 15 16:30:45.32 Z.

4. The transmission packet contains subfolders.

   The transmitted ZIP file may not contain subfolders and data packets should only contain archived files at the root level.

5. The transmission packet contains additional files.

   There are too many files archived in a folder. The ZIP file should only contain one payload file, one metadata file, and either one or two keys. No other files can be included. Ensure you have the proper naming UTC_FATCAEntitySenderId.zip.

DRAFT

Type of File	Model 1, Option 2 (Only) - Attach 4 Files	Models 1 & 2 - Attach 3 Files
Metadata	FATCAEntitySenderId_Metadata.xml	FATCAEntitySenderId_Metadata.xml
Key File(s):	FATCAEntityReceiverId_Key	FATCAEntityReceiverId_Key
	HCTAFATCAEntityId_Key	N/A
Payload	FATCAEntitySenderId_Payload	FATCAEntitySenderId_Payload

6. The transmission packet failed virus scan.

   The transmission packets are scanned for viruses during the upload process and will be rejected and/or deleted if a virus or other threats are detected.

Payload file

7. The payload was not attached to the file.

   A valid XML payload is required with each transmission packet. The requirement also applies to test packages. If the payload file is not present, the transmission is rejected even if the other parts of the data packet are created properly.

8. The payload file was not in the proper XML format.

   The payload file must be in XML format document and created according to the published XML schema. If the data is presented in a non-XML format, your transmission will be rejected.

9. The payload file has an incorrect filename.

   The payload file name must be in the proper naming convention or format FATCAEntitySenderID_Payload.

   For example, if the sender is an HCTA, the file name should be 000000.00000.TA.NNN_Payload, where NNN is the three digit ISO code for the HCTA's countryNote that there is no extension on the file. Also check for correct capitalization.

10. The payload file is not encrypted or fails entropy check.

    It is not possible to determine whether a file is properly encrypted. IDES applies an entropy check to determine if a file was likely to be encrypted. If the file does not pass the entropy check, it will not be accepted. Encrypt the payload using a randomly generated AES-256 key with the following settings:

    - Cipher Mode: ECB
    - Salt: No Salt
    - Initialization Vector: no IV
    - Key size: 256 bits/32 bytes
    - Encoding: None
    - Padding: PKCS#5 or PKCS#7

11. The payload file is not signed.

    The payload file must be digitally signed by the sender using the standard RSA digital signature method. More information can be found at http://www.irs.gov/Businesses/Corporations/Digital-Signatures-for-Data-Preparation.

DRAFT

12. The digital signature is not valid.

    IDES requires an enveloping signature and the SHA2-256 algorithm. If an incorrect digital signature type or algorithm is used, the digital signature will fail validation. Any changes to the XML after the digital signature has been performed will cause the validation to fail. There are digital signature validation tools available that can be used to verify the signature is valid before submission.

13. The digital signature used the wrong signature type, such as enveloped or detached.

    The XML must be signed with an enveloping digital signature. If the wrong digital signature type is applied the data packet will fail validation. If you create a different kind of signature but move the signature block within the XML file so that it appears to be an enveloping signature, the file will still fail validation.

14. The key used for signature does not match the certificate store.

    The private key used to perform the digital signature must correspond with the certificate that was uploaded during IDES enrollment. IRS sample keys and certificates should not be included as part of the data packet.

15. The file contained incorrect encryption settings. The file may contain one or more incorrect settings, such as:
    - Wrong cipher mode
    - Salt settings
    - Wrong key size
    - Encoding applied
    - Wrong padding

    More information can be found at http://www.irs.gov/Businesses/Corporations/IDES-Data-Transmission-and-File-Preparation or review Item 10 above.

16. The FATCA XML Schema v1.1 contains invalid elements.

    Only elements described in the published XML schema may be used. Certain elements are required in the transmitted payload XML. Review the FATCA XML Schema v1.1 User Guide at http://www.irs.gov/pub/irs-utl/Pub5124UserGuide.pdf for details.

17. The FATCA XML Schema v1.1 contains illegal characters.

    Certain characters cannot be used in the FATCA data packet or must be replaced with entity references. Review the information at http://www.irs.gov/Businesses/Corporations/FATCA-XML-Schemas-and-Business-Rules-for-Form-8966 for details.

    Note that some signature tools may insert illegal characters in the KeyInfo element when generating a signature. The KeyInfo element should be removed before submitting the data packet.

Key files

18. There is no key file in the transmission data packet.

    A key file representing each receiver for the package must be present in the data packet.

19. The key file has an incorrect file name.

    The key file name must be in the correct format FATCAEntityReceiverId_Key. Files received by the IRS should have a file named 000000.00000.TA.840_Key.

20. The data packet has the incorrect key size.

DRAFT

The unencrypted key file should have a length of 32 bits. Encrypt the key file and place it in the archived data packet. The key size should be 256 bytes. Verify the key size before and after encryption. If you move the key file between operating systems, it may add extra characters that cause an incorrect key size or transmission failure.

21. The key file is not encrypted or fails entropy check.

    It is not possible to determine whether a file is properly encrypted. IDES applies an entropy check to determine if a file was likely to be encrypted. If the file does not pass the entropy check, it will not be accepted. Encrypt the payload using a randomly generated AES-256 key with the following settings:

    - Cipher Mode: ECB
    - Salt: No Salt
    - Initialization Vector: no IV
    - Key size: 256 bits/32 bytes
    - Encoding: None
    - Padding: PKCS#5 or PKCS#7

22. The key file is encrypted with an incorrect key.

    The key must be encrypted with the AES public key of the recipient. For files received by the IRS, use the public key available at www.ides-support.com.

23. The wrong padding was used during the encryption process.

    The padding used during the key encryption must be PKCS#1 v1.5. Ensure the tool used to perform the encryption has the correct padding settings.

24. The data packet is missing the second key file (Model 1 Option 2 Only).

    If you submit under Model 1 Option 2, there should always be two keys present in the archived data packet. One key for the IRS and the second key will be used by the HCTA.

    More information on keys required for the Model 1 Option 2 can be found in Step 5, Section 9.2 of the IDES User Guide.

25. The data packet contains a second key file and you are not under a Model 1 Option 2 (M1O2) IGA.

    Only submitters under a Model 1 Option 2 agreement should submit a data packet with two key files. All other submitters should submit an archived data packet that contains only one key file.

Type of File	Model 1, Option 2 (Only) - Attach 4 Files	Models 1 & 2 - Attach 3 Files
Metadata	FATCAEntitySenderId_Metadata.xml	FATCAEntitySenderId_Metadata.xml
Key File(s):	FATCAEntityReceiverId_Key	FATCAEntityReceiverId_Key
	HCTAFATCAEntityId_Key	N/A
Payload	FATCAEntitySenderId_Payload	FATCAEntitySenderId_Payload

DRAFT

Metadata file

26. The metadata file has an incorrect file name.

    The metadata file name must be in the recommended format FATCAEntitySenderId_Metadata.xml.

    For example, if the sender is an HCTA, the file name should be 000000.00000.TA.NNN_Metadata.xml, where NNN is the three digit ISO code for the HCTA's country

27. The metadata file is encrypted.

    The metadata file must NOT be encrypted. IDES reads the metadata file and uses the elements to identify and route the transmission.

28. There are invalid elements in the metadata schema.

    Please review the Metadata user guide at http://www.irs.gov/pub/irs-pdf/p5188.pdf for information on the fields to use in the Metadata file.

29. There are missing required elements in the metadata schema.

    IDES validates the following mandatory elements in the metadata Schema:

    - FATCAEntitySenderID (see #31 below)
    - FATCAEntityReceiverID
    - FATCAEntCommunicationTypeCd
    - SenderFileID
    - FileCreateTS
    - TaxYear (see #33 below)
    - FileRevisionInd

30. There is an incorrect type code (NTF or RPT) in the metadata schema.

    All FATCA reporting files submitted to the IRS should have the transmission type code RPT. RPT is the only allowable entry. The NTF code is used for Notifications that are sent in response by IRS. If the incorrect code (NTF) is used on a report, the file cannot be processed and will fail validation.

31. The metadata SenderID element does not match the IDES account used.

    The SenderID in the metadata file must represent the GIIN associated with the user who is logged in to IDES and transmitting the data packet.

32. The metadata ReceiverID element is not the IRS GIIN.

    The ReceiverID in the metadata file must be the IRS GIIN: 000000.00000.TA.840.

33. The metadata TaxYear element is invalid or missing.

    A valid TaxYear must be specified. At this time, the only valid Tax Year is 2014 in the YYYY format.

34. The metadata file contains illegal or restricted characters.

    Certain characters are prohibited and must be encoded or replaced with entity references. Review the information at http://www.irs.gov/Businesses/Corporations/FATCA-XML-Schemas-and-Business-Rules-for-Form-8966 for details.

DRAFT