HttpsPost User Guide

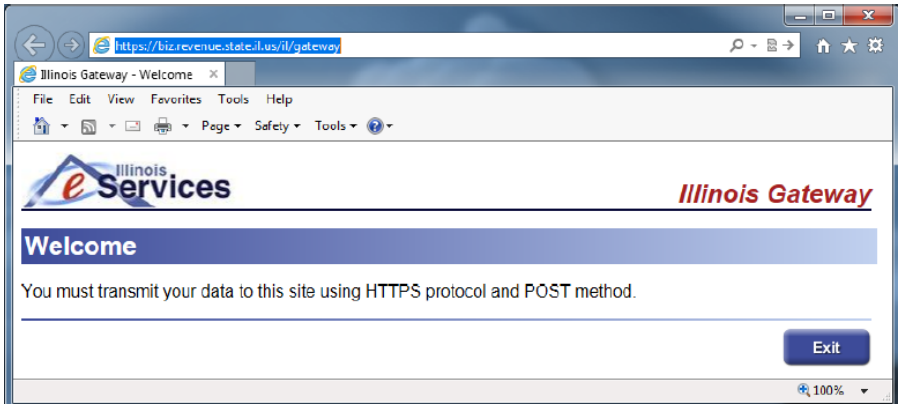
Description

The HttpsPost Utility Program transfers files to and from the Illinois Department of Revenue's (IDOR) Gateway server via the Internet using Secure Socket Layer (SSL) technology. The utility runs as a stand-alone application under Microsoft Windows 95, 98, NT, 2000, XP, 7, 10 and 11. The HttpsPost Utility Program supports both a graphical user interface (GUI) mode of operation as well as a command line mode suitable for batch processing.

The program requires a connection to the internet and makes use of Windows' built-in Winsock and certificate management software. These items must have already been installed and set up correctly before attempting to run the program. The best approach is to test the computer setup and internet connectivity first by trying to connect to the IDOR Gateway through a web browser. The web address has the following URL:

https://biz.revenue.state.il.us/il/gateway

For example, browsing to this URL with Internet Explorer, one should see a web page like the illustration below. In addition to testing the computer's network connectivity, seeing this page also proves that the SSL certificate exchange has been successful, and your computer system recognizes our site as being authentic. Issues involving SSL site certificate exchange must be resolved by emailing rev.ecstech@illinois.gov.



Installation

Installation consists of simply copying the executable file to an **empty** directory or folder.

Download as a .zip: https://www.revenue.state.il.us/ecs/HttpsPost.zip

Download as an .exe: https://www.revenue.state.il.us/ecs/HttpsPost.exe

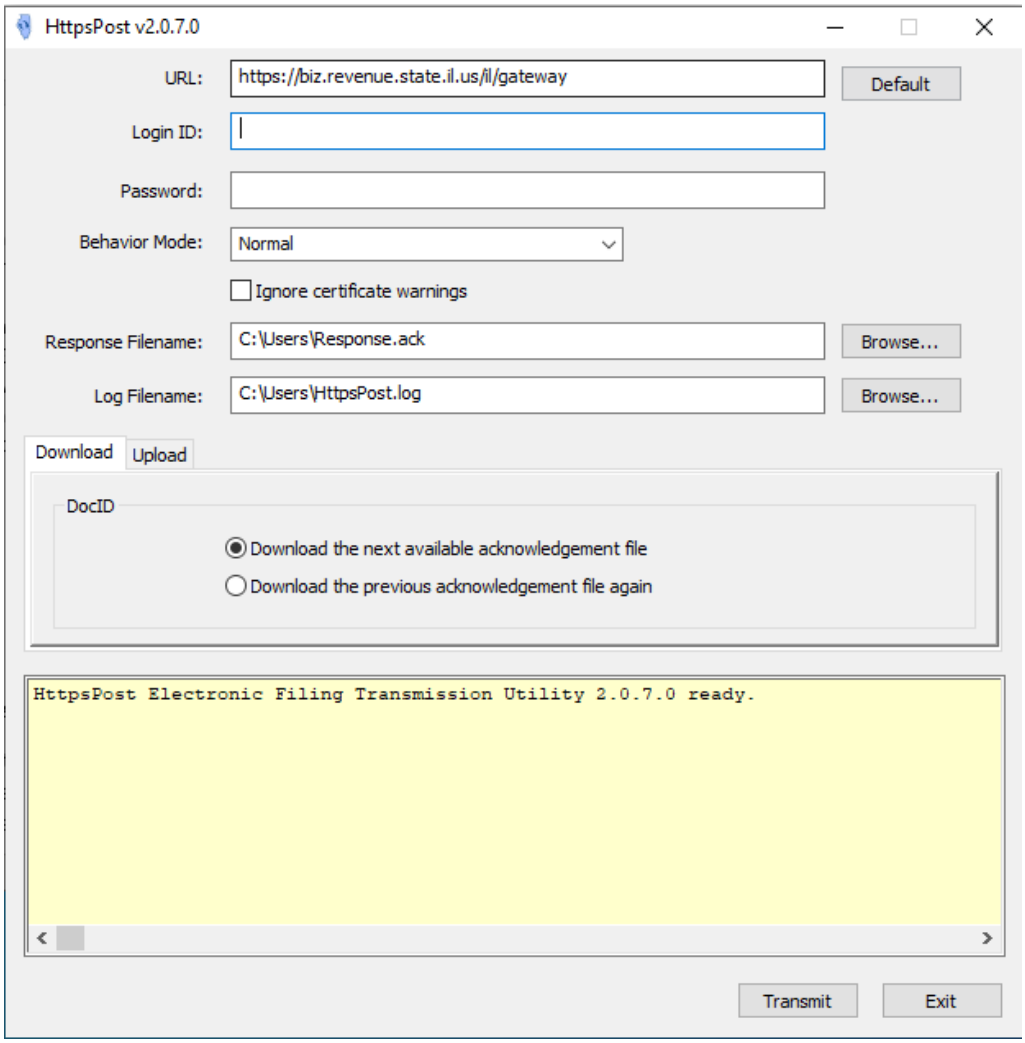
Program Use

For convenience in launching the application in its GUI mode, place shortcuts to the executable on the desktop or in the Windows start menu. Simply launching the executable without command line arguments starts the application in its GUI mode.

During operation, the program creates two files in the current working directory. One is named HttpsPost.log, which is a text file of logging information showing some messages regarding the HTTP session. This log file provides session record keeping and may be helpful for debugging. The file is overwritten each time a new HTTP connection is made so that it contains only the log of the last full session completed, so it is important to edit the file name prior to transmission.

The other file, named Response.ack, contains the body of the HTTP response data returned to the application from the IDOR Gateway. This file will contain all acknowledgements sent by the server during the connection. Whenever a new connection or new transmission is made, the content of the Response.ack file is completely erased and all new response data are recorded here in its place. Therefore, before initiating a new transmission, be sure to edit the file name, or move the Response.ack file to another directory where it will not be overwritten.

After launching the HttpsPost program in its GUI mode, one should see a window similar to the illustration below.



The input field labeled "Login ID" should contain the user's five-character login ID (ETIN) that was assigned by IDOR. The input field labeled "Password" should contain the user's password. The drop-down list labeled "Behavior Mode" should remain set to its default setting of "Normal" for most users. The other behavior mode settings will be explained later in this document. The "Ignore certificate warnings" check box will allow you to automatically ignore digital certificate warnings. This should only be checked for troubleshooting connection failures resulting from errors involving digital certificate exchange during SSL handshaking. You can also edit your Response Filename and Log Filename, if desired, from this interface. One of the tabs labeled "Download" and "Upload" should be selected to indicate whether the user wants to download an acknowledgement file from the gateway or upload a file to the gateway. If the Download tab is selected, the user must select one of

the options labeled “Download the next available acknowledgement file” and “Download the previous acknowledgement file again”. If the Upload tab is selected, the input field labeled "DocID" may be used at the discretion of the user.

It should generally contain any character string that conveys meaning to the user uniquely related to the file that will be uploaded. Any alphanumeric sequence, including leaving the input field blank, may be used here with the exception of two reserved values. The reserved values are "NewAck" and "LastAck", neither of which is case sensitive. The "NewAck" and "LastAck" values have special meanings to the IDOR Gateway for transmitting acknowledgements as will be discussed later.

At the end of a transmission, whatever character string value was in the "DocID" input field will be echoed back to the transmitter as part of an Acknowledgement One receipt for the transmission as the TransmissionIDNumber. Hence, the "DocID" value may be useful to the user as a way of associating an Acknowledgement One receipt to its transmitted file. At the end of every successful file transmission the server returns this Acknowledgement One as proof of receipt of transmission. The Acknowledgement One receipt will appear in the Response.ack file similar to the following text:

```
  Status Code = 200
Downloading 235 bytes from response
Illinois Department of Revenue Acknowledgement One
   1. ETIN = 00000
   2. TransmissionIDNumber = null
   3. TransmissionTimeStamp = 10/22/2020 02:03:46 PM
   4. FileSize = 450728
   5. SysFileName = T000002020102214034624l.296
Operation completed
**** End    ****
```

No transmission should ever be considered successful unless an Acknowledgement One receipt is received. Keep in mind that the Acknowledgement One response only confirms file “receipt” and not file “acceptance”. It is the user’s responsibility to pick up acknowledgment files at a later time to use to verify if the transaction(s) were accepted or rejected.

The input field labeled "Filename" should contain the full path to the file the user intends to upload to the IDOR Gateway. Click on the "Browse" button to use a dialog window to navigate interactively to this file. Finally, click on the "Transmit" button to begin the transmission.

If the Download tab is selected, for downloading an acknowledgement file, then one of the two, special, reserved values will automatically be supplied for the "DocID" of the transmission. Selecting the “Download the next available acknowledgement file” option will automatically use the DocID of "NewAck", not case sensitive, to download the next available new acknowledgement file waiting to be retrieved. In case some error prevents an acknowledgement file from downloading successfully, then select the “Download the previous acknowledgement file again” option which will automatically use the DocID of "LastAck", also not case sensitive, to request that the last acknowledgement file downloaded be resent. The "Download the previous acknowledgement file again" option may be used repeatedly. However, once the "Download the next available acknowledgement file" option is used again, the previously downloaded acknowledgement file will no longer be available. The acknowledgement file downloaded using the "Download the next available acknowledgement file" option becomes the file available for retransmission in a subsequent use of the "Download the previous acknowledgement file again" option. The presence of either of the two special values, either “NewAck” or “LastAck”, is what triggers the IDOR Gateway to send an acknowledgement file. When one of these values is present in the DocID transmission request, the gateway immediately responds with the contents of the

acknowledgement file and no file will be uploaded to the IDOR Gateway even if the “Filename” input field is filled in.

A single transmission request cannot both upload a file and download an acknowledgement file.

Command Line Operation

Adding command line arguments automatically switches the HttpsPost program into its command line mode of operation. In this mode, the program will display the user interface during transmission, but no interaction with the user interface will be possible. The values of each input field will be supplied by the command line parameters. If command line parameters are supplied, the program requires between a minimum of four parameters, up to a maximum of eight parameters, each separated by a space. If a parameter contains embedded space characters, use double quotation characters before and after the parameter. The command line has the following form where [] indicate optional parameters and | separates a list of acceptable values for a parameter:

HttpsPost.exe <url | /Default> <loginid> <password> <docid | NEWACK | LASTACK> [<filename>] [</ProxyUser:user>] [</ProxyPassword:password>] [</BehaviorMode:NORMAL>] [</IgnoreCerts>]

Where:

<url | /Default> = The URL of the site or /Default will always go to “https://biz.revenue.state.il.us/il/gateway”.

<loginid> = The user’s 5 digit login ID (ETIN).

<password> = The user’s password.

<docid | NEWACK | LASTACK> = Since the GUI options are not available in command line mode, the DocID must be specified with either one of the special values NEWACK or LASTACK described above to download an acknowledgement file, or any other value to upload the file specified as the <filename> parameter.

<filename> = Optional parameter containing the full path filename of the file to be uploaded. This is only used if the docid parameter contains a value other than NEWACK or LASTACK.

</ProxyUser:user> = Optional parameter containing /ProxyUser: followed with the user’s proxy server login name. This is only used if Windows is configured to use a proxy server when connecting via the internet and only if the proxy server requires user authentication for such connectivity.

</ProxyPassword:password> = Optional parameter containing /ProxyPassword: followed with the user’s proxy server password. This is only used if Windows is configured to use a proxy server when connecting via the internet and only if the proxy server requires user authentication for such connectivity.

</BehaviorMode:NORMAL > = Optional parameter containing /BehaviorMode: followed with the following value NORMAL. The use for this parameter will be explained later in this document.

</IgnoreCerts> = Optional parameter containing /IgnoreCerts. This parameter is used to ignore digital certificate warnings that can occur for several reasons including encountering a digital certificate that was issued by an unrecognized Certificate Authority, a digital certificate whose name does not match the name of the server, expired digital certificates, etc.

In command line mode, the HttpsPost program returns error level 0 upon successful completion, returns error level 1 if an error occurs while sending data or error level 2 if an error occurs while receiving data. Below is a sample Windows batch file that demonstrates uploading a file, and using the error level to determine success or failure of the transmission:

```
@setlocal

start /w HttpsPost /default myetin mypassword mytransid c:\my\folder\file.txt
@if errorlevel 2 @goto badreceive
@if errorlevel 1 @goto badsend
@if errorlevel 0 @goto okay

@echo Unknown errorlevel %errorlevel%
@goto done

:okay
@echo OKAY
@goto done

:badsend
@echo SEND FAILED
@goto done

:badreceive
@echo RECEIVE FAILED
@goto done

:done
@echo.
@endlocal
```

Technical Information

The IDOR Gateway is available to use seven days a week except between the times of 11:30 pm to 3:00 am Central Time. This system down-time is required to allow for scheduled system maintenance.

Content-Length Header

File transfers are verified through the use of the Content-Length HTTP header. Every file transmission request to the IDOR Gateway must contain a Content-Length header specifying the number of bytes in the body of the message that will be transmitted. The IDOR Gateway verifies that all bytes were received by comparing the received file size with this header value. Discrepancies result in the transmission being rejected.

Likewise, a Content-Length header precedes all HTTP response data returned by the IDOR Gateway. This header specifies the number of bytes that will be transmitted in the body of the HTTP response. The HttpsPost program automatically checks this header and compares it to the received file size. If the two values do not match, the program will display an error message with a note of explanation. If you encounter a transmission error while receiving acknowledgements, the best error handling practice is to wait a few minutes, then request retransmission of the acknowledgement file using the “LastAck” value in the “DocID” command line parameter or choose the “Download the previous acknowledgement file again” option of the HttpsPost window.

Users who prefer to use their own software to send and receive files to the IDOR Gateway must supply a Content-Length header for file uploads, and their software is responsible for verifying file receipt by checking the file size against the value of the Content-Length header of the IDOR Gateway response.

Behavior Mode and Headers

When transmitting with "Behavior Mode" set to "Normal", the value of the "DocID" field of the HttpsPost program is passed to the IDOR Gateway as the value of the extended HTTP request header X-Transmit-ID, and the Content-Type HTTP header will contain the value text/plain. Users who write their own software must supply these headers in their HTTP requests and set the values appropriately. As described previously, acknowledgements will be returned whenever the X-Transmit-ID header contains the value "NewAck" or "LastAck". These two reserved values are not case sensitive. Also, any other value for this header will cause the IDOR Gateway server to expect to receive a file from the user. After the file transfer, the value of the extended header will be returned in the acknowledgement-one response as a convenient form of document tracking for the user. The use of the extended header for document tracking is optional and remains at the discretion of the user.

The following shows an example of a complete http post transmission including all HTTP MIME headers:

POST /il/gateway HTTP/1.1 Host: biz.revenue.state.il.us
Authorization: Basic MDAwMDA6cGFzc3dvcmQ= *(Base64 encoded)*
Accept: text/plain, text/html, text/xml
User-Agent: (*optional header)*
X-Transmit-ID: DOC1
Content-Type: text/plain
Content-Length: 99
****
The transmitted file goes here.
****

Below is the complete HTTP response to the above transmission:

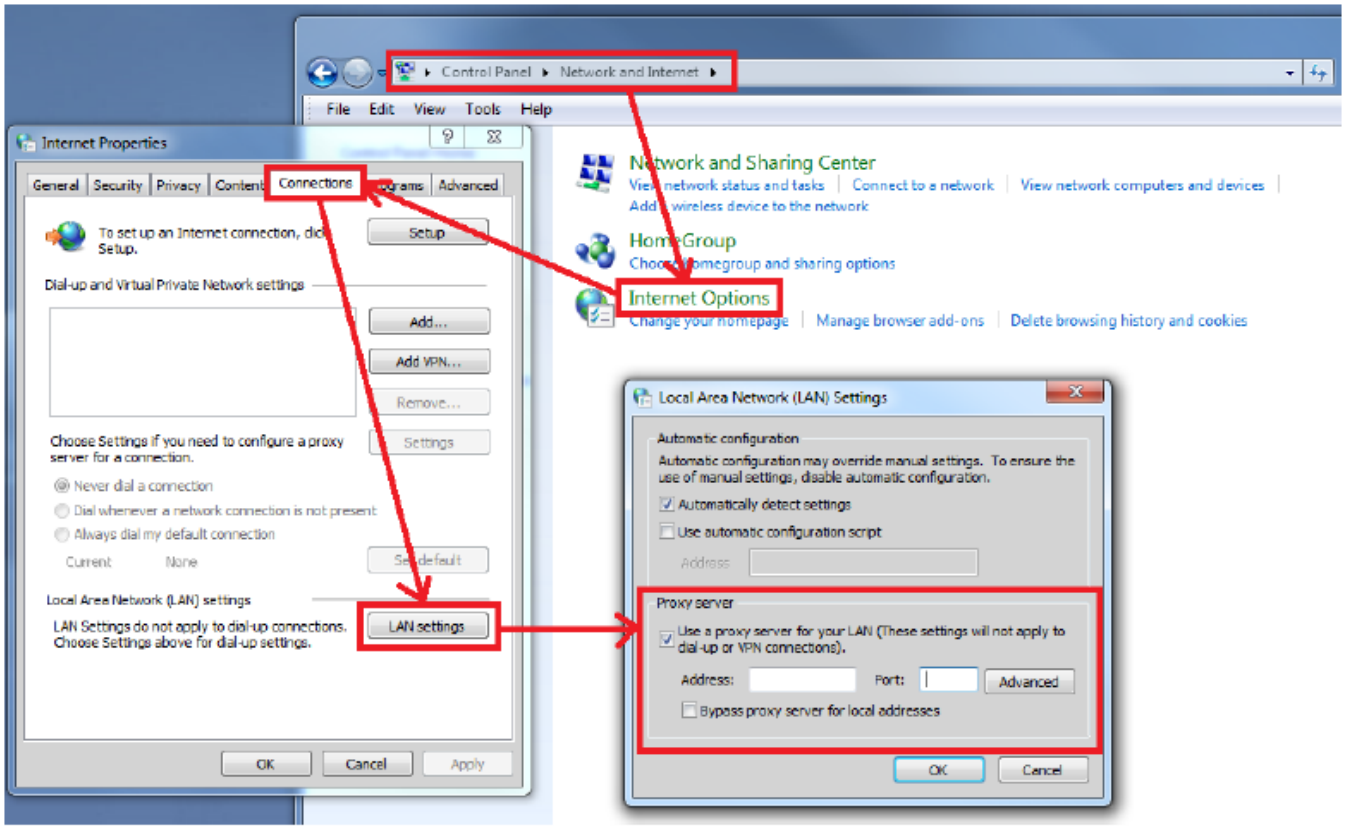
HTTP/1.1 200 OK
X-Powered-By: Servlet/3.0
HttpsPostVersion: 2.0.4.0
Pragma: no-cache
Cache-Control: no-cache
Expires: Wed, 30 Oct 2013 19:35:45 GMT
Last-Modified: Wed, 30 Oct 2013 19:35:45 GMT
Content-Type: text/plain
Content-Length: 231
Content-Language: en-US
Date: Wed, 30 Oct 2013 19:35:45 GMT
Server: WebSphere Application Server/8.5

Illinois Department of Revenue Acknowledgement One
1. ETIN = 00000
2. TransmissionIDNumber = DOC1
3. TransmissionTimeStamp = 10/30/2013 02:35:45 PM

4. FileSize = 99
5. SysFileName = T00000201310301435457O4.303

Using a Proxy Server

The HttpsPost program will now automatically detect and utilize a proxy server when establishing an internet connection to the IDOR Gateway, provided that the proxy server settings have been properly configured using the Windows control panel. The illustration below shows the steps necessary to configure Windows to utilize a proxy server:



Some proxy servers will require user authentication prior to establishing an internet connection. When the HttpsPost program is running in GUI mode and the proxy server requires authentication, a dialog box will automatically display in which the user can enter the user and password information for the proxy server authentication. When the HttpsPost program is running in command line mode and the proxy server requires authentication, the proxy server user and password information must be supplied using the /ProxyUser: and /ProxyPassword: command line parameters. Note that the proxy user and password are usually assigned by your network administrator. These should not be confused with your IDOR Gateway login ID (ETIN) and password which are assigned by the Illinois Department of Revenue.