ELECTRONIC DATA COLLECTION, PROCESSING AND DATA DELIVERY FOR NATIONAL HOSPITAL CARE SURVEY

Detailed Instructions on How to Submit UB-04/ State File Data using The Secure Transfer Network

INTRODUCTION/PURPOSE

The purpose of this document is to outline the process Hospitals will use to deliver UB-04 claims data and state-specific claims files to Westat for the National Center for Health Statistics (NCHS) National Hospital Care Survey (NHCS) for 2018.

The intended audience for this document is Hospital Interface Specialists, Westat Support Specialists, CGI Federal management, and Centers for Disease Control (CDC) and NCHS management.

OVERVIEW

Westat collects claims data from hospitals who have been recruited to participate in the NCHS hospital survey. If the hospital is unable to deliver clinical data in the form of a CCD or CDA-R xml file, then accepting claims data is the next best approach to acquiring the data needed to populate NCHS statistical databases.

Westat, under a subcontract agreement with CGI Federal will act as a consolidation agent to receive and forward patient claims data to CDC for those hospitals who agree to participate in the NHCS.

Each hospital agreeing to participate will sign a Business Associates Agreement (BAA) authorizing Westat to release patient data to CDC exclusively for the purpose of populating the NCHS database. The identity of participating hospitals and all Patient Health Information (PHI) and Personally Identifiable Information (PII) will be protected at all stages of the process.

The number of hospitals submitting data via the UB-04/state file process is capped at 100 hospitals.

TABLE OF CONTENTS

Introduction/Purpose 2
Overview 2
1. Using the Westat Secure Transfer System (WSTS) 4
1.1 Getting Started - Sign On 4
1.2 First Sign On 5
1.3 The Home Screen 9
1.4 Uploading a File or Files 9
1.5 Troubleshooting 13
1.5.1 Common Reasons Access is denied 13
1.5.2 Webpage Has Expired 13
1.5.3 Warning Message When Signing On 14
1.5.4 Installing the Wizard on browsers other than Internet Explorer 15
1.5.5 Uploading Files Without Using the Wizard 16
1.5.6 Uploading Problems 17
1.6 Appendix 18
1.6.1 Supported Web Browsers 18
1.6.2 Supported Secure FTP/SSL Clients 18
1.6.3 Supported Secure FTP/SSH (and SCP2) Clients 19
1.6.4 Supported AS2/AS3 Clients 21

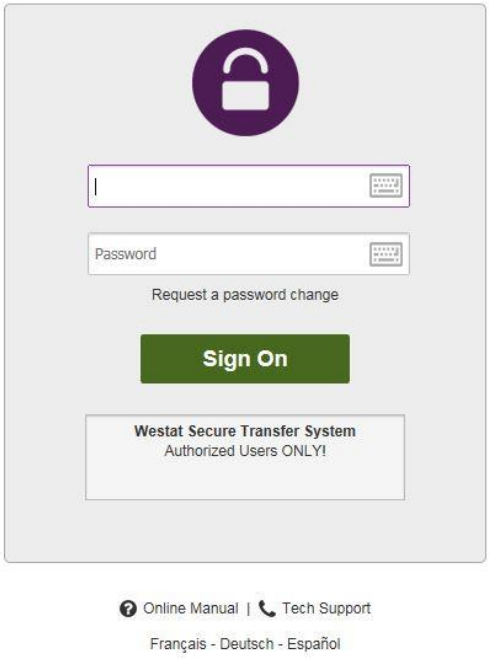
1. USING THE WESTAT SECURE TRANSFER SYSTEM (WSTS)

Welcome to the National Hospital Care Survey! You now have a username and password to sign on to the Westat Secure Transfer System (WSTS), maintained by Westat, an agent of the CDC's National Center for Health Statistics (NCHS) working with CGI Federal in the collection and processing of data for the survey. This user guide will provide you with easy to follow instructions on: how to log in to the system; uploading your data for transmission; receiving notification of transmission; and solving common problems. Supported browsers are listed on the last page. Using this system will allow for the secure transfer of your UB-04, State file data or EHR data. If you need assistance at any point, please contact Terry Pierce at Westat at: 301-610-4831.

1.1 Getting Started - Sign On

To transmit your files, please visit the Westat Secure Transfer System (WSTS) website.

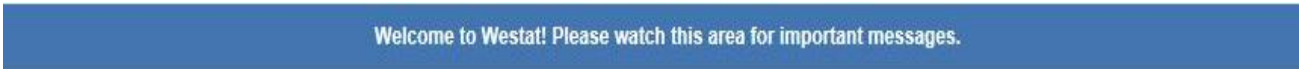
The Sign On page is the first page you will see from the site. This page contains fields for your Username and Password, a "Sign On" button to send this information to the WSTS and a "Reset" button to clear it.



Enter your authentication information using either your computer keyboard or the on screen clickable keyboard, which you can open by clicking on the keyboard icons next to the Username and Password. Using the clickable keyboard gives added security against hackers.

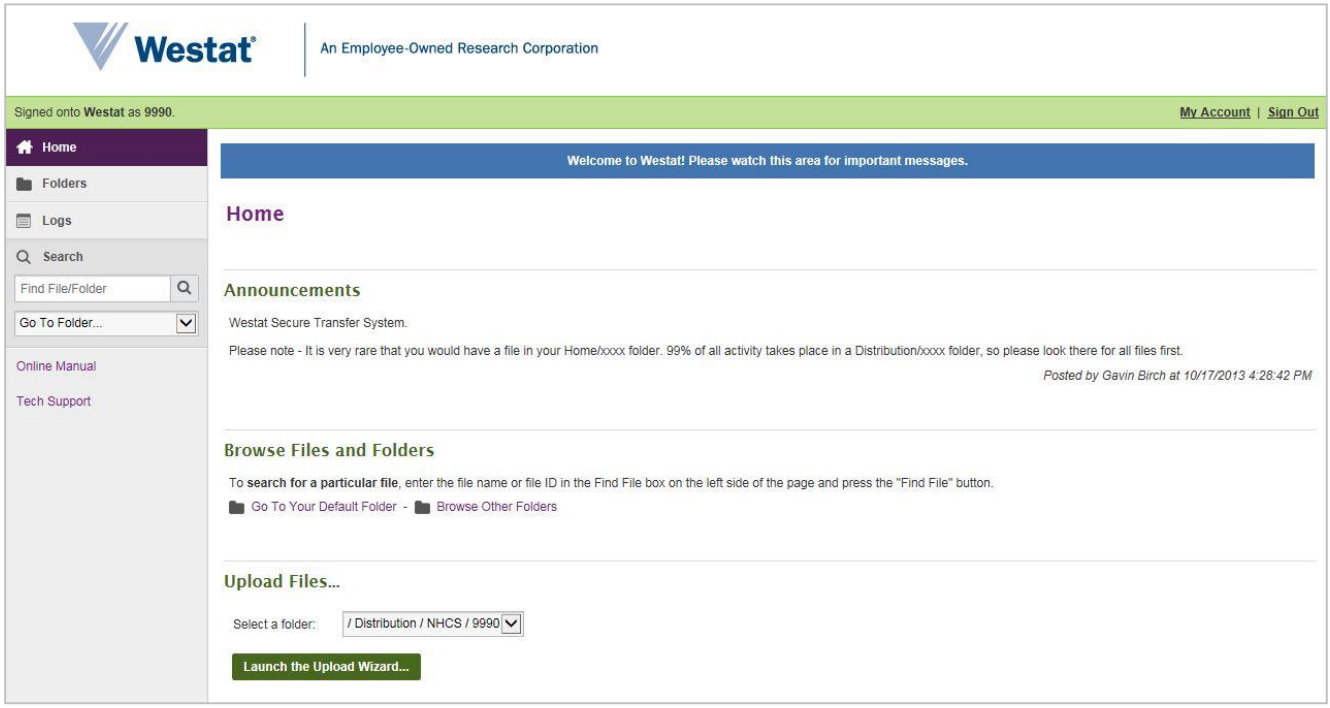
When you press the Sign On button, your Username and Password are transmitted securely (via HTTPS) to the WSTS. If your sign on attempt fails, you will see an error message in the banner above the sign on box. If you attempt to sign on too many times in a short period of time your account may get permanently locked out of the system. If this happens, contact your Regional Operations Manager.

If your sign on is successful you will be rewarded with a success message.



1.2 First Sign On

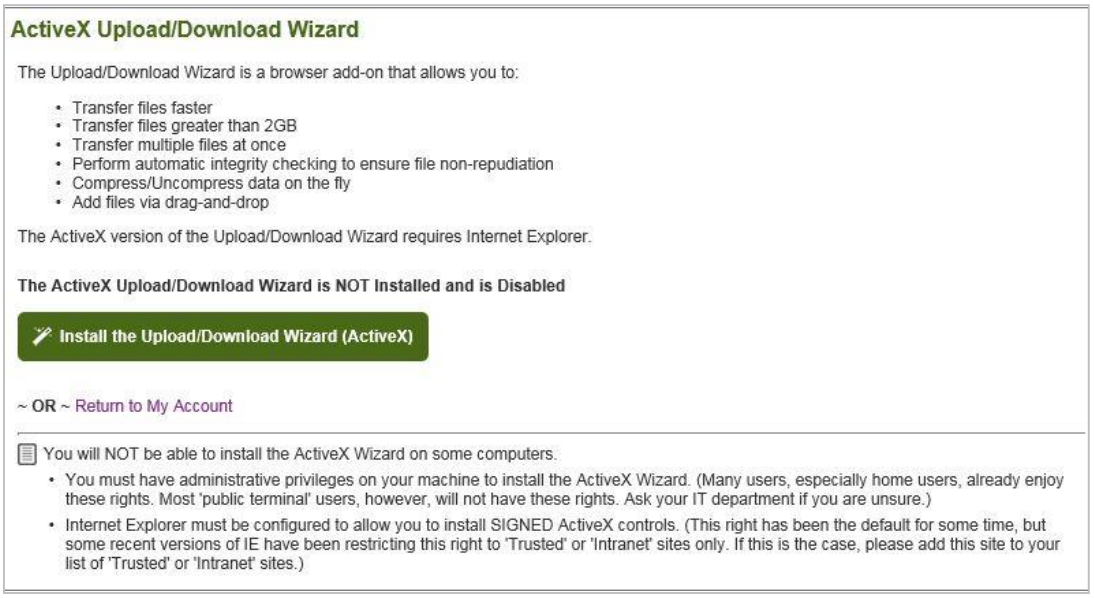
WSTS detects if you have not logged in before and provides an option to install the Upload Wizard. We strongly recommend that you install the Wizard if possible. Using the Wizard provides integrity checks of transmitted files, supports uploading multiple files at once and allows you to zip files for uploading files quickly. If the wizard has loaded, you will see the "Launch Upload Wizard" button under Upload Files.



You may be prompted to try to install the Upload/Download Wizard, in which case you will see:

We understand that you may not be able to install ActiveX components on your PC due to security restrictions. Should this be the case, refer to the Troubleshooting section of this manual for an alternate way to upload your files. If you are able to install the component, follow the steps below.

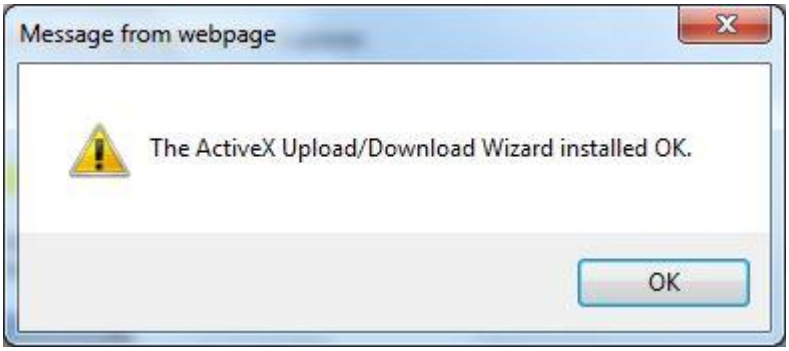
First, click the “reinstall the ActiveX Upload/Download Wizard” link as seen in the screenshot above.



Click on the “Install the Upload/Download Wizard (ActiveX)” button.

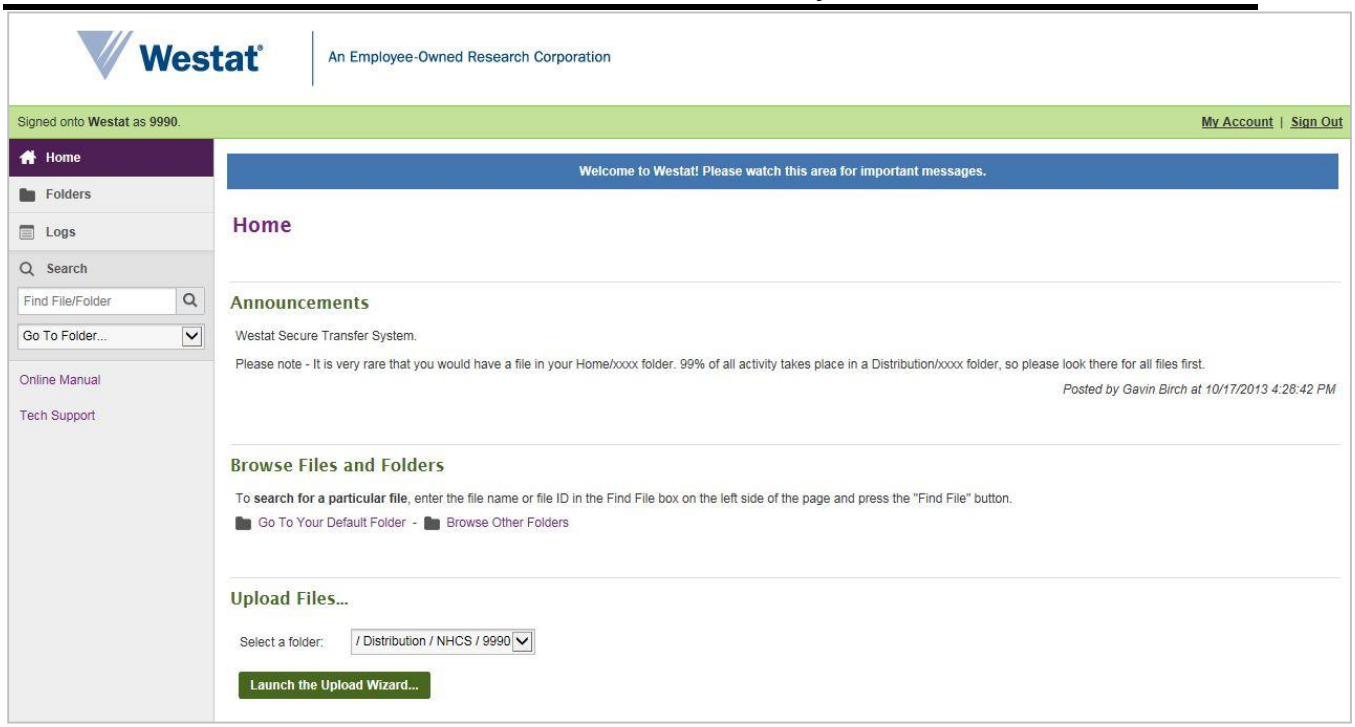
You will see the screen change to reflect the status and an install dialog should appear shortly thereafter.

Once completed, the status window below appears.



Click the “OK” button.

If the wizard installed successfully, you should see a screen that looks like this. This is also the screen you will see when you subsequently sign on to the system.

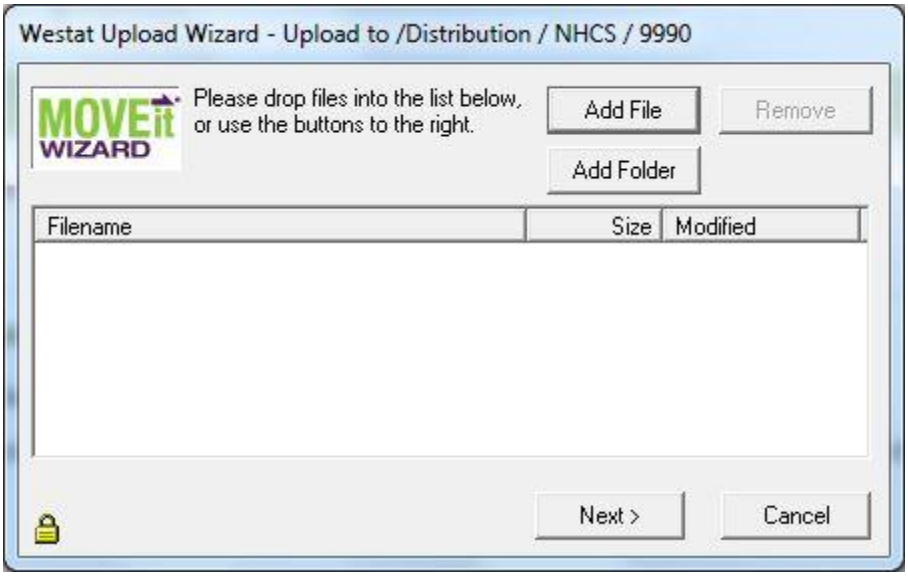

Westat
An Employee-Owned Research Corporation
Signed onto Westat as 9990.
My Account | Sign Out
Home
Folders
Logs
Search
Find File/Folder
Go To Folder...
Online Manual
Tech Support
Welcome to Westat! Please watch this area for important messages.
Home
Announcements
Westat Secure Transfer System.
Please note - It is very rare that you would have a file in your Home/xxxx folder. 99% of all activity takes place in a Distribution/xxxx folder, so please look there for all files first.
Posted by Gavin Birch at 10/17/2013 4:26:42 PM
Browse Files and Folders
To search for a particular file, enter the file name or file ID in the Find File box on the left side of the page and press the "Find File" button.
Go To Your Default Folder - Browse Other Folders
Upload Files...
Select a folder:
/ Distribution / NHCS / 9990
Launch the Upload Wizard...

1.3 The Home Screen

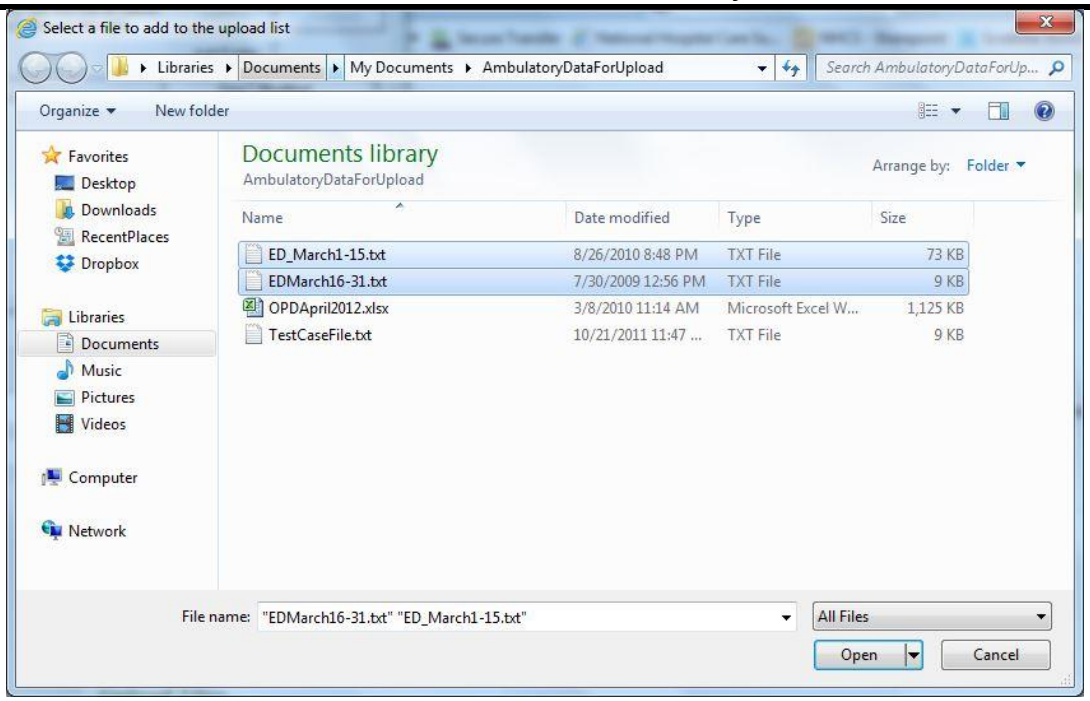
From the “Home” screen shown above, you can perform a number of tasks, such as clicking on My Account to change your notification settings or password. To sign out of the site, click on the Sign Out link. To upload files to the site, click on the button at the bottom of the page to launch the Upload Wizard. The next section will take you step by step through the Upload Wizard screens.

1.4 Uploading a File or Files

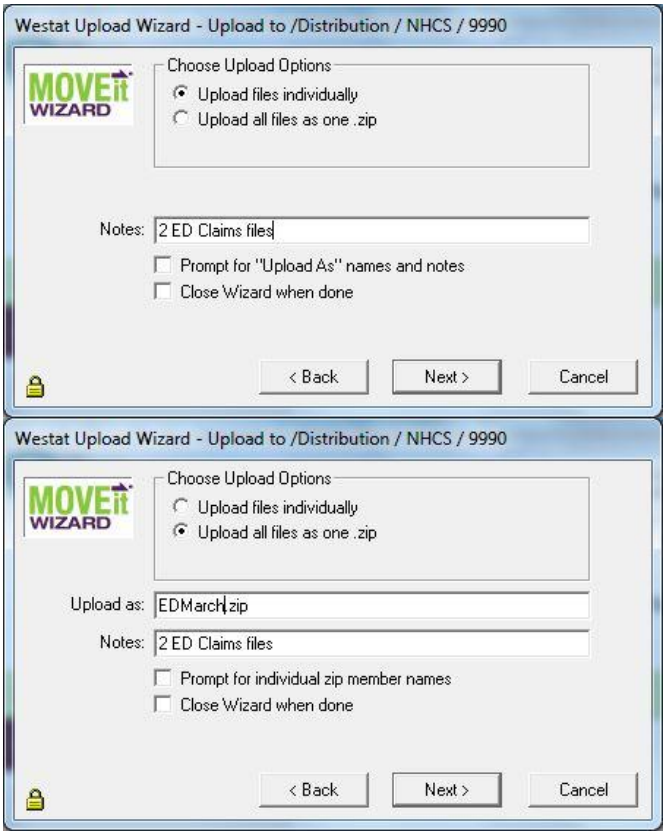
Clicking the Upload Wizard link opens the following window:



Clicking on the “Add File” button brings you to a file selection window. You can then navigate to the folder that contains the file(s). Select one or more files and then click on the “Open” button.



You will then be prompted to choose your upload options.

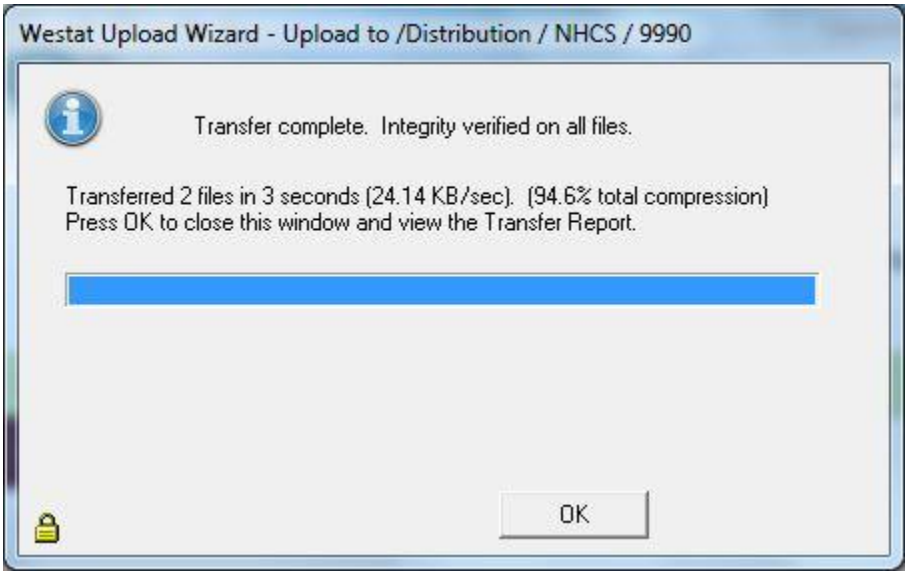


The Notes box is where you will enter the text describing the contents of the transmission. **It is very important to enter the following information into the Notes field above:**

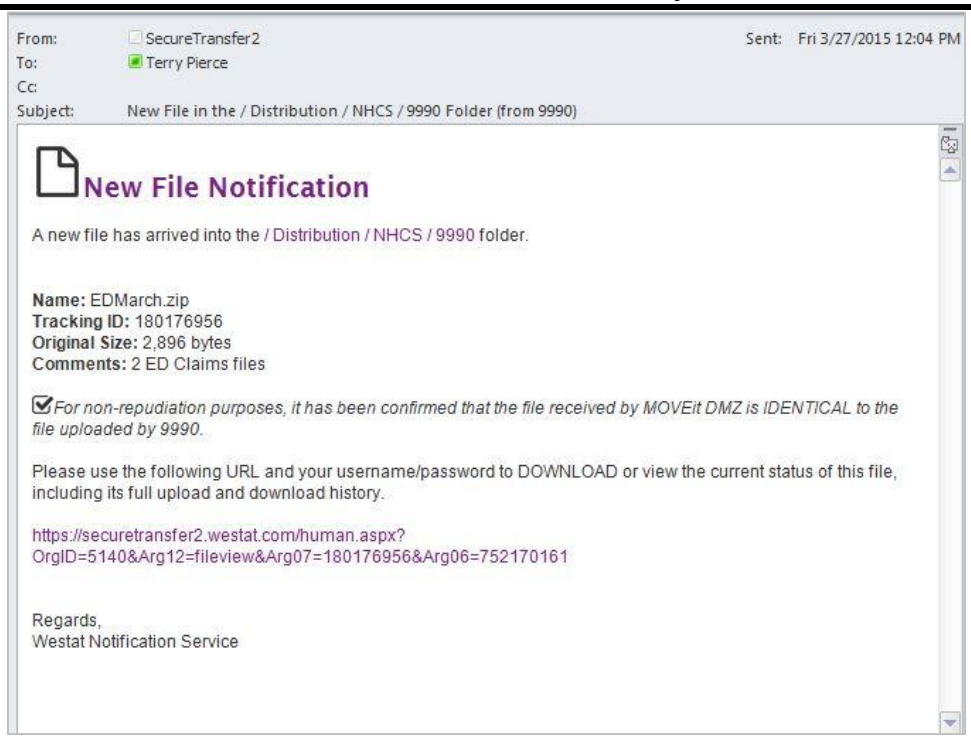
1) **Number of files submitted**
2) **File format**
3) **Timeframe of the files being submitted**
4) **Number of visits in the file(s)**

If you choose to upload files as a zip, you will be prompted to enter a name for the zip file. WSTS will handle zipping the files prior to transmission and the transfer of the zip file.

Clicking "Next" transmits the file(s) to the secure server. You will see a screen briefly flash by (this is the email being sent by the server) and then you will see the confirmation screen shown below.



You will receive a confirmation email from SecureTransfer2 for each file that was transferred. If you bundle a number of files in a zip, you will only receive a single email.



From: SecureTransfer2 Sent: Fri 3/27/2015 12:04 PM
To: Terry Pierce
Cc:
Subject: New File in the / Distribution / NHCS / 9990 Folder (from 9990)

New File Notification

A new file has arrived into the / Distribution / NHCS / 9990 folder.

Name: EDMarch.zip
Tracking ID: 180176956
Original Size: 2,896 bytes
Comments: 2 ED Claims files

☑ *For non-repudiation purposes, it has been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file uploaded by 9990.*

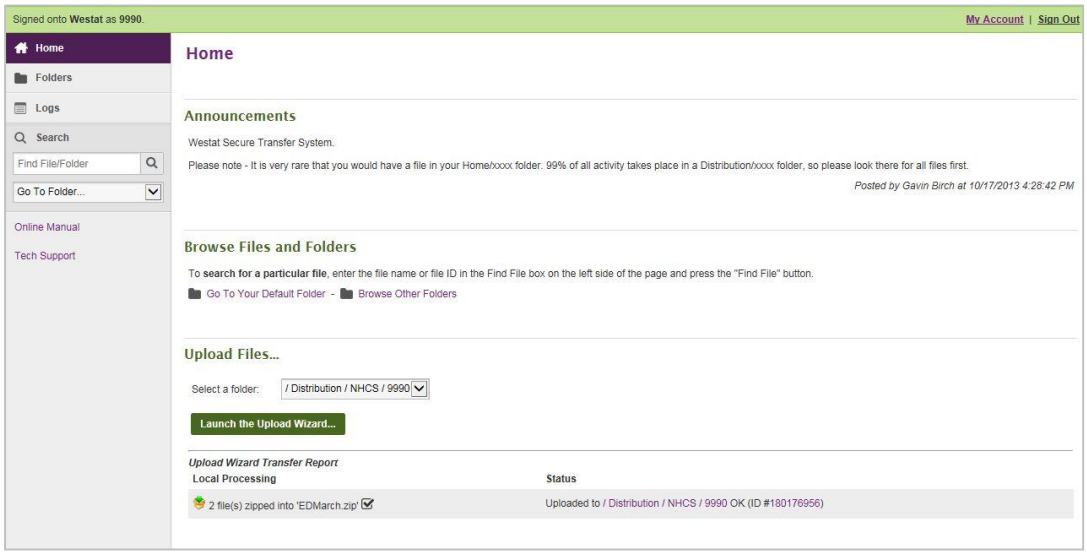
Please use the following URL and your username/password to DOWNLOAD or view the current status of this file, including its full upload and download history.

https://securetransfer2.westat.com/human.aspx?OrgID=5140&Arg12=fileview&Arg07=180176956&Arg06=752170161

Regards,
Westat Notification Service

The file that was transferred, along with a tracking ID and size and any notes/comments are displayed in the message. Note that integrity checking is done as part of the process.

If you click the URL near the bottom of the email, you will be returned to the Sign-On page. Once logged in, you will see the history associated with your file.



Signed onto **Westat** as **9990**. My Account | Sign Out

Home
Folders
Logs
Search
Find File/Folder
Go To Folder...
Online Manual
Tech Support

Home

Announcements

Westat Secure Transfer System.

Please note - It is very rare that you would have a file in your Home/xxxx folder. 99% of all activity takes place in a Distribution/xxxx folder, so please look there for all files first.

Posted by Gavin Birch at 10/17/2013 4:28:42 PM

Browse Files and Folders

To **search for a particular file**, enter the file name or file ID in the Find File box on the left side of the page and press the "Find File" button.

Go To Your Default Folder - Browse Other Folders

Upload Files...

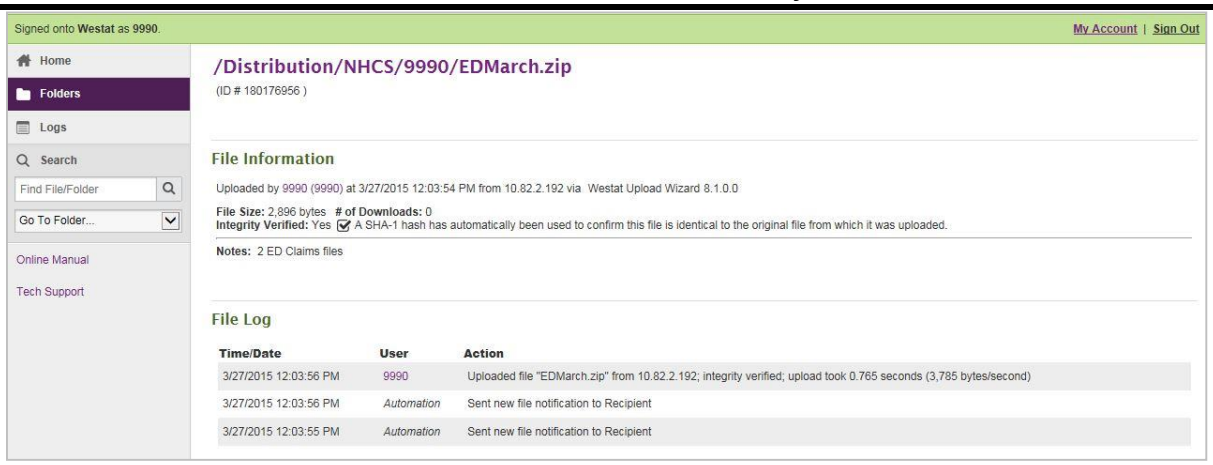
Select a folder: / Distribution / NHCS / 9990

Launch the Upload Wizard...

Upload Wizard Transfer Report

Local Processing	Status
2 file(s) zipped into 'EDMarch.zip' ☑	Uploaded to / Distribution / NHCS / 9990 OK (ID #180176956)

Clicking the ID# link under the Status column will display the log of events related to the upload.



1.5 Troubleshooting

1.5.1 Common Reasons Access is denied

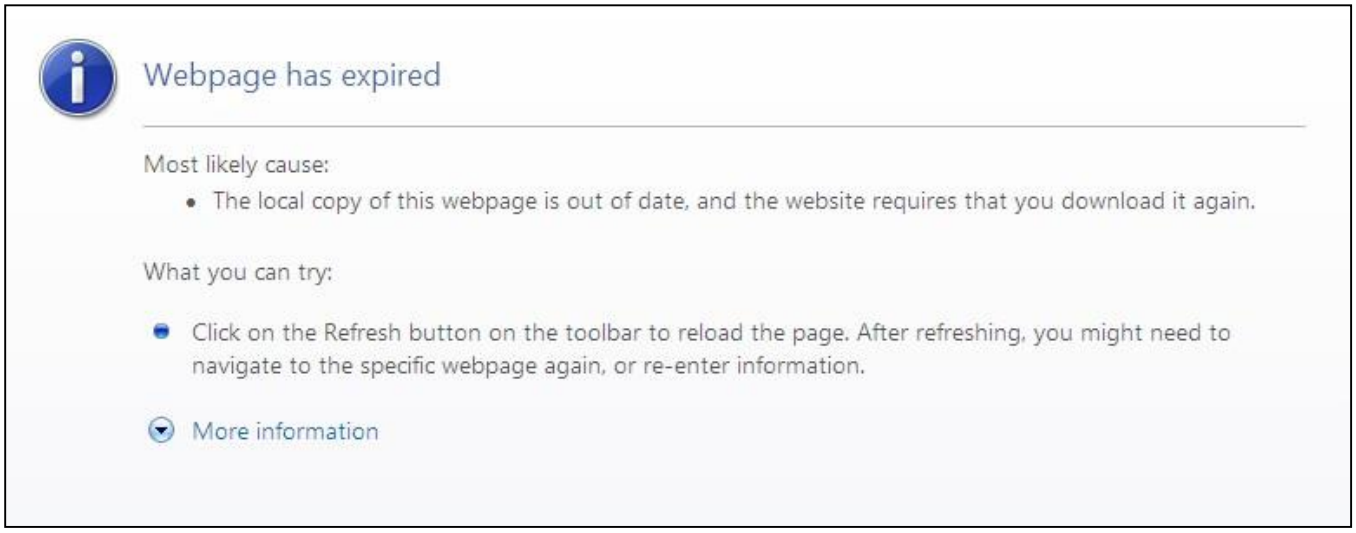
For security reasons the SAME message is displayed to anyone who fails to sign on for any of the following reasons.

1) Username is incorrect
2) Password is incorrect
3) Account has been suspended (too many incorrect sign-on attempts, password aging, or manual administrator action)
4) IP address has been locked out (too many incorrect sign-on attempts, often with different usernames)

Note, the application will only indicate that access was denied, but not WHY access was denied.

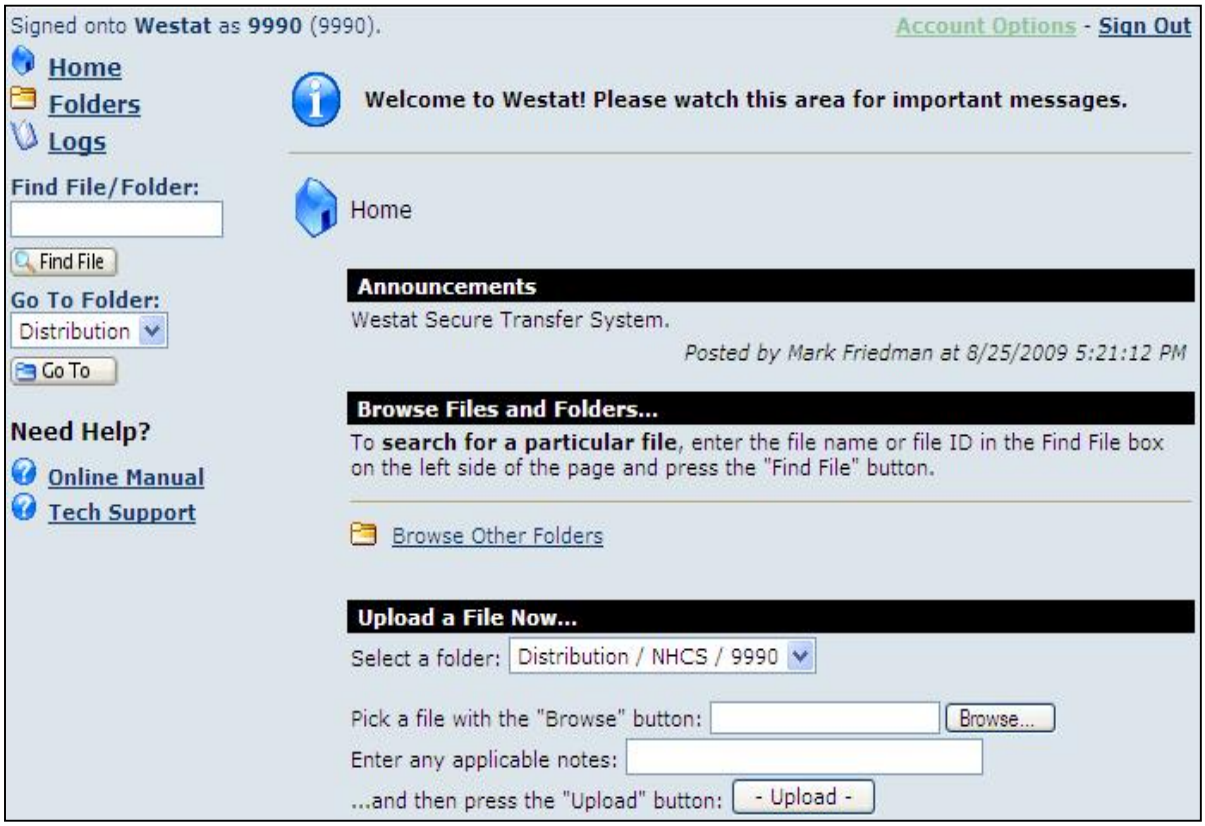
1.5.2 Webpage Has Expired

Use of the browser's Back or Forward buttons occasionally result in a "Webpage has expired" message in the browser. Clicking on Refresh often resolves the issue.



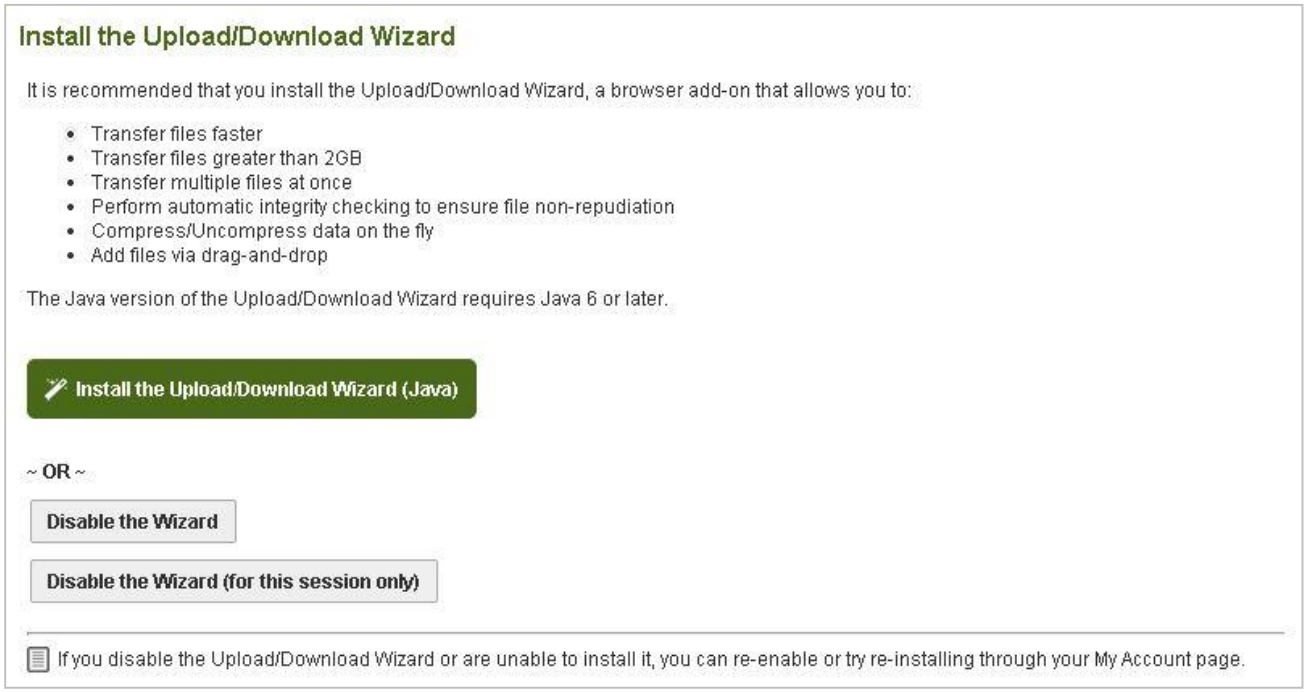
1.5.3 Warning Message When Signing On

If you cannot install the wizard or it failed to install, you may see red Warning messages alerting you that the file wizard did not load. The following section explains how you can upload files without using the Wizard.



1.5.4 Installing the Wizard on browsers other than Internet Explorer

If you are using Chrome, Firefox or other non-Internet Explorer browsers, the site will show you the JAVA installer. You will see this on your first log in.



Try to install the Java version of the wizard by clicking the install button.

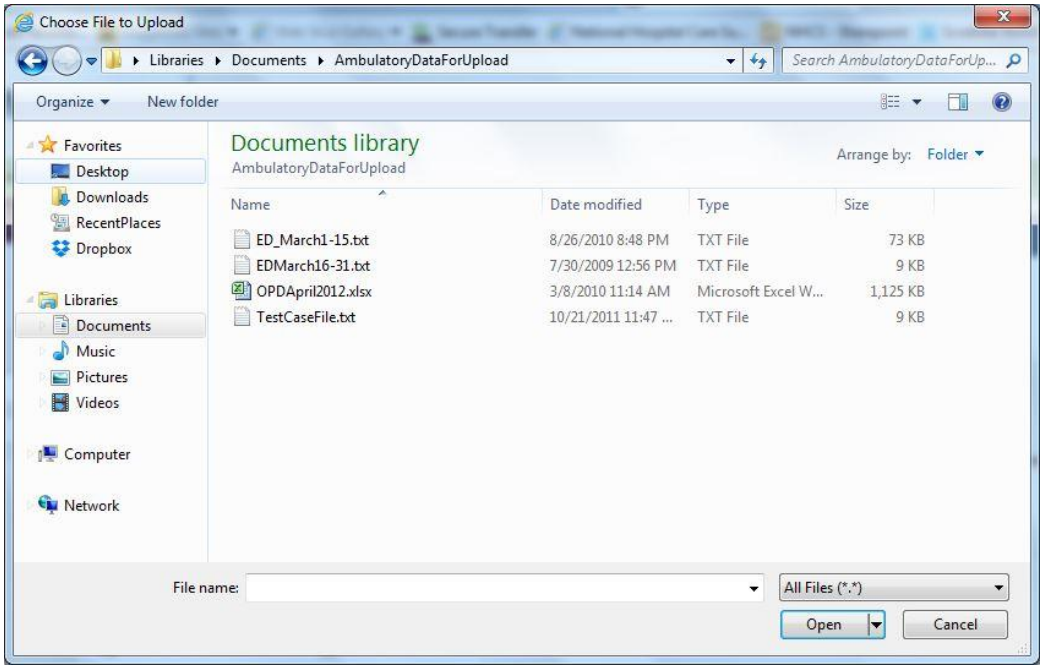
When the Java dialog pops up, click “Run” and follow the prompts.

You can then continue from “Uploading a File or Files” found on Page 5.

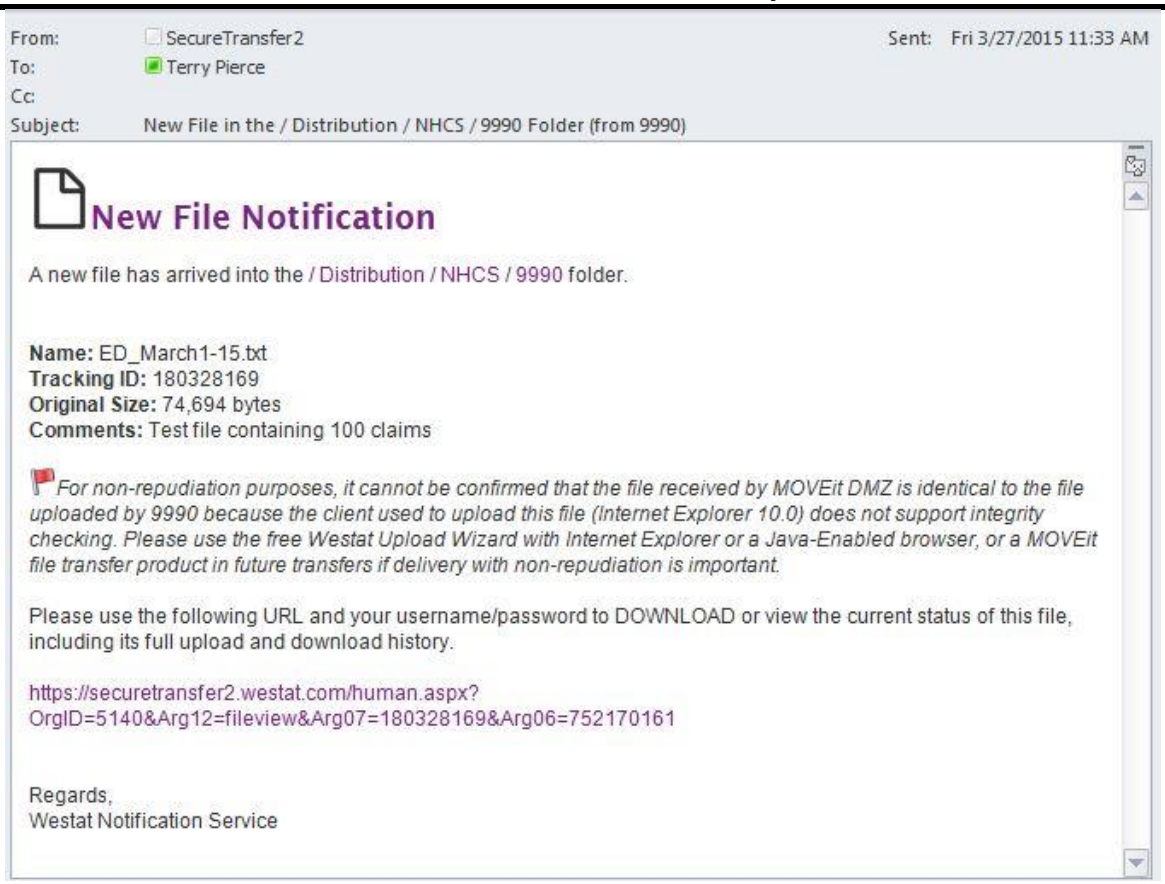
1.5.5 Uploading Files Without Using the Wizard

If you cannot install the Upload Wizard for any reason or have chosen not to, you will be presented with an alternate version of the Home Screen. At the bottom, you will see the following under “Upload a File”.

Click the “Browse” button to bring up the Dialog box shown below and then navigate to the file you are transmitting.



Enter notes regarding the file and then click the “Upload” button. Note that you can only select and upload one file at a time when the Upload Wizard is not installed. After the file has been uploaded, you will receive an email message similar to the one shown below. Note that WSTS cannot confirm the integrity of the file, since the upload Wizard was not used.



From: SecureTransfer2 Sent: Fri 3/27/2015 11:33 AM
To: Terry Pierce
Cc:
Subject: New File in the / Distribution / NHCS / 9990 Folder (from 9990)

New File Notification

A new file has arrived into the / Distribution / NHCS / 9990 folder.

Name: ED_March1-15.txt
Tracking ID: 180328169
Original Size: 74,694 bytes
Comments: Test file containing 100 claims

For non-repudiation purposes, it cannot be confirmed that the file received by MOVEit DMZ is identical to the file uploaded by 9990 because the client used to upload this file (Internet Explorer 10.0) does not support integrity checking. Please use the free Westat Upload Wizard with Internet Explorer or a Java-Enabled browser, or a MOVEit file transfer product in future transfers if delivery with non-repudiation is important.

Please use the following URL and your username/password to DOWNLOAD or view the current status of this file, including its full upload and download history.

https://securetransfer2.westat.com/human.aspx?
OrgID=5140&Arg12=fileview&Arg07=180328169&Arg06=752170161

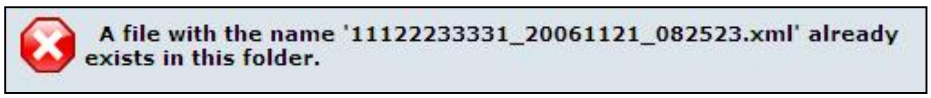
Regards,
Westat Notification Service

1.5.6 Uploading Problems

If your file(s) failed to be transmitted, you may see something on the banner like this:

You cannot upload a file with the same name if one exists in your folder.

A common reason for this error is that your session has expired or timed out. Please reconnect and try your transmission again. However, if the file exists on the server, a message like this appears on the Home screen:



1.6 Appendix

1.6.1 Supported Web Browsers

MOVEit has been tested against and fully supports the following major browsers:

- Microsoft Internet Explorer (IE) 9.0, 10.0, 11.0 (on Windows only)
- when using the ActiveX, Java, or JavaScript Wizard
- Microsoft Edge (on Windows 10 only)
- when using the JavaScript Wizard
- Mozilla FireFox (FF): Latest version (on Windows, Macintosh and RedHat Linux)
- when using the Java or JavaScript Wizard (Java - Windows/*nix/Mac OS X)
- Google Chrome: Latest version (on Windows only)
- when using the Java or JavaScript Wizard (Java - Windows/*nix/Mac OS X)
- Apple Safari: Latest version (on Macintosh only)
- when using the Java Wizard

Indicates this client ensures the integrity of transferred files and proves who uploaded and who downloaded a specific file (non-repudiation).

Use of the MOVEit Java Wizard on the Macintosh version of Firefox requires that you use the Java Preferences applet to select Java 7.

1.6.2 Supported Secure FTP/SSL Clients

MOVEit has been tested against and fully supports a large number of secure FTP clients using FTP over SSL:

- MOVEit Freely (free command-line)
- MOVEit Buddy (GUI)
- MOVEit Central (w/Admin)
- WS_FTP Professional and WS_FTP Home (GUI, version 7 and higher, Windows) (v12 & higher)
- SmartFTP(GUI, version 1.6 and higher, Windows)
- SmartFTP (free GUI, version 1.0 and higher, Windows)
- Cute FTP Pro (GUI, version 1.0 and higher, Windows)
- BitKinex (GUI, version 2.5 and higher, Windows)
- Glub FTP (GUI, Java 2.0 and higher)
- FlashFXP (GUI, version 3.0 and higher)
- IP*Works SSL (API, Windows, version 5.0)
- LFTP (free command-line, Linux, Unix, Solaris, AIX, etc.)
- NetKit (command-line, Linux, Unix, Solaris, etc.)
- SurgeFTP (command-line, FreeBSD, Linux, Macintosh, Windows, Solaris)
- C-Kermit (command-line; v8.0+, AIX, VMS, Linux, Unix, Solaris)
- AS/400 native FTPS client (OS/400 minicomputer)
- z/OS Secure Sockets FTP client(z/OS mainframe)
- TrailBlaxer ZMOD (OS/400 minicomputer)
- NetFinder (GUI, Apple)

- Sterling Commerce (batch, various)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)
- Cleo Lexicom (batch, various)
- bTrade TDAccess (batch, AIX, AS/400, HP-UX, Linux, MVS, Solaris, Windows)
- FTP-Specific Clients -cURL(command-line, AIX, HP-UX, Linux, QNX, Windows, AmigaOS, BeOS, Solaris, BSD)
- South River Technologies "WebDrive" (Windows "drive letter" - requires "passive, implicit and 'PROT P'" options)
- Stairways Software Pty Ltd. "Interarchy" (Mac "local drive" and GUI)

FTP Client Developers: Please consult the "FTP - Interoperability - Integrity Check How-To" documentation for information about how to support integrity checks with your FTP client too.

1.6.3 Supported Secure FTP/SSH (and SCP2) Clients

MOVEit has been tested against and fully supports the most popular secure FTP clients using FTP over SSH as well:

- OpenSSH sftp for *nix(free command-line, Unix - including Linux and BSD, password and client key modes)
- OpenSSH for Windows (free command-line, Windows, password and client key modes)
- OpenSSH sftp for Mac (preinstalled command-line, Mac, password and client key modes)
- OpenSSH sftp for z/OS (part of "IBM Ported Tools for z/OS", z/OS 1.4+, password and client key modes)
- Putty PSFTP, (command-line, Windows, password and client key modes)
- WS_FTP (GUI, Windows, version 7.0 and higher; version 7.62 has a compression-related bug which prevents it from uploading large, highly compressible files)
- BitKinex (GUI, version 2.5 and higher, Windows)
- F-Secure SSH (command-line, 3.2.0 Client for Unix, password and client key modes)
- FileZilla (GUI, Windows)
- SSH Communications SSH Secure Shell FTP (GUI, Windows, password and client key modes; requires setting # of transfers to 1)
- SSH Tectia Connector (Windows)
- SSH Tectia Client (Windows,AIX,HP-UX,Linux,Solaris)
- J2SSH (free Java class - requires Java 1.3+)
- Net::SFTP - Net::SSH::Perl (free Perl module for Unix)
- MacSSH (GUI, Mac, password mode only)
- Fugu (free GUI, Mac, password mode only)
- Cyberduck (free GUI, Mac, password and client key modes)
- Rbrowser (GUI, Mac, password mode only)
- Transmit2 (GUI, Mac, password and client key modes)

- gftp (GUI, Linux, password and client key modes)
- Magnetk LLC sftpdrive (Windows "drive letter", password mode only)
- South River Technologies "WebDrive" (Windows "drive letter", password mode only)
- Cyclone Commerce Interchange (Solaris, client key mode only)
- Stairways Software Pty Ltd. "Interarchy" (Mac "local drive" and GUI, password mode only)
- Miklos Szeredi's "SSH FileSystem", a.k.a. "SSHFS" (*nix "mount file system" utility, password and client key modes; requires OpenSSH and FUSE)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)

Note: Two of the clients above, (OpenSSH for Windows & SSH Communications), are capable of uploading files using multiple independent threads which may send blocks of data non-sequentially. This mode is not supported by MOVEit SSH and should be disabled using the "-R1" command-line option.

In addition to the SFTP clients listed above, MOVEit has limited support for some SCP clients. This list of clients is limited to those that implement the SCP2 protocol, which uses SFTP as its underlying transfer mechanism. MOVEit has been successfully tested with these SCP clients:

- PSCP, (command-line, Windows, password and client key modes)
- F-Secure SCP2 (command-line, 3.2.0 Client for Unix, password and client key modes)
- WinSCP (command-line; SFTP mode)

Indicates this client ensures the integrity of transferred files and proves who uploaded and who downloaded a specific file (non-repudiation).

MOVEit Central and MOVEit is the FIRST client and server solution to offer FTP over SSL (ftps) and FTP over SSH (sftp) support in a single product. MOVEit was also the first family of Windows-based products to support all three modes of FTP over SSL transport. Our commitment to full implementation of industry security standards ensures that a wide variety of clients using the FTP protocol over SSL or/and SSH can exchange files with MOVEit.

1.6.3.1 Additional FTP over SSL Information:

The three modes of FTP over SSL are:

- TLS-P (aka "Explicit, Always", "SSL" and "TLS")
- TLS-C (aka "Explicit, Negotiate")
- Implicit (usually connected over port 990)

Most administrators prefer their clients to connect to MOVEit using the IMPLICIT mode of FTP over SSL (TCP port 990). There are two advantages implicit mode enjoys over the other two modes due to its requirement to establish a secure channel before passing any commands at all. (The other two modes connect insecurely on TCP port 21, then build up a secure channel before passing sensitive information.)

- Implicit mode offers fewer interoperability problems because there are almost no options to haggle over during the connection.

- Implicit mode protects against the case where a fumble-fingered user or a poorly written script "leaks" a username, password or other information during the non-secure negotiation of the channel.

Please see the "FTP Server" section of this manual for additional information about supported FTP clients as well as a technical description of secure FTP and what a secure FTP client must do in general to be supported by MOVEit's secure FTP server.

1.6.4 Supported AS2/AS3 Clients

MOVEit supports any AS2 client that has been "Drummond" or "eBusinessReady" certified; the software MOVEit uses to handle incoming AS2 files and MDNs has itself been certified "eBusinessReady" under a program now managed by Drummond.

AS3 clients are just FTP/SSL clients as far as MOVEit is concerned. MOVEit Central handles the encryption/decryption, signing and verification of AS files in either case.