

Michigan Department of Health and Human Services

Electronic Submissions Manual

June 26, 2023

Submitting
Electronic Health Care Transactions

Table of Contents

| | |
|---------------------------------------------------------------------|----|
| Section 1 - Introduction..... | 4 |
| 1.1 Medicaid Billing Agents | 4 |
| Section 2 - Resources | 5 |
| Section 4 - File Transfer Service (FTS)..... | 7 |
| 4.1 FTS - Internet Connection | 7 |
| 4.2 FTS Web Client (https) Java and Non-Java Mode | 7 |
| 4.2.1 PC Setup | 7 |
| 4.2.2 Logging onto the MDHHS Internet Connection | 9 |
| 4.2.3 Downloading Files from FTS..... | 10 |
| 4.2.4 Uploading Files to the FTS..... | 11 |
| Section 5 – File Transfer Service (FTS) - SFTP, FTPS (FTP/SSL)..... | 15 |
| 5.1 Overview | 15 |
| 5.2 Software | 15 |
| 5.3 Connecting Issues..... | 15 |
| 5.4 Change Directory and Filename Requirements | 15 |
| Section 6 - ACA CORE Transport Modes..... | 16 |
| 6.1 Connectivity Overview | 16 |
| 6.2 System Availability..... | 17 |
| 6.2.1.1 Real-time Inquiry Response..... | 17 |
| 6.2.2 Batch Inquiry Response..... | 17 |
| 6.3 Process Flows | 17 |
| 6.3.1 Real-time Request and Response Handling | 17 |
| 6.3.2 Batch Request and Response Handling..... | 19 |
| 6.4 Transmission Administrative Procedures..... | 23 |
| 6.5 Retransmission Procedures..... | 23 |
| 6.6 Communication Protocols..... | 23 |
| 6.6.1 HTTP MIME Multipart | 23 |
| 6.6.2 SOAP + WSDL | 23 |
| 6.6.3 Header Requirements..... | 24 |
| 6.6.4 Error Reporting | 25 |
| Section 7 - Passwords..... | 26 |
| 7.1 SOAP+WSDL and MIME Multipart Passwords | 26 |

Electronic Submissions Manual (ESM)

| | | |
|-------------------------------------------------------------------|-------------------------------------------------|----|
| 7.1.1 | Password Maintenance..... | 27 |
| 7.1.2 | Password Replacement..... | 28 |
| 7.3 | File Transfer Service (FTS) Passwords..... | 29 |
| 7.3.1 | Change Password function..... | 29 |
| 7.3.2 | Unknown Password..... | 29 |
| Section 8 - Electronic Batch Web Upload Through CHAMPS..... | | 29 |
| Section 9 - B2B Testing..... | | 33 |
| 9.1 | Billing Agent IDs for New Trading Partners..... | 33 |
| 9.2 | 5010 Test Instructions by Transaction..... | 33 |
| 9.3 | Stage 1 - Ramp Manager Testing..... | 33 |
| 9.4 | Stage 2 - CHAMPS B2B Testing..... | 33 |
| Section 10 - 999 Acknowledgement File..... | | 34 |
| Section 11 - Class ID/Filename..... | | 37 |
| 11.1 | *Notes Regarding TEST Files..... | 38 |
| Addendum A. File Transfer Service (FTS) internet connections..... | | 39 |
| Addendum B. File Transfer Service (FTS) web client..... | | 40 |
| Addendum C: Put Command formats..... | | 45 |

Section 1 - Introduction

This Electronic Submission Manual (ESM) describes how to submit data electronically to the Michigan Department of Health and Human Services (MDHHS).

Section 4, File Transfer Service (FTS), offers a secure internet connection using HTTPS (website), SFTP, or FTP (FTP/SSL) EXPLICIT.

Section 6 - ACA CORE required SOAP+WSDL or HTTP/S MIME transport modes.

Instructions are also included on how to submit transaction files directly into the CHAMPS web portal using Electronic Batch Web Upload through CHAMPS.

Regardless of the method used to exchange Medicaid transactions or queries, **you must first test your electronic transactions with MDHHS to ensure adherence to national and Michigan standards**, and to reduce errors in your production file submissions to MDHHS.

The use or storage of data on any system or servers outside of the United States is expressly prohibited pursuant to the State of Michigan and DTMB policy.

This document replaces all previous MDHHS Electronic Submission Manuals.

1.1 Medicaid Billing Agents

Any entity that submits claims electronically to Michigan Medicaid is considered a billing agent for Michigan Medicaid. Billing agents can be software companies, providers, clearinghouses, etc.

This manual will help all Medicaid billing agents in the submission of electronic files. If you do not have a billing agent ID, please refer to the Resources in the following section of this manual.

There are several advantages to submitting claims and other data electronically:

- ❖ Electronic data reduces the need to re-type information;
- ❖ Electronic data eliminates the amount of errors;
- ❖ Electronic claims can be processed and paid much more quickly;
- ❖ Electronic claims can be posted more easily; and
- ❖ Electronic claims can be used for additional services, such as claim status information.

This manual provides the necessary instructions for the actual transmission and receipt of electronic information. Only billing agents will be able to send and retrieve information with MDHHS.

Any entity submitting a 270 eligibility or a 276 claim status request must first be associated in CHAMPS with the Billing Agent or Trading Partner that originated the claim.

Section 2 - Resources

MDHHS informational resources for electronic billing can be found at the MDHHS website: <http://michigan.gov/tradingpartners> >> Electronic Submissions Transactions

Please make sure to review the documentation available on the website before contacting MDHHS directly. This ESM and other resources are available at the MDHHS website, including:

- ❖ CHAMPS Testing Instructions for 837 Fee for Service (FFS) Claims, 837 Encounters, NCPDP files, and 270, 276, and 278 Requests
- ❖ Electronic Updates
- ❖ Michigan Companion Guides
- ❖ 835 Electronic Remittance Advice Instructions
- ❖ Links to Additional Information about electronic Health Care transactions

Michigan's *EDI Services*, *B2B Testing*, *Provider Support*, and *Encounter* teams are available to assist you:

EDI Services: Michigan Medicaid's EDI Services Section will handle all questions related to electronic Fee for Service (FFS) claims file exchange and FTS issues.

Website: <http://michigan.gov/tradingpartners>

EDI Services Email: AutomatedBilling@michigan.gov

Business to Business (B2B): The B2B Test Team will handle test processing of electronic transactions. Trading Partners (including new Providers, Billing Agents, Clearinghouses, and Health Plans) are required to initially test before sending electronic transactions.

Michigan provides two test systems for this purpose:

1. *Ramp Manager* (format and syntax testing) and
2. *CHAMPS B2B* (claim adjudication testing).

Please access the MDHHS website for testing information, and contact *EDI Services* or the *B2B Test Team* to obtain test system access credentials and further instructions.

Website for Testing Information: <http://michigan.gov/tradingpartners> >> Electronic Submissions Transactions >> B2B Testing

B2B Testing Email: MDHHS-B2B-Testing@michigan.gov

Provider Support: The Provider Support Section will handle all billing and claim denial questions.

Website: www.Michigan.gov/MedicaidProviders

Provider Support Line: 1-800-292-2550

Provider Support Email: ProviderSupport@michigan.gov

Encounter The Encounter Team will handle all electronic questions related to Encounter file submission and FTS issues for Trading Partners. The Encounter team also handles issues related to NCPDP submissions.

Encounter Support MDHHEncounterData@michigan.gov

Section 3 – Software and Programming

Michigan Medicaid does not provide software to billing agents for electronic claims creation. All billing agents must have a way to create or produce electronic files to submit to Michigan Medicaid.

Section 4 - File Transfer Service (FTS)

MDHHS has established an Internet connection to the FTS, which is a Secure Sockets Layer connection. This connection is independent of the platform used to transmit data.

Billing agents will use the FTS to submit and retrieve files electronically with MDHHS. Every billing agent receives an FTS “mailbox”, which is where their files are stored and maintained. You can access this mailbox to send and retrieve files through the Internet connection.

4.1 FTS - Internet Connection

The FTS offers 3 types of secure internet connections: SFTP, FTPS (FTP/SSL) and HTTPS (website). See Addendum A for details.

After receiving an FTS User ID, users are required to change the temporary password using the FTS Website. New or reset FTS User ID are set to “Force password change on next logon”

Users MUST change their password through the FTS Web sites before they can login using SFTP, FTP/SSL/TLS, or Web site (HTTPS).

For Internet users: <https://MiFTS.state.mi.us> (internet)

When connecting to this web page it will automatically take you to the Change Password process.

4.2 FTS Web Client (HTTPS) Java and Non-Java Mode

Web-based access to the FTS can be run using Java mode or non-Java mode. The use of Java mode will provide additional features compared to running in non-Java mode.

See Addendum B for FTS Web client and reasons to use Java.

The Chrome internet browser does not support Java, so FTS will run in non-Java mode when accessed using Chrome. Internet Explorer and Firefox internet browsers will allow the user to run using Java. Consult your organization’s IT support team with questions about the browser available at your work location.

4.2.1 PC Setup

1. You must have an Internet Browser installed on your PC. FTS has been tested on Windows 7 with the following browsers:
 - ❖ Microsoft Edge
 - ❖ Internet Explorer 8, 10 and 11
 - ❖ Firefox 38
 - ❖ Chrome 43

Note: Using an untested Internet Browser may cause some screens to appear

different than the screens you see in this documentation, which are based on Chrome (for Non-Java mode) and Internet Explorer (for Java mode).

2. Make sure you have a reliable Internet Service Provider (ISP) for your PC's Internet connection.
3. For the most reliable and fastest transfers, use a high-speed internet connection from your PC. This is a LAN, T1, DSL, or Cable connection to the internet.

4.2.2 Logging onto the MDHHS Internet Connection

1. Log onto <https://MiFTS.state.mi.us>

DTMB File Transfer Service

MICHIGAN.GOV
Michigan's Official Website

State of Michigan FTS Web Client

Logon to State of Michigan FTS Web Client

Please enter your credentials below

Username:

Password:

WARNING!
THIS SYSTEM CONTAINS U.S.GOVERNMENT INFORMATION.
By accessing and using this computer system you are consenting to system

Logon

Powered by MessageWay

IPSWITCH
FILE TRANSFER

MI.gov

2. All Billing Agents must contact MDHHS to obtain unique credentials for accessing the FTS.
 - To logon, enter your MDHHS assigned billing agent FTS Username in the **Username** box, such as **DCH????** using all caps (where “????” is your unique Username assigned by MDHHS).
 - In the **Password** box, enter your password. Then, click on the “**Logon**” button.
3. If you need to have your FTS password reset, please send a password reset request to AutomatedBilling@michigan.gov

4.2.3 Downloading Files from FTS

Billing agents can download response files from their FTS “mailbox”. These files include TA1, 999 Acknowledgement files, 835 files, etc. Your available messages (files) to download are displayed on the **Available** tab when you log on.

DTMB File Transfer Service

MICHIGAN.GOV Michigan's Official Website

State of Michigan FTS Web Client. Home Help Change Password Logout

Mailbox: [redacted] Filename: [input] Class ID: [input] Search

Available Downloaded Canceled Uploaded Upload Message

Download As Zip Download As Binary Download As Text Cancel

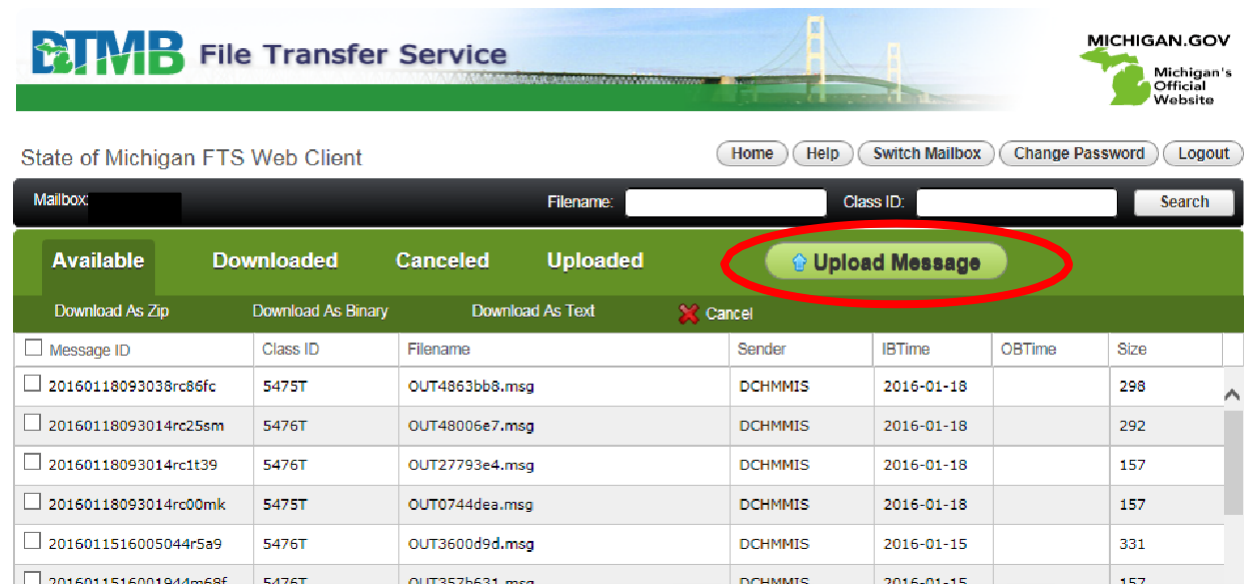
| Message ID | Class ID | Filename | Sender | ITime | OTime | Size |
|-----------------------------------------------|----------|---------------------------|---------|------------|-------|----------|
| <input type="checkbox"/> 20170131190057jtm2rs | 4956 | | | 2017-01-31 | | 20203334 |
| <input type="checkbox"/> 20170131161724yfgnkq | 5890T | M20170131161724yfgnkq.dat | DOHMMIS | 2017-01-31 | | 3971 |
| <input type="checkbox"/> 20170131161723yif9z0 | 4950T | M20170131161723yif9z0.dat | DOHMMIS | 2017-01-31 | | 561 |
| <input type="checkbox"/> 2017013108300981j166 | 5476T | 5476T.170131.0830.09590 | DOHMMIS | 2017-01-31 | | 292 |
| <input type="checkbox"/> 2017013108300981hbku | 5414T | 5414T.170131.0830.09411 | DOHMMIS | 2017-01-31 | | 291 |
| <input type="checkbox"/> 2017013108300981b36t | 5414T | 5414T.170131.0830.09119 | DOHMMIS | 2017-01-31 | | 157 |
| <input type="checkbox"/> 20170131083006813hzf | 5776T | 5776T.170131.0830.06047 | DOHMMIS | 2017-01-31 | | 296 |
| <input type="checkbox"/> 2017013108300580v3ys | 5776T | 5776T.170131.0830.05827 | DOHMMIS | 2017-01-31 | | 157 |
| <input type="checkbox"/> 2017013108300280qysz | 5475T | 5475T.170131.0830.02681 | DOHMMIS | 2017-01-31 | | 157 |
| <input type="checkbox"/> 2017013108300280mz2c | 5476T | 5476T.170131.0830.02534 | DOHMMIS | 2017-01-31 | | 157 |

1. Check the box next to the “Message ID” you would like to download.
2. Select one of the following: *Download As Zip*, *Download As Binary*, or *Download As Text*, in the dark green band.

Once a file downloads, it will no longer appear on the **Available** tab; users will need to click on the **Downloaded** tab to re-download previously downloaded files.

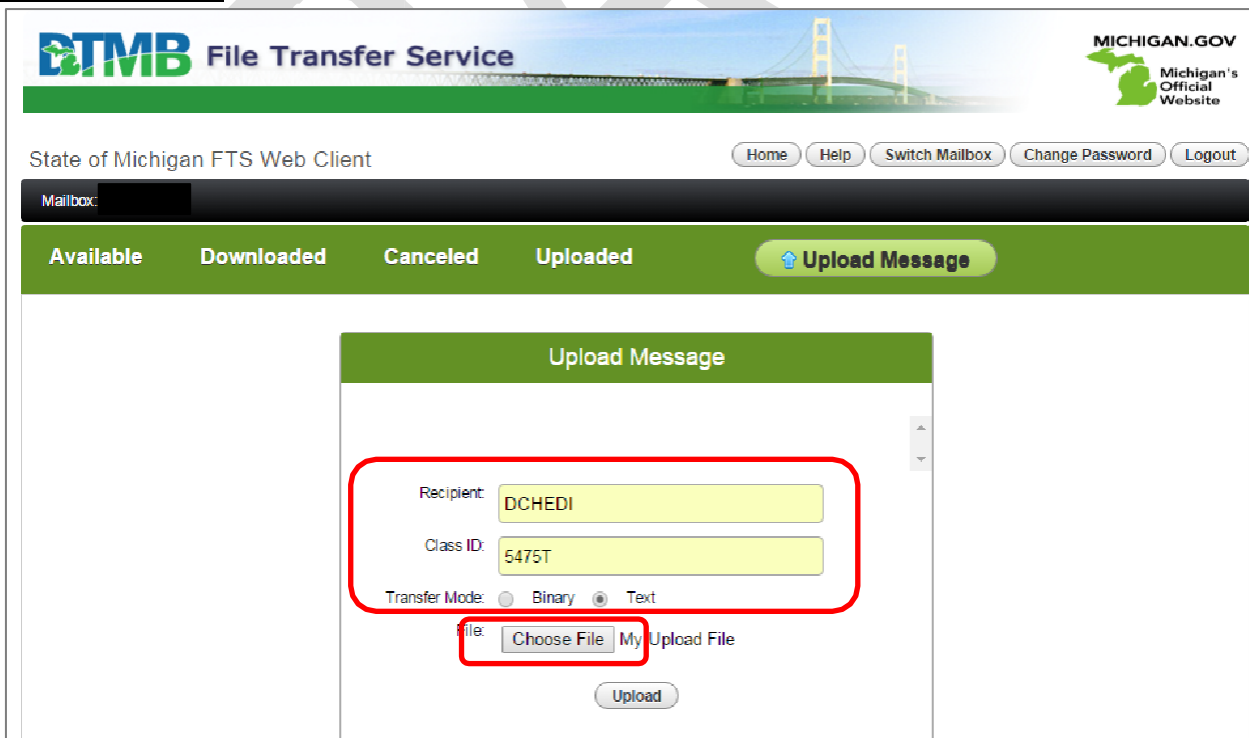
4.2.4 Uploading Files to the FTS

1. To start the Uploading process, click on **Upload Message**:



2. The following screen will appear; complete the screen entries (see *Reference Notes*, below) and use the **Choose File** or **Browse...** button to select a file from your PC.

Non-Java Mode:



Java Mode:

The screenshot shows the DTMB File Transfer Service web client interface. At the top, there is a banner with the DTMB logo and the text 'File Transfer Service'. To the right of the banner is the Michigan.gov logo and the text 'MICHIGAN.GOV Michigan's Official Website'. Below the banner, there is a navigation bar with buttons for 'Home', 'Help', 'Switch Mailbox', 'Change Password', and 'Logout'. Below the navigation bar, there is a 'Mailbox:' label and a dropdown menu. Below the dropdown menu, there is a green bar with tabs for 'Available', 'Downloaded', 'Canceled', and 'Uploaded', and an 'Upload Message' button. Below the green bar, there is a white box with a green header 'Upload Message'. Inside the white box, there is a form with the following fields: 'Recipient' (DCHEDI), 'Class ID' (5475), 'Transfer Mode' (Binary and Text), and 'File' (C:\Files Folder\My Upload File). A red box highlights the 'Recipient', 'Class ID', and 'Transfer Mode' fields, and another red box highlights the 'Browse...' button. Below the form, there is an 'Upload' button.

Reference Notes:

- ❖ **Recipient** will be “DCHEDI” or “DCHBULL” for most files that you are uploading to MDHHS.
- ❖ **Class ID** is the MDHHS File Name of the file that you are submitting. Please see *Section 11. CLASS ID/FILENAME* for a listing of Class ID/File Names (ex.: **5475** is the Class ID/File Name for 837 FFS files). Please note that all test files must use “T” as the fifth digit of the Class ID/File Name (ex.: **5475T**).
- ❖ **Transfer Mode** needs to be changed to “Text” if Recipient is “DCHEDI”.
- ❖ **File** is the file that you are submitting to MDHHS through the FTS. You will need to click on the **Choose File** or **Browse...** button to select the file to be uploaded from your PC.

1. When you have selected your file, click the **Upload** button to submit the file.
2. Once the upload is complete, the following display and message, in red, will appear:

Non-Java Mode:

The screenshot displays the DTMB File Transfer Service web client interface. At the top, the DTMB logo and 'File Transfer Service' text are visible, along with the Michigan.gov logo and 'Michigan's Official Website' tagline. The page title is 'State of Michigan FTS Web Client'. A navigation bar includes buttons for 'Home', 'Help', 'Switch Mailbox', 'Change Password', and 'Logout'. Below this is a 'Mailbox:' dropdown menu. The main content area features a green navigation bar with tabs for 'Available', 'Downloaded', 'Canceled', and 'Uploaded', and a prominent 'Upload Message' button. A modal window titled 'Upload Message' is open, showing a success message: 'Message 201601181324341727k successfully uploaded from [redacted] to DCHEDI'. The modal contains input fields for 'Recipient:' and 'Class ID:', radio buttons for 'Transfer Mode:' (with 'Binary' selected), a 'File:' section with a 'Choose File' button and 'No file chosen' text, and an 'Upload' button at the bottom.

DRAFT

Java Mode:

DTMB File Transfer Service

MICHIGAN.GOV Michigan's Official Website

State of Michigan FTS Web Client

Home Help Switch Mailbox Change Password Logout

Mailbox

Available Downloaded Canceled Uploaded Upload Message

Upload Message

Recipient: DCHEDI

Class ID: 5475T

Transfer Mode: Binary Text

File: Browse...

Upload

Hide Detail

Close All

| File Name | File Path | To | Class ID | Direction | | Status |
|----------------|-----------------|--------|----------|-----------|----------------------|-----------|
| My Upload File | C:\Files Folder | DCHEDI | 5475T | Upload | 20160118130625uDraxf | Completed |

Close

NOTE: This is not your 999-acknowledgement file.

If you are submitting a file to MDHHS and would like to verify your return acknowledgement file, you will have to go to the **Available** tab to verify that your 999-acknowledgement file has been returned for each file that you sent. The Class ID/Filename of your 999 is the same Class ID of the file you sent. (Example: An 837 claims file submitted as **5475** would receive a 999-acknowledgement file also named **5475**.)

Section 5 – File Transfer Service (FTS) - SFTP, FTPS (FTP/SSL)

5.1 Overview

The addendums have the specifics for connecting to the FTS. Also included are put command examples for billing agents using scripts.

1. Addendum A: Connect to the FTS using the IP and port information.
2. Addendum C: Put Command formats using mailbox and class id values.

5.2 Software

There is purchasable as well as freeware available for SFTP, FTPS(FTP/SSL) to use to connect to the FTS. Example freeware: FileZilla runs on Windows and Linux. Please check with your establishment on what is available for your use.

5.3 Connecting Issues

1. If you can't logon with SSLFTP, make sure you have the right port number 11250 and advanced – server type select – FTP/SSL (AUTH SSL); or with SFTP, make sure you have the right port number 2222 and advanced – server type select – SFTP/SSH.
2. If you are getting a logon OK, but don't get a directory back from your mailbox, you are having a problem with the return data port 11200. First, try turning on PASSIVE MODE; if that doesn't work, you may have a problem with your firewall.
3. If you get an error and you try automatically again, you might want to check your software if there is an option to make AUTOCONNECT = 0 and RETRIES = 0. (Refer to your user guide).

5.4 Change Directory and Filename Requirements

1. Change Directory to Mailbox (example: CD /DCHEDI)
2. Class IDs are listed in Section 11.
 - a. Note: Your source file name must be restricted to one of the four- or five-character Class-ID Filenames from the chart in Section 11 of this document (Ex.: "5475" or "5475T"). **Test** files must always use a "T" as the fifth character of the filename.
3. Once the file is moved to /DCHEDI, look in your FTS mailbox for the corresponding response file ("**5475**", in this example); the Modified date and time will be included in the name of the response file. Response files are typically sent within two hours of your submission; if no response file is received, please contact AutomatedBilling@michigan.gov.

Section 6 - ACA CORE Transport Modes

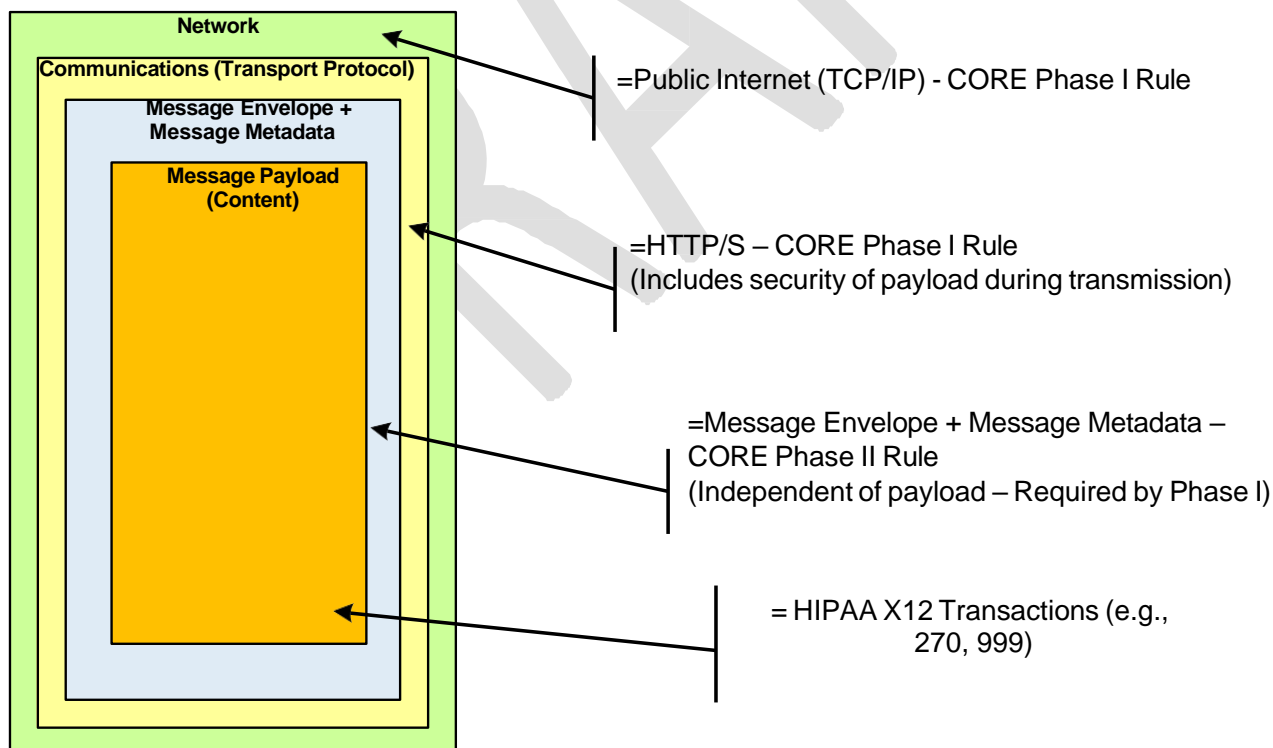
6.1 Connectivity Overview

As part of the ACA CORE requirements, CHAMPS supports batch and real-time transmission modes and the following envelope standards for the 270/271 and 276/277 transaction sets:

1. HTTP MIME Multipart (Envelope Standard A)
2. SOAP+WSDL (normative) (Envelope Standard B)

Please refer to the *Phase II CORE 270: Connectivity Rule* document at the link below for detailed information and specifications for HTTP MIME Multipart and SOAP+WSDL based interactions: <http://www.caqh.org/pdf/CLEAN5010/270-v5010.pdf>

The following diagram depicts the relationship of the transport modes to the submitted transaction.



6.2 System Availability

The MDHHS CHAMPS system is available 24 hours per day, 7 days per week, except for a regular monthly maintenance window, which starts at 6 pm on the second Saturday of each month and ends at 6 am on Sunday. For information on unscheduled outages, see the Provider Alerts page at:

www.Michigan.gov/MedicaidProviders >> Provider Alerts

6.2.1.1 Real-time Inquiry Response

A response to a real-time inquiry will be provided within 20 seconds during hours of availability.

6.2.2 Batch Inquiry Response

The v5010 271 response to a v5010 270 batch inquiry submitted by 9:00 pm Eastern time of a business day will be returned by 7:00 am Eastern time the following business day. Similarly, a v5010 277 response to a v5010 276 batch inquiry submitted by 9:00 pm Eastern time of a business day will be returned by 7:00 am Eastern time the following business day.

6.3 Process Flows

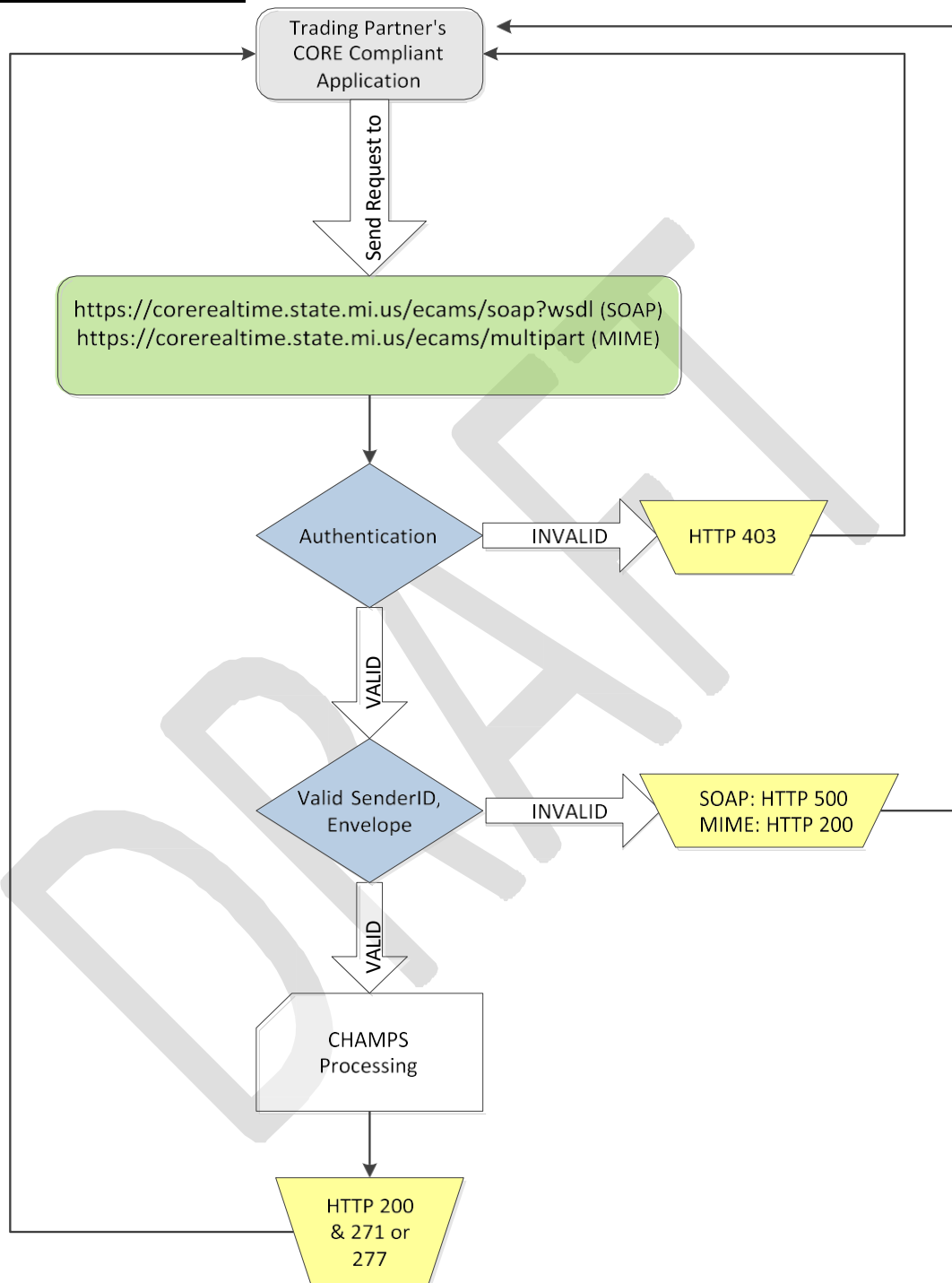
6.3.1 Real-time Request and Response Handling

HTTP/S supports a request-response message pattern, meaning that the sender submits a message and then waits for a response from the message receiver. The process for real-time request and response works as follows:

1. The user application submits a real-time SOAP or MIME request.
 - a. Submit **SOAP** to:
Real-Time Production: <https://corerealttime.state.mi.us/ecams/soap?wsdl>
Real-Time Testing: <https://corerealttimeqa.state.mi.us/ecams/soap?wsdl>
 - b. Submit **MIME** to:
Real-Time Production: <https://corerealttime.state.mi.us/ecams/multipart>
Real-Time Testing: <https://hccorerealttimeuat.state.mi.us/ecams/multipart>
2. The CHAMPS system authenticates the username and password. If unable to authenticate, an HTTP 403 Forbidden response is returned.
3. If the username and password are successfully authenticated, an HTTP 200 OK status response is returned to the user within 20 seconds along with the 271 or 277 response.
4. The CHAMPS system validates SenderId and other elements of the CORE envelope metadata.
If validation fails, the following errors are returned:
 - a. For SOAP: HTTP 500 SOAP fault with Code=Sender & Reason=Authentication Failure
 - b. For MIME: HTTP 200 with ErrorCode=Sender & ErrorMessage=Authentication Failure

The diagram below depicts the real-time request and response flow.

Real-time Process Flow

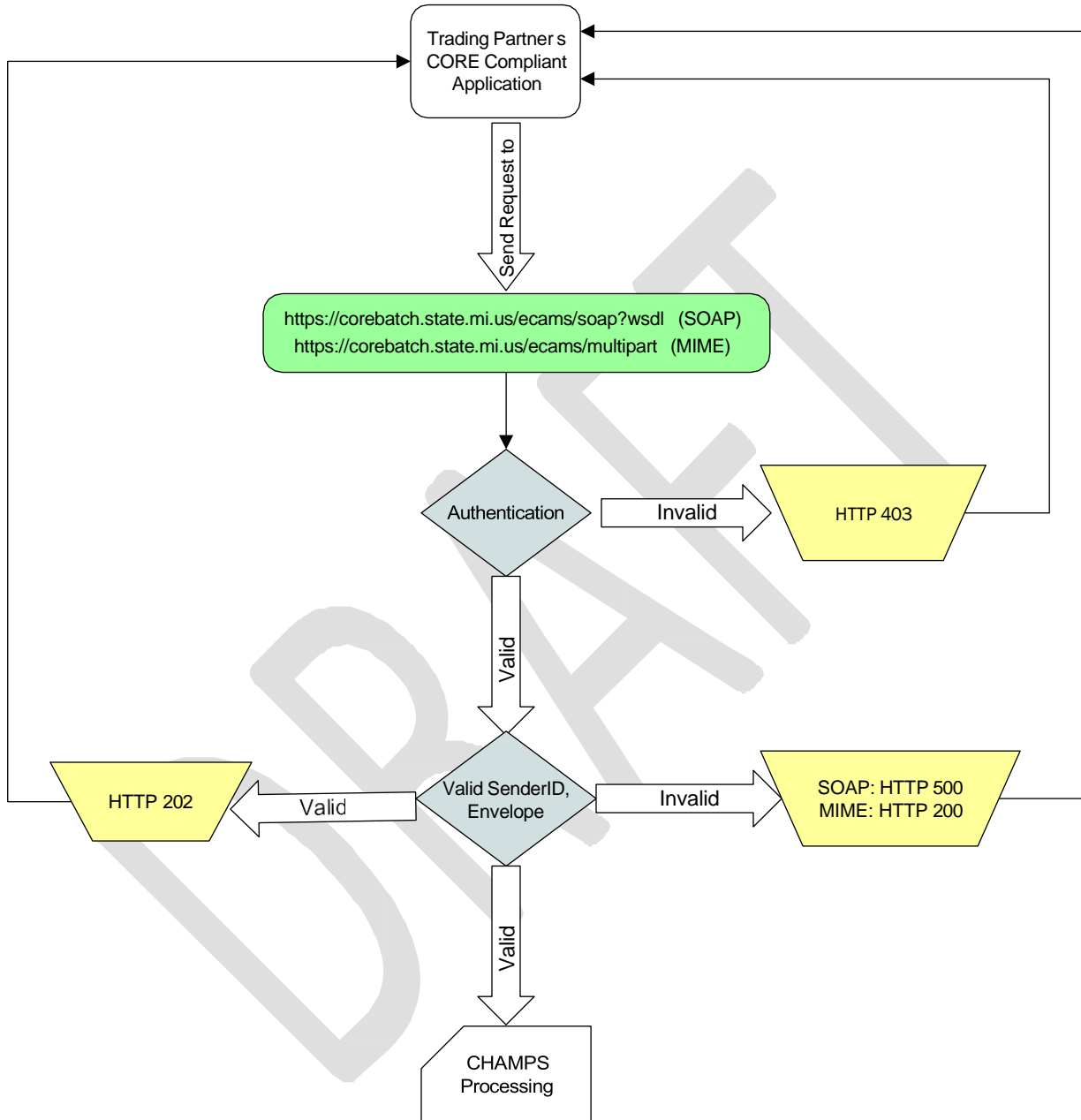


6.3.2 Batch Request and Response Handling

6.3.2.1 Initial Batch Submission

1. The user application submits a batch SOAP or MIME request.
 - a. Submit **SOAP** to:
 - Batch Production: <https://corebatch.state.mi.us/ecams/soap?wsdl>
 - Batch Testing: <https://corebatchqa.state.mi.us/ecams/soap?wsdl>
 - b. Submit **MIME** to:
 - Batch Production: <https://corebatch.state.mi.us/ecams/multipart>
 - Batch Testing: <https://corebatchqa.state.mi.us/ecams/multipart>
2. The CHAMPS system authenticates the username and password. If unable to authenticate, an HTTP 403 Forbidden response is returned.
3. The CHAMPS system validates SenderId and other elements of the CORE envelope metadata. If validation fails, the following errors are returned:
 - a. For SOAP: HTTP 500 SOAP fault with Code=Sender & Reason=Authentication Failure
 - b. For MIME: HTTP 200 with ErrorCode=Sender & ErrorMessage=Authentication Failure
4. If the username and password are successfully authenticated and the envelope metadata validated, an HTTP 202 OK status response is returned to the user indicating CHAMPS has accepted the batch submission for processing.

6.3.2.2 Batch Process Flow

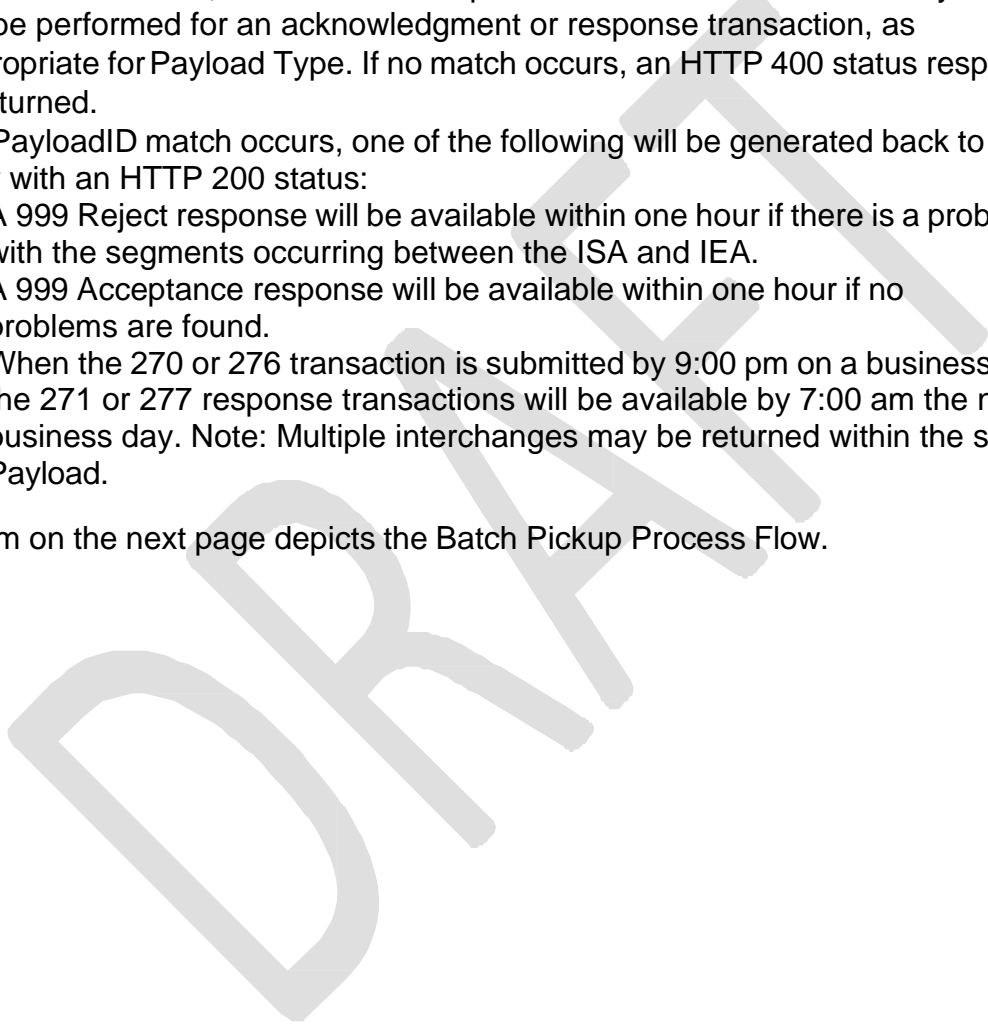


6.3.2.3 Batch Pickup

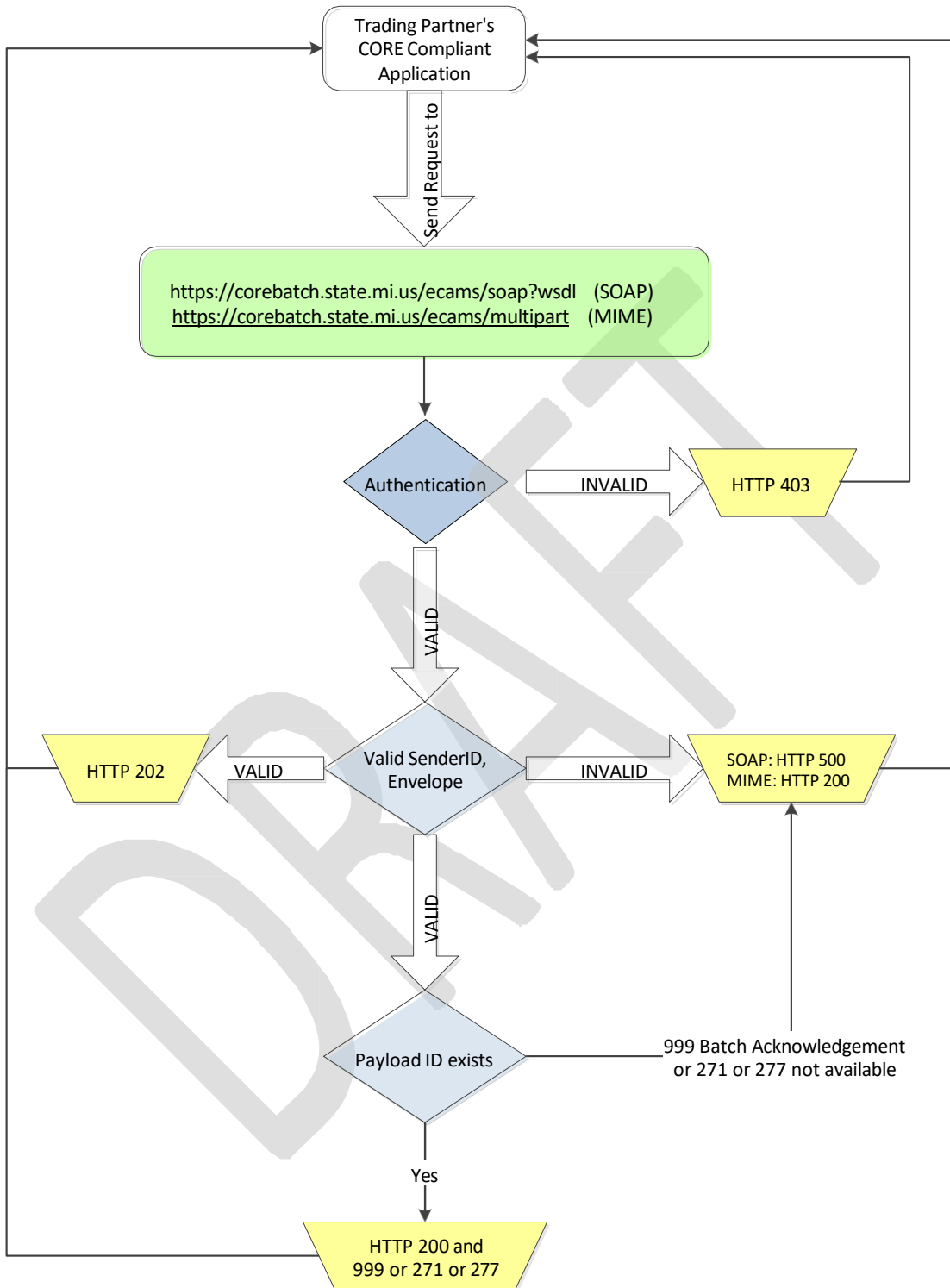
1. The user application submits a time-delayed batch pickup request.
 - a. Submit **SOAP** to:
 - Batch Production: <https://corebatch.state.mi.us/ecams/soap?wsdl>
 - Batch Testing: <https://corebatchqa.state.mi.us/ecams/soap?wsdl>
 - b. Submit **MIME** to:
 - Batch Production: <https://corebatch.state.mi.us/ecams/multipart>
 - Batch Testing: <https://corebatchqa.state.mi.us/ecams/multipart>
2. The CHAMPS system authenticates the username and password. If unable to authenticate, an HTTP 403 Forbidden response is returned.

3. The CHAMPS system validates SenderId and other elements of the CORE envelope metadata. If validation fails, the following errors are returned:
 - a. For SOAP: HTTP 500 SOAP fault with Code=Sender & Reason=Authentication Failure
4. For MIME: HTTP 200 with ErrorCode=Sender & ErrorMessage=Authentication Failure
5. If the username and password are successfully authenticated and the envelope metadata validated, an HTTP 202 response is sent and a match for PayloadID will be performed for an acknowledgment or response transaction, as appropriate for Payload Type. If no match occurs, an HTTP 400 status response is returned.
6. If a PayloadID match occurs, one of the following will be generated back to the user with an HTTP 200 status:
 - a. A 999 Reject response will be available within one hour if there is a problem with the segments occurring between the ISA and IEA.
 - b. A 999 Acceptance response will be available within one hour if no problems are found.
 - c. When the 270 or 276 transaction is submitted by 9:00 pm on a business day, the 271 or 277 response transactions will be available by 7:00 am the next business day. Note: Multiple interchanges may be returned within the same Payload.

The diagram on the next page depicts the Batch Pickup Process Flow.



6.3.2.4 Batch Pickup Process Flow



6.4 Transmission Administrative Procedures

Response Times: A response to a real-time inquiry will be provided within 20 seconds during hours of availability. A response to a batch inquiry submitted by 9:00 pm on a business day will be provided by 7:00 am the following business day.

6.5 Retransmission Procedures

If a real-time response message is not received within the 60-second response period, the submitter's system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.

If no real-time response is received after the second attempt, the submitter's system should submit no more than 5 duplicate transactions within the next 15 minutes. If the additional attempt results in the same timeout termination, the submitter's system should notify the submitter to contact MDHHS directly to determine if system availability problems exist or if there are known internet traffic constraints causing the delay. Please verify your file contents before any further resubmission.

6.6 Communication Protocols

6.6.1 HTTP MIME Multipart

MDHHS supports standard HTTP MIME messages. The MIME format used must be that of multipart/form-data. Responses to transactions sent in this manner will also be returned as multipart/form-data.

6.6.2 SOAP + WSDL

MDHHS also supports transactions formatted according to the Simple Object Access Protocol (SOAP) conforming to standards set for the Web Services Description Language (WSDL) for XML envelope formatting, submission, and retrieval.

- ❖ SOAP + WSDL XML Schema
The XML schema definition set forth by CORE is located at:
<http://www.cagh.org/SOAP/WSDL/CORERule2.2.0.xsd>

6.6.3 Header Requirements

The envelope metadata requirements are described briefly in the table below.

| Field | Accepted Values | Comment |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PayloadType | X12_270_Request_005010X279A1 X12_005010_Request_Batch_Results_271 X12_276_Request_005010X212 X12_005010_Request_Batch_Results_277 X12_835_Request_005010X221 X12_TA1_Response_00501X231A1 X12_999_Response_005010X231A1 | Real-time & batch submissions Batch results retrieval for 270/271 Real-time & batch submissions Batch results retrieval for 276/277 Batch retrieval for 835 (RA) TA1 response (real-time) 999 response (real-time) |
| ProcessingMode | RealTimeBatch | Batch used for either submission or pickup |
| PayloadID | PayloadID will conform to ISO UUID standards (described at ftp://ftp.rfceditor.org/in-notes/rfc4122.txt), with hexadecimal notation. | Generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address33, to ensure uniqueness. |
| Payload Length | Length of the X12 document | Required only if ProcessingMode is Batch; otherwise do not send. |
| TimeStamp | YYYY-MM-DDTHH:MM:SSZ | See: http://www.w3.org/TR/xmlschema11-2/#dateTime |
| User Name | MDHHS Assigned | For SOAP+WSDL and MIME Multipart use only. |
| Password | MDHHS Assigned | For SOAP+WSDL and MIME Multipart use only. |
| SenderID | MDHHS Assigned | This is assigned based on how you are enrolled in CHAMPS. It will be your NPI number, Provider ID, or FTS Username ID |
| ReceiverID | D00111 | This is the Michigan Medicaid receiver ID. |
| CORERuleVersion | 2.2.0 | |

| Field | Accepted Values | Comment |
|----------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Checksum | Checksum of the X12 document | Algorithm is SHA-1; encoding is Hex; required only if ProcessingMode is Batch. Checksum must be computed only on the payload and not on the metadata. Do not send for Real-time. |
| Payload | | Contains the X12 request. |

6.6.4 Error Reporting

The HTTP and envelope processing status and error codes are described briefly here. For comprehensive instructions on using the SOAP+WSDL and MIME Multipart transport protocols, please use the web references provided earlier in this section in addition to the information provided here.

6.6.4.1 HTTP Status and Error Codes

The HTTP status and error codes included in the following table represent only a few of the commonly used status and error codes in the standard. An exhaustive list of HTTP Status Codes and descriptions are included in the HTTP specification at:

<http://tools.ietf.org/html/rfc2616#section-6.1.1>

| HTTP Status/Error Codes (Normative, Not Comprehensive) | Status Code Description (Intended Use) |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| 200 OK | Success |
| 202 Accepted | Batch file submission has been accepted (but not necessarily processed) |
| 400 Bad Request | Incorrectly formatted HTTP headers |
| 403 Forbidden | Access denied |
| 500 Internal Server Error | The webserver encountered a processing error, or there was a SOAP fault (in case of SOAP envelope method) |
| 5xx Server errors | Standard set of server-side errors (e.g. 503 Service Unavailable) |

6.6.4.2 Envelope Processing Status and Error Codes

When SOAP is used, some of the CORE-compliant Envelope Processing errors map to SOAP Faults; refer to: <https://www.w3.org/TR/soap12-part1/>

To handle CORE-compliant envelope processing status and error codes, two fields called ErrorCode and ErrorMessage are included in the CORE-compliant Envelope. ErrorMessage is a free form text field that describes the error (for troubleshooting and logging). When an error occurs, PayloadType is set to CoreEnvelopeError.

The following table shows commonly used error codes and descriptions.

| CORE-compliant Envelope Processing Status/Error Codes (Normative, Comprehensive) | Status Code Description (Intended Use) |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Success | Envelope was processed successfully. |
| <FieldName>Illegal | Illegal value provided for <FieldName>. |
| <FieldName>Required | The field <FieldName> is required but was not provided. |
| <FieldName>NotUnderstood | The field <FieldName> is not understood at the receiver. In the case of SOAP, this error is returned as a NotUnderstood SOAP fault. |
| VersionMismatch | The version of the envelope sent is not acceptable to the receiver. If the SOAP version is not valid at the receiver, a SOAP fault is returned with this fault code. |
| Unauthorized | The username/password or Client certificate could not be verified. |
| ChecksumMismatched | The checksum value computed on the recipient did not match the value that was sent in the envelope. |
| Sender | The envelope sent by the sender did not conform to the expected format. In the case of SOAP, this error should be sent as a SOAP fault with "Sender" fault code. |
| Receiver | The message could not be processed for reasons attributable to the Receiver (e.g., the upstream process is not reachable). In the case of SOAP, this error should be sent as a SOAP fault with "Receiver" fault code. |

Section 7 - Passwords

7.1 SOAP+WSDL and MIME Multipart Passwords

A username and password are required to authenticate the submitted transaction request when using the SOAP+WSDL or MIME Multipart modes. Passwords must be changed every 90 days.

- ❖ The Initial request for a SOAP or MIME password must be sent to Automated Billing at: AutomatedBilling@michigan.gov with a subject line of "CORE Password Request".
- ❖ Automated Billing will reply with a temporary password, see 7.1.1 on how to set up a personal password.
- ❖ Trading Partners can only reset their password using CHAMPS password maintenance screens. Please note, anyone with a Domain Administrator CHAMPS profile in your organization has the authority to request password resets for your organization.

7.1.1 Password Maintenance

To change your personal (or temporary) SOAP or MIME password:

1. Log in to CHAMPS; select the **My Inbox** tab;
2. Select **EDI Password Maintenance**;
3. Enter your old password, new password, and confirm new password;
4. Choose security questions and answers;
5. Enter the displayed security code in box;
6. Click the **Submit** button in the upper-left portion of the screen.

The **Change Password** screen is shown below:

CHAMPS

My Inbox Admin

Provider Portal

Close Submit

Change Password

Password Policy

- Must be 8-32 characters long
- Must include at least one letter and one number
- Must have special characters or punctuation (for example: !\$#%)
- Must not match the UserID or the previous three passwords

User Login ID: m

Old Password:

New Password:

Confirm Password:

Do you wish to change your Security question and Answer? Yes No

c 5DB2 F

Reload

7.1.2 Password Replacement

To replace a lost SOAP or MIME password, your designated CHAMPS Domain Administrator must request a temporary password as follows:

1. Login to CHAMPS using their Domain Administrator profile;
2. Select the **My Inbox** tab;
3. Select **EDI Forgot Password** (shown below);
4. Enter your email address for temporary-password delivery, and click the **Go** button.

A temporary password will be emailed to the email address you entered on the screen. The **Forgot Password** screen is shown below:

Welcome to MMIS - Google Chrome
https://sso.state.mi.us/dch-waps11/ecams/CNSIControlServlet

CHAMPS My Inbox Admin

Provider Portal

Close

Forgot Password

Please enter your email address below. A temporary password will be emailed to this address.

User Login ID: m

Email Address:

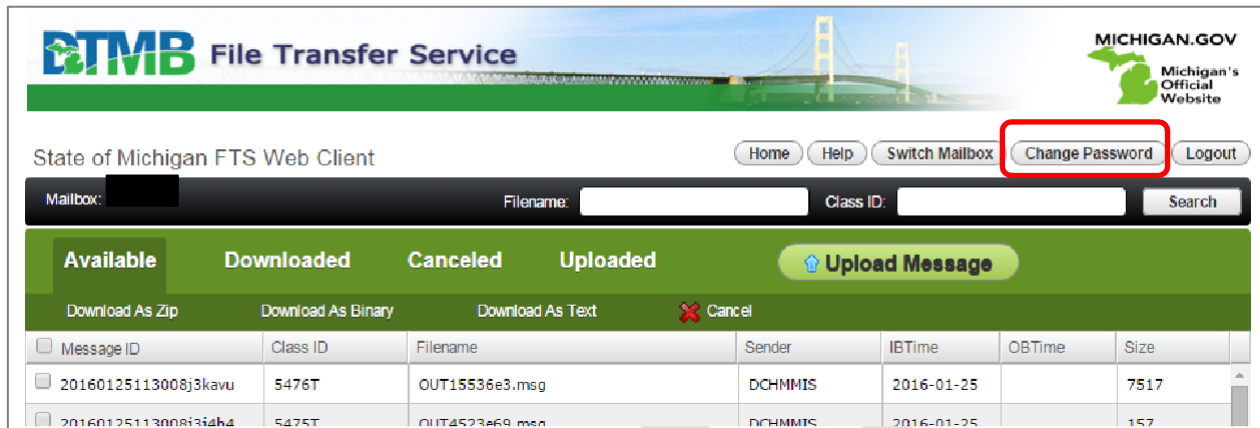
Go

7.2 SSLFTP/SFTP Passwords

To change the SSLFTP/SFTP password, use the Change Password function within FTS; please refer to section 7.3.

7.3 File Transfer Service (FTS) Passwords

7.3.1 Change Password function



The screenshot shows the Michigan File Transfer Service (FTS) web client interface. At the top, there is a banner with the 'ETMB File Transfer Service' logo and the Michigan state logo with 'MICHIGAN.GOV Michigan's Official Website'. Below the banner, there are navigation buttons: 'Home', 'Help', 'Switch Mailbox', 'Change Password' (highlighted with a red box), and 'Logout'. The main area contains a 'State of Michigan FTS Web Client' header, a 'Mailbox:' dropdown menu, and input fields for 'Filename:' and 'Class ID:' with a 'Search' button. Below this is a green navigation bar with tabs for 'Available', 'Downloaded', 'Canceled', and 'Uploaded', along with an 'Upload Message' button. A table below the navigation bar shows a list of messages with columns for 'Message ID', 'Class ID', 'Filename', 'Sender', 'IBTime', 'OBTime', and 'Size'. The table contains two rows of data.

| Message ID | Class ID | Filename | Sender | IBTime | OBTime | Size |
|-----------------------------------------------|----------|----------------|---------|------------|--------|------|
| <input type="checkbox"/> 20160125113008j3kavu | 5476T | OUT15536e3.msg | DCHMMIS | 2016-01-25 | | 7517 |
| <input type="checkbox"/> 20160125113008i3idh4 | 5475T | OUT4523469.msg | DCHMMIS | 2016-01-25 | | 157 |

7.3.1.1 Password Restrictions

Passwords have a minimum length of 8 characters. With at least 1 uppercase character, 1 lowercase character, 1 number, and 1 special character.

7.3.2 Unknown Password

An email request to Automated Billing at AutomatedBilling@michigan.gov must come from the Technical Contact listed within CHAMPS.

Section 8 - Electronic Batch Web Upload Through CHAMPS

1. Log on to CHAMPS as a Billing Agent or NPI. If using Billing Agent or NPI the enrollment must have Electronic Batch in their Mode of Claim Submission.
2. You will need either the CHAMPS Full Access or Billing Agent Access profile
3. From the tabs toolbar at the top click on **My Inbox**;
4. Select **Upload File** from the **My Inbox** drop-down list;
5. Click the **Upload** button.

Welcome to MMIS - Google Chrome
https://sso.state.mi.us/dch-waps11/ecams/CNSIControlServlet

CHAMPS < My Inbox ▾ Provider ▾ Claims ▾ Member ▾ PA ▾

Provider Portal > Batch Attachment Response

Close Upload

Please click on the Upload button to upload your file.
Please use below naming conventions for web upload files.

837 Fee For Service:

- 1) NPI.5475.CCYMMDDhhmm
- 2) CHAMPS PROVIDERID.5475.CCYMMDDhhmm

837 ENC:

- 1) NPI.5476.CCYMMDDhhmm
- 2) CHAMPS PROVIDERID.5476.CCYMMDDhhmm

270:

- 1) NPI.5414.CCYMMDDhhmm
- 2) CHAMPS PROVIDERID.5414.CCYMMDDhhmm

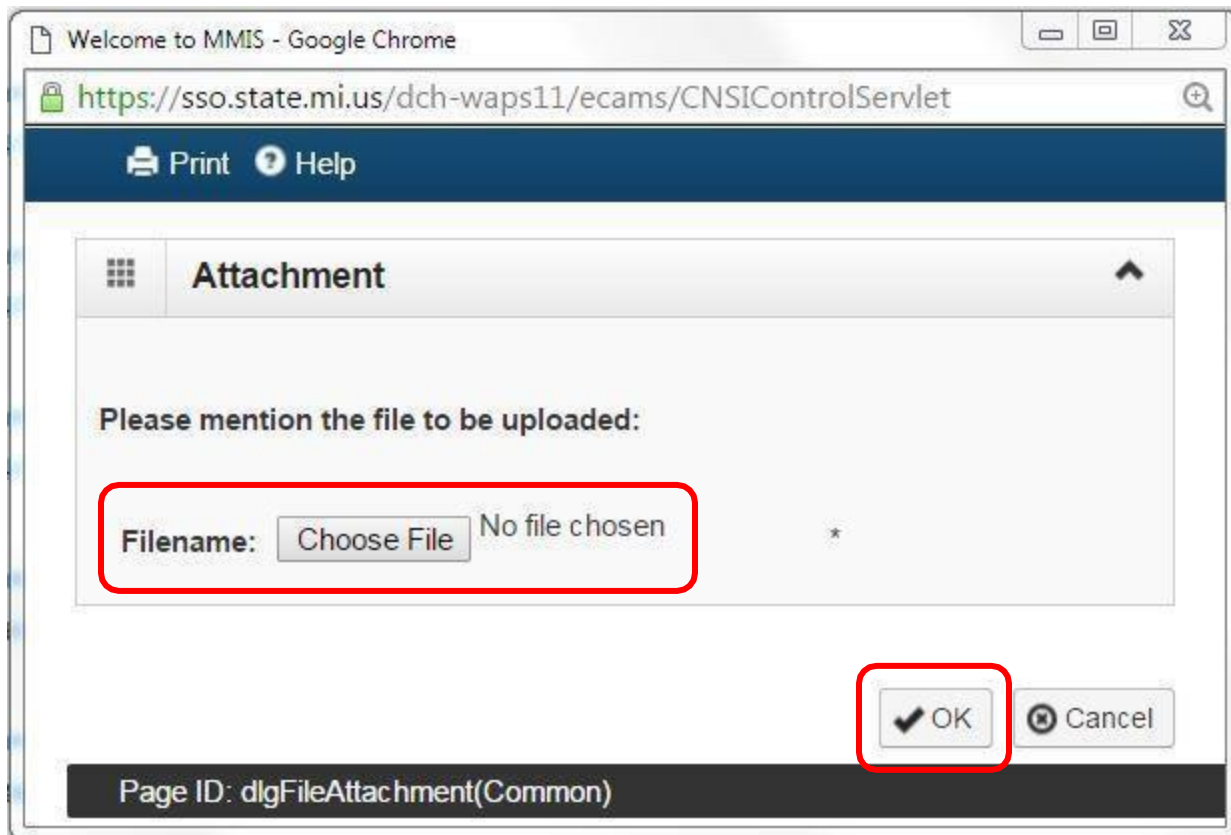
276:

- 1) NPI.4952.CCYMMDDhhmm
- 2) CHAMPS PROVIDERID.4952.CCYMMDDhhmm

278:

- 1) NPI.5386.CCYMMDDhhmm
- 2) CHAMPS PROVIDERID.5386.CCYMMDDhhmm

- Click the **Choose File** button to select the file on your PC that you wish to submit, then click the **OK** button:



Please note:

- The file name must include the Class ID from the list below.
 - ❖ 5475 (837) – Health Care Claim
 - ❖ 5414 (270) – Eligibility Inquiry
 - ❖ 4952 (276) – Claim Status Inquiry
 - ❖ 5386 (278) – Prior Authorization Inquiry
- A new file-naming convention was implemented for all Electronic Web upload files. The following examples are based on how you log into CHAMPS by NPI or Provider ID.
 - ❖ NPI.5475.CCYYMMDDhhmm (example: 1234567890.5475.201210261208.dat)
 - ❖ ProviderID.5475.CCYYMMDDhhmm (example:1234567.5475.201210261209.dat)
- All web batch files must have an extension of .dat
- File size of 50MB file or smaller is acceptable.
- You can send in as many files as you want per day.

Retrieving Files

1. Within 1 hour you should logon to CHAMPS;
2. Select **My Inbox**;
3. Select **Retrieve Response/Acknowledgement**;
4. Use the **Retrieve Acknowledgement Response File** screen to download your 999.

Welcome to MIMIS - Google Chrome
https://sso.state.mi.us/dch-waps11/ecams/CNSIControlServlet

CHAMPS My Inbox Admin Provider Claims Reference Member

MyInbox > Retrieve Acknowledgement Response File

Close

HIPAA Response/Acknowledgement

Upload/Sent Date 12/16/2015 And Filter By

Go

| Provider ID | File Name | Transaction Type | Interchange Control Number | Upload/Sent D |
|-------------|-----------|------------------|----------------------------|---------------|
| ▲▼ | ▲▼ | ▲▼ | ▲▼ | ▲▼ |

5. You may choose a filter in the leftmost drop-down box, such as the **Upload/Sent Date** that you submitted the file. The percent sign (%) may be used as a wildcard when entering a partial search filter value, other than a date.
6. Review your acknowledgement response file to make sure your file was accepted. The acknowledgement will contain the same Class ID/File Name as the file you uploaded.

Section 9 - B2B Testing

Business to Business (B2B) testing is the process of submitting test files to MDHHS for validation before a new business partner receives approval from MDHHS to submit electronic transactions. This section describes B2B testing for HIPAA v5010 transactions.

MDHHS' testing process consists of two stages for Trading Partners. Only HIPAA 5010 compliant files will be accepted.

9.1 Billing Agent IDs for New Trading Partners

New Trading Partners (who do not already have a billing agent ID with MDHHS) will need to apply for a Billing Agent ID. For more information, please refer to: "New Billing Application CHAMPS Instructions" at:

<http://Michigan.gov/tradingpartners> >> Electronic Submissions Transactions >> [New Billing Application CHAMPS Instructions](#)

9.2 5010 Test Instructions by Transaction

For specifics on testing and the v5010 certification criteria, please review the B2B Testing Instructions (see Section 2 for B2B Testing website location). The summary below will give you an overview of the testing process.

9.3 Stage 1 - Ramp Manager Testing

Integrity testing is required for all new electronic submitters and must be completed before a Trading Partner can start Stage 2 testing, using the *EDIFECs* Ramp Manager automated testing website. Ramp Manager is an easy-to-use environment to test v5010 transactions for syntax errors and is available at no cost to MDHHS Trading Partners. More information on integrity testing is available at <http://michigan.gov/tradingpartners>. You must request enrollment in this test system by sending an email to: MDHHS-B2B-Testing@michigan.gov.

9.4 Stage 2 - CHAMPS B2B Testing

For Stage 2 testing, you must successfully complete Stage 1 testing. Refer to "Billing Agent IDs for New Trading Partners" above for instructions on how to become a Billing Agent in CHAMPS and "5010 Test Instructions by Transaction" above for instructions on creating test files. Please refer to the following Sections regarding file submission and file naming conventions:

Section 4 - FILE TRANSFER SERVICE (FTS)

Section 5 - SSLFTP/SFTP (WS_FTP) SETUP

FOR THE FTS Section 6 - ACA CORE
TRANSPORT MODES

Section 8 - ELECTRONIC BATCH WEB UPLOAD

THROUGH CHAMPS Section 11 - CLASS ID/FILENAME

Once a test file is submitted to the FTS, you must send an email with a telephone

number, to the B2B Test Team, at MDHHS-B2B-Testing@michigan.gov; and to the Automated Billing team AutomatedBilling@michigan.gov to inform MDHHS that a test file has been submitted.

To ensure proper retrieval of your files, use a subject line in your email such as: “5475T Test File DCH????” or “5476T Test File DCH????” where “????” is your MDHHS-assigned FTS Username ID.

Your files will be retrieved and processed through the CHAMPS B2B system. We will not send you a TA1 or 999 Acknowledgment for these files until they have been uploaded to the test environment. Once that is done, you can retrieve your TA1 or 999 in your FTS mailbox.

If you have a question, send an email to the B2B Test Team, at MDHHS-B2B-Testing@michigan.gov; and the Automated Billing team at AutomatedBilling@michigan.gov.

Section 10 - 999 Acknowledgement File

The 999-acknowledgment file is a document that billing agents can use to verify that the files they submitted were received by MDHHS. MDHHS requests that all billing agents save all acknowledgment files until claims appear on a Remittance Advice (RA). This will show proof of receipt that the files were submitted to MDHHS.

Below is an example of an **Accepted 999**; certain data is removed per HIPAA regulations. The FTS ID has been replaced with ????:

```
ISA*00*      *00*      *ZZ*D00111  *ZZ*????
*120425*1551*^*00501*000000001*0*P*::~~
GS*FA*D00111*????*20120425*1551*1*X*005010X231~ ST*999*0001*005010X231~
AK1*HC*95*005010X223A2~
AK2*837*000000220*005010X223A2~
IK5*A~
AK2*837*000000221*005010X223A2~
IK5*A~
AK2*837*000000222*005010X223A2~
IK5*A~
AK2*837*000000223*005010X223A2~
IK5*A~
AK2*837*000000224*005010X223A2~
IK5*A~
AK9*A*5*5*5~
SE*14*0001~
GE*1*1~
IEA*1*000000001~
```

Below is an example of an **Accepted 999 with non-fatal errors** that was accepted for further processing. Each error is identified in the IK3 and IK4 segments. Please refer to the HIPAA Implementation Guide and the Michigan Companion Guide.

```
ISA*00*      *00*      *ZZ*D00111  *ZZ*????
*120426*1701*^*00501*000000001*0*P*::~~
GS*FA*D00111*????*20120426*1701*1*X*005010
X231~ ST*999*0001*005010X231~
AK1*HC*126*005010X222A1~
AK2*837*000020606*005010X222A1~
IK5*A~
AK2*837*000020637*005010X222A1~
IK3*HI*3952*2300*8~
CTX*CLM01:0014887951~
IK4*1:2*1271*112*E8889~
IK5*E*I5~
AK2*837*000020650*005010X222A1~
IK5*A~
AK9*E*3*3*3~
SE*13*0001~
GE*1*1~
IEA*1*000000001~
```

Below is an example of a **Partially Accepted 999 with fatal and non-fatal errors** for further processing. Each error is identified in the IK3 and IK4 segments. Keep in mind you can have the same fatal or non-fatal error multiple times throughout the file. Please refer to the HIPAA Implementation Guide and Michigan Companion Guide.

```
ISA*00*      *00*      *ZZ*D00111  *ZZ*????
*120426*1540*^*00501*000000001*0*P*::~~
GS*FA*D00111*????*20120426*1540*1*X*005010X231~ ST*999*0001*005010X231~
AK1*HC*126*005010X222A1~ AK2*837*000020575*005010X222A1~
IK5*A~
AK2*837*000020576*005010X222A1~
IK5*A~
AK2*837*000020577*005010X222A1~
IK3*SVD*3619*2430*8~
CTX*CLM01:TPRF1106003808401~
IK4*3:5*1339*113*KX~
CTX*SITUATIONAL TRIGGER*SVD*3619**3:4*3:1339~
IK5*R*5*I5~
AK2*837*000020578*005010X222A1~
IK3*HI*3952*2300*8~
CTX*CLM01:0014887951~
IK4*1:2*1271*112*E8889~
IK3*REF*4494*2400*8~
CTX*CLM01:0014831301~
IK4*2*127*112*23D01025908~
```

Electronic Submissions Manual (ESM)

IK3*REF*4522*2400*8~
CTX*CLM01:0014831301~
IK4*2*127*112*23D01025908~
IK3*REF*4546*2400*8~
CTX*CLM01:0005893440~
IK4*2*127*112*23D01025908~
IK3*REF*4570*2400*8~
CTX*CLM01:0005893440~
IK4*2*127*112*23D01025908~
IK3*REF*4617*2400*8~
CTX*CLM01:0013800419~
IK4*2*127*112*23D01025908~
IK3*REF*4645*2400*8~
CTX*CLM01:0013822403~
IK4*2*127*112*23D01025908~
IK3*REF*4673*2400*8~
CTX*CLM01:0014902207~
IK4*2*127*112*23D01025908~ IK3*REF*4697*2400*8~ CTX*CLM01:0014894637~
IK4*2*127*112*23D01025908~
IK5*R*5*15~
AK2*837*000020579*005010X222
A1~ IK3*AMT*116*2320*8~
CTX*CLM01:BA-108989T37863~
IK4*2*782*112*-6.07~
IK3*SVD*128*2430*8~
CTX*CLM01:BA-108989T37863~
IK4*2*782*112*-6.07~
IK5*R*5*15~
AK2*837*000020580*005010X222A1~
IK5*A~
AK2*837*000020581*005010X222
A1~ IK3*NM1*43*2310*8~
CTX*CLM01:CLM49978~
IK4*4*1036*19~
IK3*NM1*74*2310*8~
CTX*CLM01:CLM50836~
IK4*4*1036*19~
IK5*E*15~
AK2*837*000020582*005010X222A1
~ IK3*SV1*17823*2400*8~
CTX*CLM01:4759~
IK4*2*782*112*5~
CTX*SITUATIONAL TRIGGER*SV1*17823**1:2*3:234~
IK5*E*15~
AK2*837*000020583*005010X222A1~
IK5*A~
AK2*837*000020584*005010X222A1~
IK3*SV1*60*2400*8~

CTX*CLM01:M1182931T22430~
 IK4*2*782*I12*.1~
 CTX*SITUATIONAL TRIGGER*SV1*60**1:2*3:234~
 IK5*E*I5~
 AK2*837*000020585*005010X222A1~
 IK5*A~
AK9*P*11*11*8~ notice the count changed to reflect 3 transactions that have failed.
 SE*921*0001~
 GE*1*1~
 IEA*1*000000001~

From the example above, the IK3 segment verifies the segment Position of a segment within Transaction Set (120) and Segment Has Data Element Errors Qualifier (8).

The IK4 segment gives you the Data Element Position within the Segment (2), the X12 Data Dictionary Reference ID (782), Segment has Data Element Errors (I12), and a Copy of Data Element in Error (92.511)

Section 11 - Class ID/Filename

You will need to use the 'Class ID Filename' for files that are submitted through the **FTS** to MDHHS, and to recognize files that MDHHS returns to your billing agent "mailbox".

If you wish to submit a file that is not listed, please contact AutomatedBilling@michigan.gov for more information.

| Class ID Filename* | HIPAA Transaction ID | Transaction Information |
|-----------------------|----------------------------|----------------------------------------------------|
| 5414 | 270 | Medical Eligibility Inquiry |
| 5415 | 271 | Medical Eligibility Response |
| 4952 | 276 | Health Care Claim Status Inquiry |
| 4953 | 277 | Health Care Claim Status Response |
| 5386 | 278 | Prior Authorization Request (Inbound to MDHHS) |
| 5383 | 278 | Prior Authorization Response (Outbound from MDHHS) |
| 4985 | 820 | Payroll Deducted and Other Premium Payment |
| 4976 | 834 | Card Cutoff Audit File |
| 5014 | 834 | Card Cutoff File – PIHP and HMP-PIHP |
| 5015 | 834 | Healthy Kids Dental – EOM/FOM Audit File |
| 5093 | 834 | HSW Audit File (Habilitation Support Waiver) |
| 5419 | 834 | MIChild-CA EOM/FOM Audit File |
| 5421 | 834 | MIChild-CMH EOM/FOM Audit File |
| 5485 | 834 | NEMT- Weekly Update - Enrollment |

| Class ID Filename* | HIPAA Transaction ID | Transaction Information |
|-----------------------|----------------------------|----------------------------------------------------------------------------------------------|
| 5610 | 834 | DHIP Update File (DHS Incentive Payment) |
| 5611 | 834 | AUT Update File |
| 5629 | 834 | PIHP & HMP-PIHP Update File |
| 5705 | 834 | Full File Audit File - Integrated Long-Term Care Audit Enrollment File sent to ICOs |
| 5721 | 834 | Update Transaction File - MI Health Link Daily Enrollment |
| 5790 | 834 | Daily File – Benefit Enrollment and Maintenance |
| 4987 | 835 | Health Care Claim Payment and Remittance Advice |
| 5475 | 837 | FFS Health Care Claims |
| 5476 | 837 | Encounters Transactions (v5010) |
| 5477 | | NCPDP Transactions |
| 5776 | 837 | <u>Medicare</u> ICO Inbound Encounter File (5890 is the ETRR outbound response for the 5776) |
| 5777 | 837 | Medicaid ICO Inbound Encounter File |
| 5786 | | Outbound ICO Medicaid File - response file for 5777 |
| 5848 | | Medicaid Inbound ICO NCPDP PA4.2 - Medicaid file |
| 5849 | | Outbound Medicaid ICO NCPDP - response file for 5848 |
| 5850 | | Medicare ICO <i>NCPDP</i> Inbound Encounter file |
| 5852 | | MHP Inbound NCPDP file |
| 5853 | | Outbound MHP NCPDP - response file for 5852 |
| 5877 | | PIHP Daily Enrollment File |
| 5890 | | ETRR outbound response for the 5776 Medicare ICO Inbound Encounter File |

11.1 *Notes Regarding TEST Files

1. You must place a “T” in the fifth position of the Class ID Filename to identify a **test** file, for example, 5414T.
2. A “T” must also be placed in the ISA15 data element within the header record of a 270, 276, 278, or 837 **test** files.
3. The transactions in a **test** file will not post to the production CHAMPS system; test files will only be routed to the CHAMPS B2B system.
4. A valid Sender ID must appear in the ISA06 and GS02 data elements, for the test system to be able to identify you as the file submitter and to return the response file to your FTS mailbox. If you do not receive a response file within two hours, verify the syntax of the test file in Ramp Manager. If it passes Ramp Manager and you still don’t receive a response file contact the B2B Test team at: MDHHS-B2B-Testing@michigan.gov.

Addendum A. File Transfer Service (FTS) internet connections



State of Michigan (SOM) File Transfer Service Internet* Trading Partner Connection information:

There are three secure protocols for exchanging files with the SOM FTS.

1. **SOM FTS Web Client: (https)**

URL: <https://MiFTS.state.mi.us>

2. **SFTP:**

URL: MiFTS.state.mi.us

Use Port: 2222 to view files by Class ID name.

Use Port: 2223 to view files by File Name.

3. **FTPS (FTP/SSL) EXPLICIT, Use Passive Mode for Data Transfers.**

URL: MiFTS.state.mi.us

Use Port: 11250 to view files by Class ID name.

Use Port: 11251 to view files by File Name.

Data Ports: 11200-11240

Notes: You may need to open ports 11200-11240 in your firewall.

Notes

- **Internet:** The IP addresses and URL in this document can only be used by connections from outside of the State of Michigan's network.
- **Software:** The SOM FTS Web Client can be accessed with Microsoft Edge or other web browsers. For file transfers using the SFTP or FTPS (FTP/SSL) protocols, the Trading Partner will provide their own software and support.
- **Passwords:** Are case-sensitive.
- **SOM Source IP:** When the State initiates a connection to send a file out over the Internet, the connection will come from IP 136.181.195.231

Addendum B. File Transfer Service (FTS) web client



Enter the SOM FTS Web site address in your Web Browser to reach the SOM FTS Web Client:

From the Internet: <https://MiFTS.state.mi.us>

Note: the 's' at the end of https - is required for a secure connection.

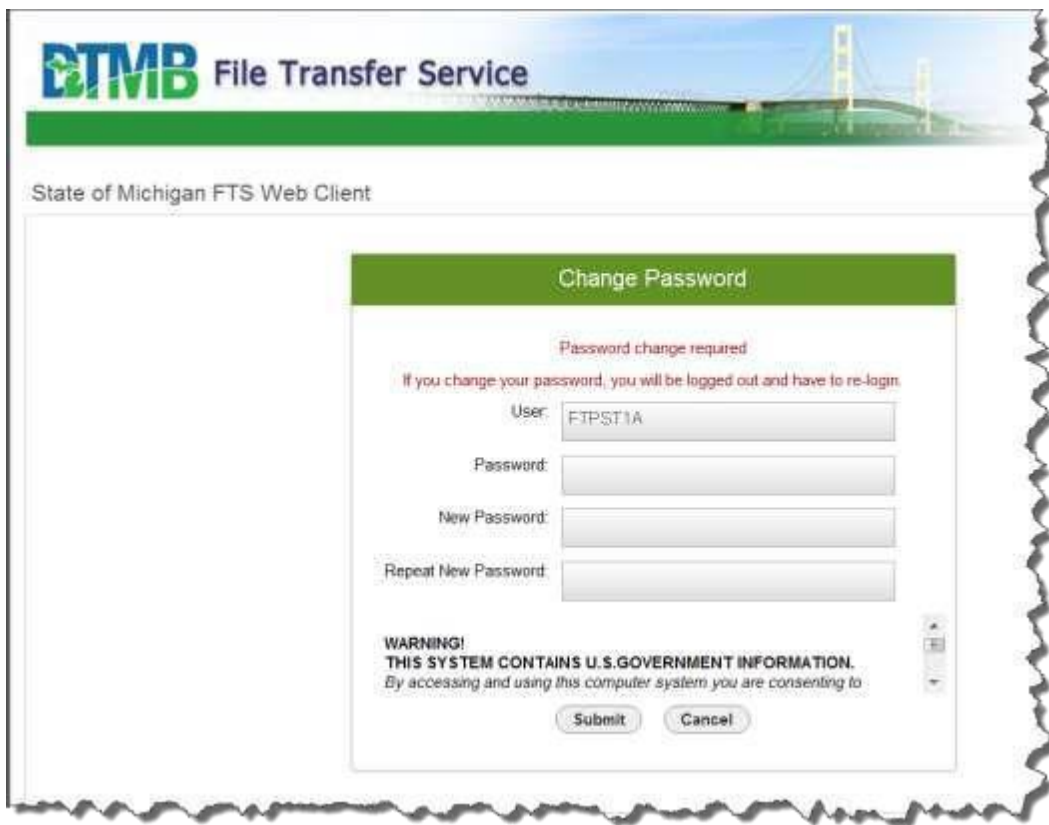
Logging in:

The following image shows the login page to the State of File Transfer Service Web Client.

A screenshot of the login page for the State of Michigan File Transfer Service. The page has a header with the DTMB logo and "File Transfer Service" text. In the top right corner, there is a "MICHIGAN.GOV" logo and the text "Michigan's Official Website". Below the header, the text "State of Michigan FTS Web Client" is displayed. The main content area features a green-bordered box titled "Logon on to: State of Michigan FTS Web Client". Inside this box, there are two input fields: "Username:" with the placeholder text "YOUR-USER-ID" and "Password:" with a masked password "*****". Below the password field is a "WARNING!" section with the text: "THIS SYSTEM CONTAINS U.S. GOVERNMENT INFORMATION. By accessing and using this computer system you are consenting to". At the bottom of the box is a "Logon" button. In the bottom left corner of the page, it says "Powered by MessageKey" and has the "IPSWITCH FILE TRANSFER" logo. In the bottom right corner, there is a "MI.gov" logo.

Type in your Username and Password and click on the Logon button.

- Note: If the 'Force password change at next login' flag has been set for your Username the Change Password screen will display next.



- Note: After you change your password you will be logged out and then must login using the new password you just set.



Running Java:

Once you login to this site you will receive the following popup messages until you select the 'Do not show...' options.

You will see the pop-up Java notice asking if you want to run the Ipswitch Inc Web Client application.



- ✓ Select the check box “Do not show this again for...”
- ✓ Click Run.

Next, you will see the pop-up Security Warning notice asking if you want to run the Ipswitch Inc Web Client application.



- ✓ Select the check box “Do not show this again for...”
- ✓ Click Allow.

Reason for running Java: *Java vs Non-Java Mode*

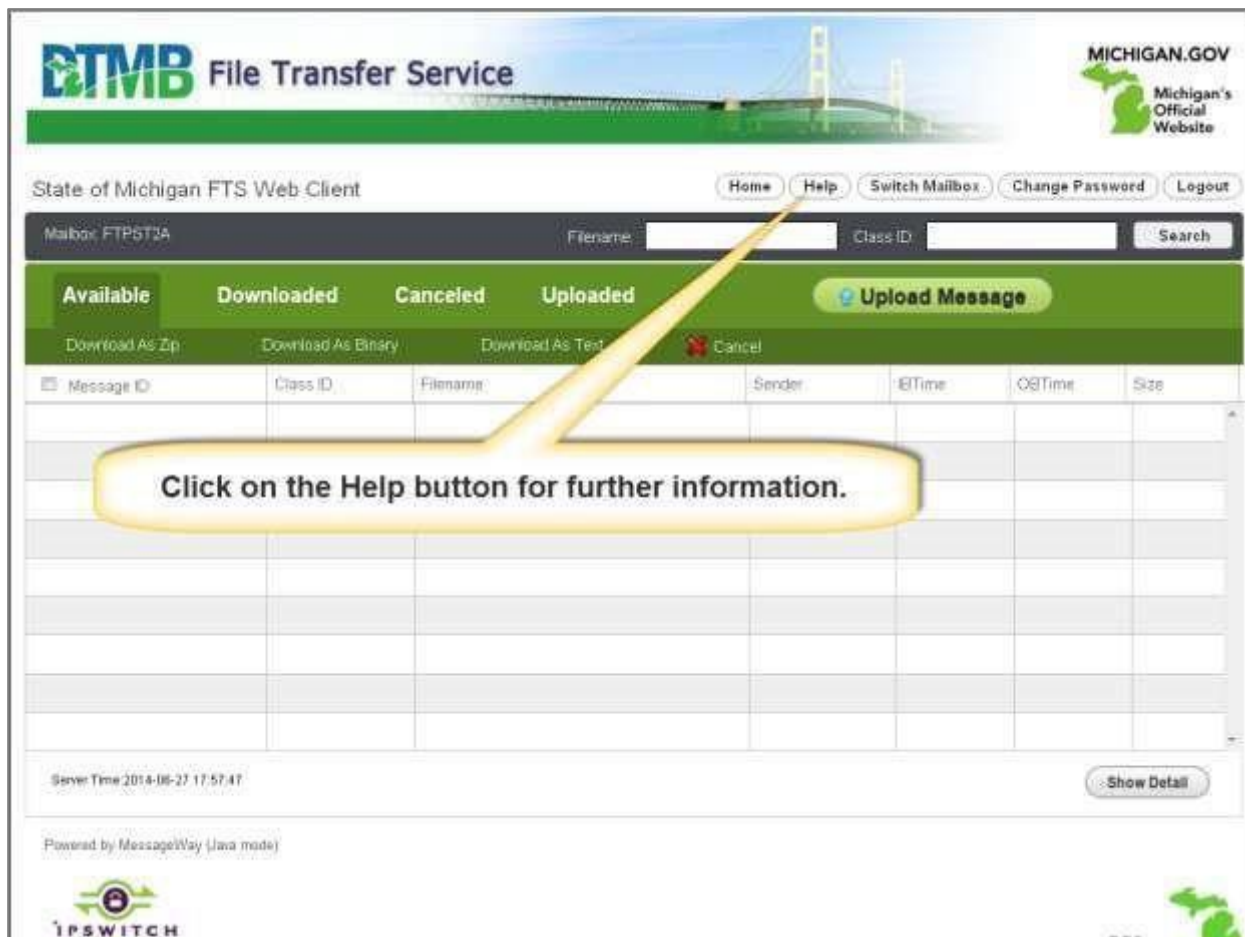
You can run the Web Client with or without Java installed. If Java (JRE version 1.7.17 or later) is not installed on your computer, the Web Client provides a link to download the latest version of Java during logon.

The following table shows the features available in Java and non-Java mode:

| Feature | Java Mode (applet) | Non-Java Mode |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------|
| Access information as defined by security settings in MessageWay | X | X |
| Change password | X | X |
| Upload message to multiple or compound addresses | X | |
| Download multiple messages at a time | X | |
| Size limits of message transfers | Transfer limit is that of system resources, e.g. disk space | Upload limit: limit of browser Download limit: 250 MB |
| Choose a file format to upload (Binary or Text) and download (Binary, Text, or Zip) messages | X | X |
| Transfer multiple files | Simultaneous transfers | Sequential transfers |
| View progress of transfer and status information | X | |
| Pause, resume or cancel transfers; retry failed or canceled transfers | X | |
| View additional error information for failed transfers | X | |
| Access messages in other mailboxes as rights permit | X | X |
| Search for messages by filename or class ID, with wild card options | X | X |
| Special characters \ / : * ? " < > ! & ` ' ; replaced with _ in Filename | Special characters not allowed | X |
| View related messages and document reconciliation status as appropriate | X | X |
| View results of transfers by category: Available, Downloaded, Canceled, Uploaded | X | X |

More information

For more information on using the SOM FTS Web Client refer to the built-in documentation by clicking on the Help button.



Addendum C: Put Command formats

CLASSID is the Class ID of the file to be sent. (AKA Appl ID or Application ID, AKA Remote file name)
 MAILBOX is the UserID/Mailbox name of the recipient (AKA Remote directory path).

Note: If the file is not placed in the correct location try typing the ClassID and Mailbox in all upper case.

<local filename> *CLASSID@MAILBOX*

OR

<local filename> *MAILBOX\CLASSID*

OR

CD *MAILBOX*

<local filename> *CLASSID*

The FTS will default to using the input filename for the CLASSID unless using SFTP and it is passed in the Put statement. (The Web page will pass the input filename.)

Example: (*INPUTNAME.TXT* is the input name passed in the Put command)

<local filename> *CLASSID@MAILBOX\INPUTNAME.TXT*

OR

<local filename> *MAILBOX\CLASSID@INPUTNAME.TXT*

OR

CD *MAILBOX* <local filename> *CLASSID@INPUTNAME.TXT*

OR

CD *MAILBOX* *INPUTNAME.CLASSID.TXT*

(where the <local filename> has the assigned CLASSID Value in the right most part of the filename, to the left of any extension.)

Example mailbox: CD /DCHEDI

| Example filenames with ClassId values | Example Prod filename | Example Test filename |
|-----------------------------------------------------------------------------------------------------|-----------------------|------------------------|
| Create your source filename to be a valid ClassId value | 5475 | 5475T |
| Create your source filename to contain the ClassId value to the left of first "." and right of "_". | 1234567890_5475.txt | 1234567890_5475T.txt |
| Supply a valid ClassId as the destination filename. | put <local-file> 5475 | put <local-file> 5475T |