Arkansas Medicaid Enterprise
MMIS Core System and Services

Arkansas Medicaid
Vendor File Exchange Specifications

Date: 05/24/2022
Version 1.5

Modification Log

Rev #	Date	Author	Section	Nature of Change
1.0	9/26/2017	K Farhat		Initial version
1.1	10/18/2017	B Dunn		Added SSH Key paragraph
1.2	3/21/2018	M Morgan		Add SSH Key Only Authentication Policy, Add test environment urls, Added File Transfer recommendations
1.3	9/19/2018	M Morgan		Updated verdor support email to @dxc.com
1.4	10/29/2018	M Morgan		Update Supported TLS Protocol
1.5	05/04/2022	M Hasty	Document	Update to Gainwell Format

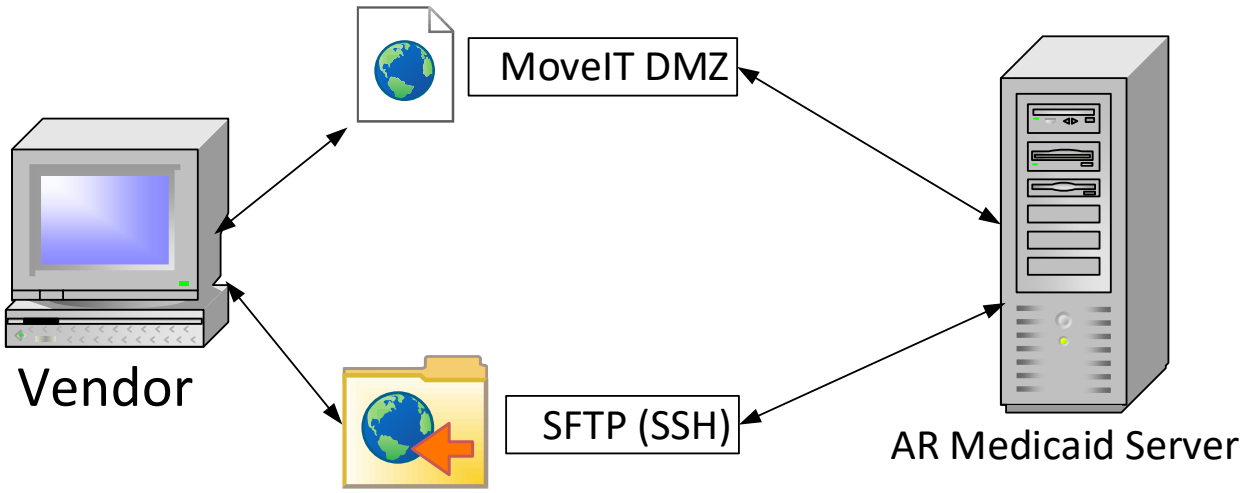
Contents

Introduction

This document is intended for software vendors who wish to develop applications that interact with Arkansas Medicaid's file delivery and retrieval system. It was created and is maintained by DXC Technology for the purpose of sending and receiving electronic interface files.

Interface Standards

Arkansas Medicaid's file exchange interfaces support two channels of communication -- HTTP/S (using MoveIT DMZ Web site) and standard SFTP.



Interface Environments

Arkansas Medicaid has 2 interface environments, a produciotn environment and a test environment, each having a separate set of credentials.

Produciton interface

Website: https://fts.mmis.arkansas.gov

SSH: fts.mmis.arkansas.gov port 22

Test interface

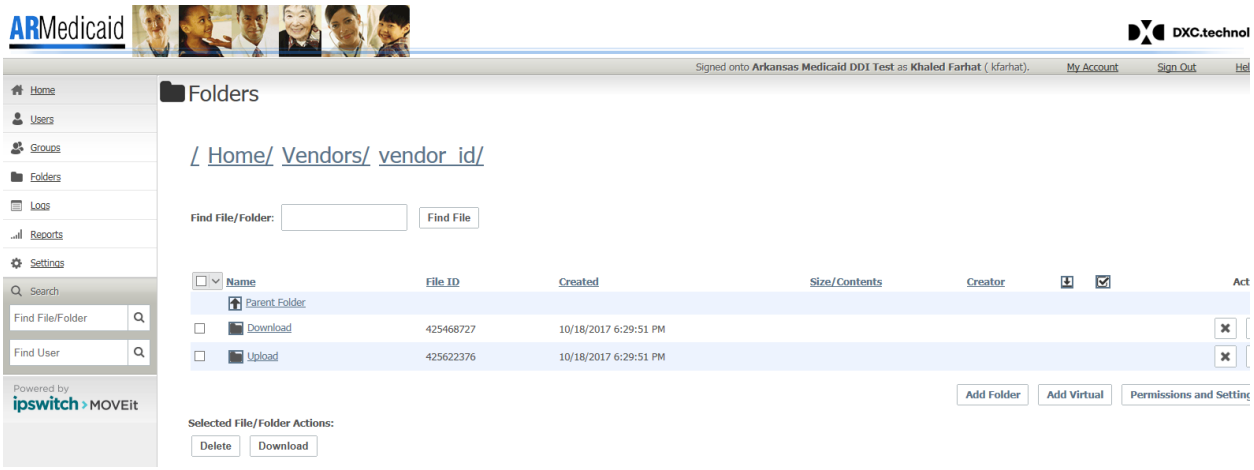
Website: https://fts-test.mmis.arkansas.gov
SSH: fts-test.mmis.arkansas.gov port 22

Here in we will discuss everything in terms of the production environment. It will however apply to the test environment as well.

MOVEit DMZ website

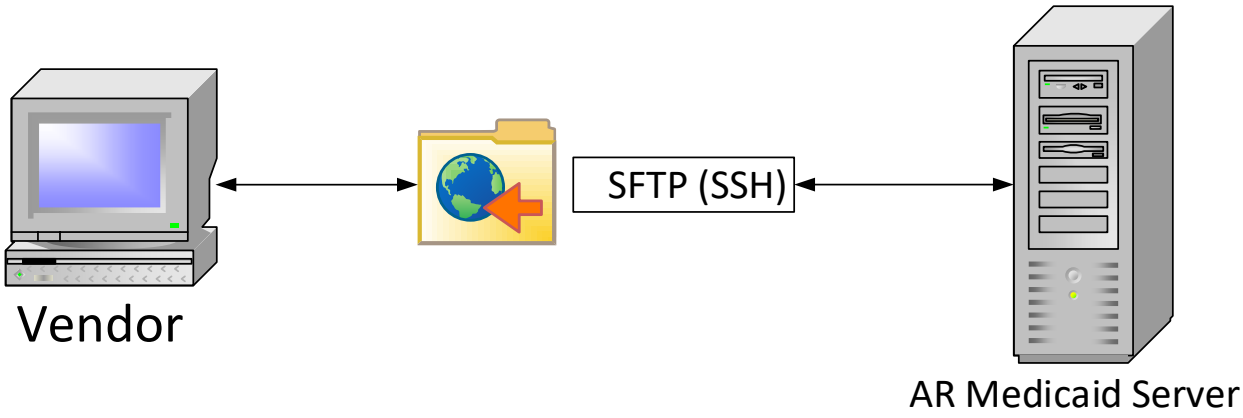
Arkansas Medicaid's MoveIT DMZ is a secure website located at https://fts.mmis.arkansas.gov and https://fts-test.mmis.arkansas.gov The website interface is integrated with file transfer wizards that allows users to upload and download files to and from the batch file repository. Once logged in, users can upload batch files to the secure server for processing. To upload batch files, navigate to the upload folder, and launch the upload/download wizard. To retrieve batch response files, navigate to the download folder, and click the download link next to each file displayed. Complete user interface documentation can be found by clicking on the "Online Manual" link found in the menu on the left of the home screen. A screenshot of the website is provided below.

NOTE: Batch files must be uploaded one at a time. Users cannot use the zip option within the upload/download wizard.



SFTP

The SFTP supports batch file uploads and downloads only. Users may use SFTP (SSH) clients such Filezilla, Putty, and WS_FTP Pro to transfer files or develop software that will logon and transfer files programmatically using SSH protocol. Complete specifications can be found in the "SFTP Specifications" section of this document.



SFTP (FTP over SSH) Specification

This section covers the most frequently used SFTP commands. An SFTP connection can be established using “fts.mmis.arkansas.gov” port 22.

NOTE: Users are required to change passwords on first login; you must log in to https://fts.mmis.arkansas.gov to change your password.

Uploading files

To upload files via SFTP, connect to “fts.mmis.arkansas.gov” using your assigned Vendor ID and password. To upload a file, navigate to /home/vendors/<Vendor ID>/upload and issue the “Put” command and the name of the file to be uploaded.

Example: put foo.txt

Directory listing

To locate available response files via SFTP, connect to “fts.mmis.arkansas.gov” using your assigned Vendor ID and password. Then, navigate to /home/vendors/<Vendor ID>/download and execute a “dir” command.

Example: dir

Downloading files

To download files via SFTP, connect to “fts.mmis.arkansas.gov” using your assigned Vendor ID and password. Then, navigate or “cd” to /home/vendors/<Vendor ID>/download and retrieve file(s) using the “get” command and the FileName or FileId.

Example: get foo.txt

Security Standards and Practices

In order for DXC Technology to guarantee a safe and stable working environment, the following security standards and practices have been established. These measures protect users and DXC Technology from potential threats.

TLS Protocol

DXC Technology supports the use of TLS 1.2

Password creation requirements

Passwords must contain:

- A minimum of 8 alpha-numeric-special characters
- At least 1 upper and 1 lower case alpha character
- At least 1 number
- At least 1 special character

Passwords **cannot**:

- Be similar to username (Vendor ID)
- Use any common ‘dictionary’ words
- Use previous six (6) passwords

New Vendor passwords

Any new client to the Arkansas Medicaid file exchange system will be given a temporary password that meets the password requirement criteria. This password will be a one-time-use only password that must be changed upon first login. The new password should be of the client’s choosing and must adhere to the required password criteria listed above.

Password aging

- Passwords expire after 90 days.
- Each method of interaction with the Arkansas Medicaid file exchange system, excluding SSH protocol, has its own procedures for changing passwords as deemed necessary by the system. Each of these procedures can be reviewed in the following subsections.
- To have your password set to **non-expiring** you must have it set up for SSH key authentication only. This will require the following, which will only be done by request.
    - Web Access turned off
    - SSH Auth Only turned on

MoveIT DMZ password change procedures

MoveIT DMZ website has a 10-day "warning period" for notifying users prior to password expiration. When a user logs in during this period, they will be prompted to change their password. If the user fails to change their password during the "warning period" and allows it to exceed its 90-day life span, the account will be locked, and the user will need to contact the EDI Help Desk for further assistance.

NOTE: Passwords may be changed at any time by logging into the Arkansas Medicaid secure website at https://fts.mmis.arkansas.gov.

Establishing/Utilizing SSH Keys (Public/Private Key Pairs) with the SSH Server vs. standard password procedures

The SFTP Server connection offers the option to utilize SSH Keys (Publick/Private Key Pairs) vs. utilizing the standard DMZ password proceedures. If the Vendor prefers to utilize this method, after changing the initial password provided by DXC, they can initiate the utilization of the SSH Key on their end. Next the Vendor must notify Arkansas Medicaid Vendor Support staff that they have done so. This notification should be accomplished by sending an email to the ARKVendorSupport@dxc.com email box. The email should indicate the Vendor ID and state that you have connected to the Arkansas Medicaid Vendor file site SFTP server utilizing SSH keys. The support team will review and approve the key and provide confirmation back to the Vendor at the email address that the request is received from.

File Transfer Recommendation

1) File naming convention are setup between the vendor and the functional area that will consume the file. However, it is recommended to put date stamps in the file names in CCYYMMDD format, time stamps as well.
2) We do not have a limit to the file size that can be sent however, we recommend files be constrained to **8G or less** to keep firewalls from closing connections.