# Revision History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Published on</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1.0</td>
<td>08/01/2018</td>
<td>Approved</td>
<td>First draft of fileX service user guide</td>
</tr>
<tr>
<td>0.1.1</td>
<td>08/15/2018</td>
<td>Approved</td>
<td>Changes to SFTP Hostnames for Production and CT Environment</td>
</tr>
<tr>
<td>1.0.0</td>
<td>09/18/2018</td>
<td>Approved</td>
<td>Enhancement to FAQs &amp; Troubleshooting section along with additional minor changes</td>
</tr>
<tr>
<td>1.0.3</td>
<td>10/18/2018</td>
<td>Approved</td>
<td>Changed the ACATS and eFOCUS upload/download paths and added FAQs</td>
</tr>
<tr>
<td>1.1</td>
<td>12/19/2018</td>
<td>Approved</td>
<td>Added HTTPS REST API Details. Formatting Updates.</td>
</tr>
<tr>
<td>1.2.0</td>
<td>02/06/2019</td>
<td>Approved</td>
<td>Added S3 Direct details and HTTPS REST API details for File Tracking</td>
</tr>
<tr>
<td>1.2.1</td>
<td>03/25/2019</td>
<td>Approved</td>
<td>Add File Archive feature details</td>
</tr>
</tbody>
</table>
| 1.2.2            | 04/30/2020    | Approved  | Added SSH config details for SFTP  
Added directory information for newly onboarded apps                                                                                     |
| 1.2.3            | 08/10/2020    | Approved  | Added HTTPS certificate information for REST API usage, section 5.1.  
Added (in FAQs) SFTP connection options to prefer password instead of keys.  
Added (in FAQs) Guidance around Packet handling.  
Added directory information for newly onboarded apps                                                                                     |
## Contents

1. Introduction .......................................................................................................................... 3
2. Access Methods .................................................................................................................... 4
3. Environment and Connectivity ............................................................................................. 5
   3.1 SFTP Transfer Method .................................................................................................... 5
   3.2 HTTPS REST API Endpoints .......................................................................................... 5
   3.3 AWS S3 DIRECT TRANSFER ....................................................................................... 6
4. Entitlement & Access Control ............................................................................................... 6
5. HTTPS REST APIs ............................................................................................................... 7
   5.1 Security .......................................................................................................................... 7
   5.2 Response Codes ............................................................................................................ 7
   5.3 Request Headers ............................................................................................................ 8
   5.4 REST API Catalog ......................................................................................................... 8
      5.4.1 List Available Applications .................................................................................... 8
      5.4.2 List Available Application Sub-Spaces ................................................................. 9
      5.4.3 List Available Files in Application Sub-Space ....................................................... 11
      5.4.4 Download File from Application Sub-Space ......................................................... 13
      5.4.5 Upload File to Application Sub-Space .................................................................... 14
      5.4.6 Track File uploaded to Application Sub-Space ...................................................... 16
6. S3 Direct Transfer ................................................................................................................ 18
   6.1 Generate Token for AWS S3 ......................................................................................... 18
7. Troubleshooting & FAQs ...................................................................................................... 20
8. Contact Information ............................................................................................................. 25
9. Supported Applications and Relevant Parameters ............................................................... 26
1 Introduction

fileX is a centralized, secure file transfer service from FINRA, where customers (member firms and industry participants) can send or receive batch file(s) to FINRA Applications like CRD, ACATS or OATS (referred within this document as ‘application’).

![Diagram of fileX and FINRA Applications](image)

The purpose of this document is to provide details for using fileX services to transfer file(s) with FINRA applications.

fileX supports multiple access methods to send/receive files, and a customer may choose to use any of the supported access methods to transfer file(s). Customers will use credentials provided by FINRA with the appropriate level of permissions granted by FINRA Entitlement service to connect to fileX. Once they connect to fileX, they can access various sub-spaces available for each application based on their entitlement. These sub-spaces are the locations within each application where customers can upload or download files. Please refer section 9 for more details on sub-spaces.
## Access Methods

fileX supports three access methods detailed below.

### FINRA customers can upload or download files through Secure File Transfer Protocol (SFTP), a standard file transfer mechanism to securely transmit files between systems/machines. fileX supports the full security and authentication functionalities provided by SFTP.

### FINRA customers can upload or download files using REST APIs over HTTPS protocol. Customers can make standard REST API calls to the endpoint URL with valid credentials for authentication. REST API calls are encrypted through HTTPS.

### FINRA customers can upload or download files natively through AWS S3 APIs. Customers who are already using Amazon AWS S3 can take advantage of this method to send/receive files directly to/from their S3 bucket.
3 Environment and Connectivity

FINRA recommends customers to first test their setup in lower environments before cutting it over to 'Production'.

<table>
<thead>
<tr>
<th>PRODUCTION</th>
<th>CUSTOMER TEST</th>
<th>LOWER (QA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment description</td>
<td>Live/production environment</td>
<td>Production-like customer test environment</td>
</tr>
<tr>
<td>Credentials</td>
<td>Production FINRA Enterprise Web Security (EWS) credentials</td>
<td>Production FINRA Enterprise Web Security (EWS) credentials</td>
</tr>
<tr>
<td>Hostname/URL</td>
<td>filex.finra.org</td>
<td>filex.ct.finra.org</td>
</tr>
<tr>
<td>Static IP Addresses for SFTP</td>
<td>52.207.197.35 35.171.199.181</td>
<td>18.209.156.254 34.225.135.103</td>
</tr>
<tr>
<td>Port for SFTP</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>Port for REST methods</td>
<td>443</td>
<td>443</td>
</tr>
</tbody>
</table>

3.1 SFTP Transfer Method

The following steps are required to use the fileX SFTP service

- Open firewall to allow outbound traffic on port 22 to FINRA SFTP host IP addresses
- Request FINRA to allow inbound traffic on port 22 for your outbound server's internet routable IP address. Please call FINRA support at 800-321-6273 and provide the list of list of external IPs to be whitelisted to open the network/firewall from FINRA.
- Request FINRA Credentials (if not already available) for specific FINRA application file transfer (see section 4)
- Install and configure a SFTP client/library to connect and transfer files
- Please ensure the following SFTP SSH configurations are set appropriately on your SFTP client
  - Supported SSH Ciphers
    - aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
  - Supported SSH Key Exchange Algorithms
    - diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha256
  - Supported SSH MAC Algorithms
    - hmac-sha1, hmac-sha1-96, hmac-sha256, hmac-sha256@ssh.com

3.2 HTTPS REST API Endpoints

The following steps are required to use the fileX HTTPS REST API service

- Open firewall to allow outbound traffic on port 443 from your outbound server IP address to fileX HTTPS REST APIs
- Request FINRA Credentials (if not already available) for specific FINRA application file transfer (see section 4)
- Open firewalls to allow traffic to/from AWS S3. Upload and Download services currently use native AWS S3 endpoints.
  - For AWS S3 IP ranges refer to: https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html
- Invoke/Call fileX HTTP REST APIs as detailed in section 5 below
3.3 AWS S3 DIRECT TRANSFER

The following steps are required to use the fileX S3 Direct service:

- Open firewall to allow outbound traffic on port 443 from your outbound server IP address to fileX HTTPS service.
- Request FINRA Credentials (if not already available) for specific FINRA application file transfer (see section 4).
- Open firewalls to allow traffic to/from AWS S3.
  - For AWS S3 IP ranges refer to: https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html
- Obtain an access token from the fileX REST API for AWS S3 as detailed in section 6.
- Use the access token to upload/download using AWS S3 APIs or AWS CLI or AWS SDK wrapper libraries.

4 Entitlement & Access Control

FINRA Entitlement Service controls access and privileges granted to customer accounts to access various services provided by FINRA, including fileX service. Customers will have the option of creating multiple file transfer accounts with different access privileges. Various supported access levels for users includes, but not limited to,

- read/download only
- submit only
- submit and download

This allows customers to support separation of duties within the firm across different departments. Administrator (typically SAA) of the firm needs to contact FINRA Entitlement Service to create file transfer accounts and request respective FINRA Application File Transfer entitlements. Currently, entitling file transfer or machine-to-machine account is a paper-based process handled by FINRA entitlement service. If you have any question about FINRA Entitlement program, please check https://www.finra.org/industry/entitlement-program.

fileX leverages FINRA provisioned entitlements to control access to specific upload/download directories or the respective HTTPS REST endpoints. Once an application is onboard the fileX platform, access to the upload and download capabilities will be controlled by specific FINRA entitlements.
5 HTTPS REST APIs

fileX service provides HTTPS REST API Endpoints to perform functions such as list of applications/files and download/upload files from/to FINRA applications. The APIs support both JSON and XML responses.

Details and sample code (for reference only) are provided for each API in the following sections. In the sample codes and other examples within this document curly braces, like \{ORCID\}, indicate input variables.

5.1 Security

fileX APIs only support basic authentication which should be provided in the Authorization header with each API request, per the format below:

   Authorization: Basic base64-encoded(username: password)

FINRA Web applications/systems use TLS Certificates signed by following Certificate Authorities:

- Entrust CA
- DigiCert CA
- Amazon CA

Please ensure your applications/system trusts all the above listed Certificate Authorities when using fileX HTTPS REST APIs.

5.2 Response Codes

fileX APIs return a range of standard HTTP response codes based on the request made to the service. Table below lists the response codes and possible reasons

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Possible Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Indicates a successful request</td>
</tr>
<tr>
<td>400 Bad Request</td>
<td>Indicates the request was malformed</td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>Indicates that either the account lacks sufficient entitlements to access requested resource or provided credentials are invalid</td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>Indicates request to an invalid resource</td>
</tr>
<tr>
<td>404 Not Found</td>
<td>Indicates the file/directory is not found/available</td>
</tr>
<tr>
<td>500 Internal Server Error</td>
<td>Indicates a possible problem with fileX service</td>
</tr>
</tbody>
</table>

If you encounter issues or response code other than 200 (success), please check your request for errors/invalid content and retry.

If you still encounter issues after fixing your request, please contact FINRA Support with the response code and the request details for further assistance. See section 8 for contact information.
5.3 Request Headers

The following header parameters should be passed (as applicable) when making all the REST API calls:

<table>
<thead>
<tr>
<th>Header</th>
<th>Required (Y/N)</th>
<th>Default</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>Y</td>
<td>N/A</td>
<td>Authorization: Basic base64-encoded(username: password)</td>
</tr>
<tr>
<td>Accept</td>
<td>N</td>
<td>application/json</td>
<td>application/json, application/xml</td>
</tr>
<tr>
<td>Content-Type</td>
<td>N</td>
<td>application/json</td>
<td>application/json, application/xml</td>
</tr>
<tr>
<td>fileX-{Attribute}</td>
<td>N</td>
<td>null</td>
<td>fileX-InternalReference=ItemNumber</td>
</tr>
</tbody>
</table>

fileX attribute headers, also referred in this document as ‘fileX metadata’, are available as an option for firms to send additional information about the files being uploaded while making the REST API calls.

Note: You may send up to 5 optional fileX metadata as key-value pairs while uploading a file to the application sub-space. The header attribute keys must start with ‘filex-’ to process the request correctly. The ‘key’ names are case insensitive while values are case sensitive. Do not send any PII data in the optional fileX metadata.

5.4 REST API Catalog

5.4.1 List Available Applications

HTTP Method: GET
GET data URI: files/{ORG_ID}

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG_ID</td>
<td>Y</td>
<td>Numerical values 0-9+</td>
<td>N</td>
<td>Number representing the account’s orgId provided by FINRA (e.g. 0001 or 888888)</td>
</tr>
</tbody>
</table>

Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the present working space/directory</td>
</tr>
<tr>
<td>type</td>
<td>Type of this object</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>metadata -&gt; writable</td>
<td>denotes if this is a writable space</td>
</tr>
<tr>
<td></td>
<td>true/false</td>
</tr>
<tr>
<td>children</td>
<td>Child spaces/directories accessible</td>
</tr>
<tr>
<td></td>
<td>Name, type, and metadata values are similar to self</td>
</tr>
<tr>
<td>_links</td>
<td>API links to self and children</td>
</tr>
</tbody>
</table>
Sample Code:

**cURL:**

```bash
```

**Python:**

```python
import base64, requests, sys
username = '1234ftp12'
password = '**********'
# Base64 encode username:password
authorization = base64.b64encode(username + ': ' + password)
# Prepare headers for GET call
requestHeaders = {
    'Authorization': 'Basic ' + authorization,
    'Accept': 'application/json'
}
# Make the request
url = 'https://filex.finra.org/files/0001'
response = requests.get(url, headers=requestHeaders)
```

### 5.4.2 List Available Application Sub-Spaces

HTTP Method: GET

GET data URI: `files/{ORG_ID}/{APPLICATION}`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG_ID</td>
<td>Y</td>
<td>Numerical values 0-9+</td>
<td>N/A</td>
<td>Number representing the account’s orgId provided by FINRA (e.g. 0001 or 888888)</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application (e.g. focus, crd, appX)</td>
</tr>
</tbody>
</table>
Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the present working space/directory</td>
</tr>
<tr>
<td>type</td>
<td>Type of this object</td>
</tr>
<tr>
<td>DIR</td>
<td><strong>DIR</strong> = directory</td>
</tr>
<tr>
<td>metadata -&gt; writable</td>
<td>denotes if this is a writable space</td>
</tr>
<tr>
<td>true/false</td>
<td></td>
</tr>
<tr>
<td>children</td>
<td>Child spaces/directories accessible</td>
</tr>
<tr>
<td>_links</td>
<td>API links to parent, self and children</td>
</tr>
<tr>
<td></td>
<td>Name, type, and metadata values are similar to self</td>
</tr>
</tbody>
</table>

Sample Code:

**cURL:**

curl https://filex.finra.org/files/0001/app1 -H "Accept: application/json" -H "Authorization: Basic ZmFrZVVzZXI6ZmFrZV8hc3M="

**Python:**
5.4.3 List Available Files in Application Sub-Space

HTTP Method: GET

GET data URI: files/(ORG_ID)/(APPLICATION)/(SUB-SPACE)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG_ID</td>
<td>N</td>
<td>Numerical values 0-9+</td>
<td>N/A</td>
<td>Number representing the account’s orgId provided by FINRA (e.g. 0001 or 888888)</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application</td>
</tr>
<tr>
<td>SUB-SPACE</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application subspace</td>
</tr>
</tbody>
</table>

Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the present working space/directory</td>
</tr>
<tr>
<td>type</td>
<td>Type of this object</td>
</tr>
<tr>
<td>metadata -&gt; writable</td>
<td>denotes if this is a writable space</td>
</tr>
<tr>
<td>children -&gt; name</td>
<td>Name of the file</td>
</tr>
<tr>
<td>children -&gt; type</td>
<td>Type of this object</td>
</tr>
<tr>
<td>children -&gt; metadata -&gt; writable</td>
<td>denotes if this file can be modified</td>
</tr>
<tr>
<td>children -&gt; metadata -&gt; contentLength</td>
<td>Size of the file in bytes</td>
</tr>
<tr>
<td>children -&gt; metadata -&gt; lastModified</td>
<td>Time file was last modified with UTC time zone</td>
</tr>
<tr>
<td>_links</td>
<td>API links to parent, self and children</td>
</tr>
</tbody>
</table>
Sample Code:

**cURL:**


**Python:**

```python
import base64, requests, sys
username = '1234ftp12'
password = '*********
# Base64 encode username:password
authorization = base64.b64encode(username + ':' + password)
# Prepare headers for GET call
requestHeaders = {
    'Authorization': 'Basic ' + authorization,
    'Accept': 'application/json'
}
# Make the request
url = 'https://filex.finra.org/files/0001/app1/out'
response = requests.get(url, headers=requestHeaders)
```
5.4.4  Download File from Application Sub-Space

Downloading a file is a two-step operation. Details are below.

HTTP Method: GET (Step 1)
GET pre-signed URL URI: files/(ORG_ID)/(APPLICATION)/(APPLICATION_SPACE)/(FILE_NAME)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG_ID</td>
<td>N</td>
<td>Numerical values 0-9+</td>
<td>N/A</td>
<td>Number representing the account’s orgId provided by FINRA (e.g. 0001 or 888888)</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application</td>
</tr>
<tr>
<td>SUBSPACE</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application subspace</td>
</tr>
<tr>
<td>FILE_NAME</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]!@,&amp;-=.'</td>
<td>Y</td>
<td>Name of the file</td>
</tr>
</tbody>
</table>

Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>URL used to execute the file download via GET call</td>
</tr>
<tr>
<td>expirationTime</td>
<td>Time URL expires. Cannot initiate download after expiration time.</td>
</tr>
</tbody>
</table>

```json
{
}
```

HTTP Method: GET (Step 2)
GET file URI: <pre-signed URL received in Step 1>

Response:
You will get 200 OK HTTP response code on successful download of the file.

Sample Code:
cURL command to get the pre-signed URL:
```bash
```
cURL command to download the file using pre-signed URL:
```bash
curl -X GET -o file1.txt "<pre-signed URL received in Step 1>"
```
5.4.5 Upload File to Application Sub-Space

Uploading a file is a two-step operation. Details are below.

HTTP Method: PUT (Step 1)

PUT pre-signed URL URI: files/{ORG_ID}/{APPLICATION}/{APPLICATION_SPACE}/{FILE_NAME}

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG_ID</td>
<td>N</td>
<td>Numerical values 0-9+</td>
<td>N/A</td>
<td>Number representing the account’s orgId provided by FINRA (e.g. 0001 or 888888)</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application</td>
</tr>
<tr>
<td>SUBSPACE</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application subspace</td>
</tr>
<tr>
<td>FILE_NAME</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]@,&amp;=.'</td>
<td>Y</td>
<td>Name of the file</td>
</tr>
<tr>
<td>file{x-attribute}</td>
<td>N</td>
<td>Alphanumeric [a-zA-Z0-9]@,&amp;=.'</td>
<td>N</td>
<td>Optional metadata that can be attached with the file e.g. filex-InternalReference</td>
</tr>
</tbody>
</table>

Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>URL used to execute the file upload via PUT call</td>
</tr>
<tr>
<td>expirationTime</td>
<td>Time URL expires. Cannot initiate download after expiration time.</td>
</tr>
<tr>
<td>trackingId</td>
<td>Unique Identifier to track the upload file request</td>
</tr>
</tbody>
</table>
HTTP Method: PUT (Step 2)

PUT pre-signed URL URL: <pre-signed URL received in Step 1>

Header:

The following headers are required for this PUT operation:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Length</td>
<td>Size of the file to be uploaded in bytes (0 or +ve integer)</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/octet-stream</td>
</tr>
</tbody>
</table>

Response:

You will get 200 OK HTTP response code on successful upload of the file.

Sample Code:

cURL without fileX Attribute Header to get the pre-signed URL (Step 1):


cURL with fileX Attribute Header to get the pre-signed URL (Step 1):


cURL to upload the file using pre-signed URL in Step 1 (Step 2):

curl -X PUT -T ./newFile.zip <pre-signed URL received in Step 1>
Python without fileX Attribute Header (Step 1):

```python
import base64, requests, sys

username = '1234ftp12'
password = '*******'
# Base64 encode username:password
authorization = base64.b64encode(username + ':' + password)
# Prepare headers for GET call
requestHeaders = {
    'Authorization': 'Basic ' + authorization,
    'Accept': 'application/json'
}
# Make the request
url = 'https://filex.finra.org/files/0001/app1/in/newFile.zip'
response = requests.get(url, headers=requestHeaders)
```

Python with fileX Attribute Header (Step 2):

```python
import base64, requests, sys

username = '1234ftp12'
password = '*******'
# Base64 encode the username and password
authorization = base64.b64encode(username + ':' + password)
# Prepare the PUT header
requestHeaders = {
    'Authorization': 'Basic ' + authorization,
    'Accept': 'application/json',
    'filex-InternalReference': '0123456'
}
# Make the request
response = requests.put('https://filex.finra.org/files/0001/app1/in/newFile.zip', headers=requestHeaders)
```

Python code to upload the file using pre-signed URL in Step 1 (Step 2):

```python
import requests, sys
# Prepare for PUT header
requestHeaders = {
    'Content-Type': 'application/octet-stream'
}
# Make the request
with open('newFile.zip', 'rb') as f:
    response = requests.put('<pre-signed URL received in Step 1>', headers=requestHeaders, files=('newFile.zip': f})
```

### 5.4.6 Track File uploaded to Application Sub-Space

**HTTP Method:** GET

**GET data URI:** /tracking?id={TRACKING_ID}

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACKING_ID</td>
<td>N</td>
<td>UUID in alphanumeric with '-'</td>
<td>Y</td>
<td>Unique identifier returned when file was uploaded to an application sub-space</td>
</tr>
</tbody>
</table>
Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trackingId</td>
<td>Unique identifier returned when file was uploaded to an application sub-space</td>
</tr>
<tr>
<td>submissionTime</td>
<td>Time at which file was submitted</td>
</tr>
<tr>
<td>userName</td>
<td>Username of the account which was used to upload the file</td>
</tr>
<tr>
<td>fileName</td>
<td>Name of the file submitted</td>
</tr>
<tr>
<td>status</td>
<td>Two possible values: Request Received (pre-signed URL sent by fileX for the upload request) Received by FINRA (file received by fileX through the pre-signed URL)</td>
</tr>
<tr>
<td>statusUpdatedTime</td>
<td>Time when status was last updated. Will be used in future by applications to update file processing status</td>
</tr>
<tr>
<td>fileSize</td>
<td>Size of the file submitted</td>
</tr>
<tr>
<td>uploadLocation</td>
<td>Location at which file was submitted</td>
</tr>
</tbody>
</table>

Note: /tracking without a specific identifier {TRACKING_ID} would return status of all the submissions made in last 90 days.

Sample Code:

cURL:

```bash
curl -X GET https://filex.finra.org/tracking?id=50e1b1c5-6150-4423-9da6-3c51ea34fc30 -H "Accept: application/json" -H "Authorization: Basic ZmFrZVVzZXI6ZmFrZVBhc3M="
```

Python:

```python
import base64, requests, sys
username = '1234ftp12'
password = '******'
# Base64 encode the username and password
authorization = base64.b64encode(username + ':' + password)
# Prepare for GET header
requestHeaders = {
    'Authorization': 'Basic ' + authorization,
    'Accept': 'application/json'
}
# Make the request
response = requests.get('https://filex.finra.org/tracking?id=50e1b1c5-6150-4423-9da6-3c51ea34fc30', headers=requestHeaders)
```
6 S3 Direct Transfer
The fileX service supports S3 Direct Transfers, allowing customers to perform upload/download actions directly to the fileX S3 bucket. Customers can perform S3 actions by first obtaining an access token from the fileX REST API for AWS S3. Customers should use the access token to upload/download using AWS S3 APIs or AWS CLI or AWS SDK wrapper libraries.

6.1 Generate Token for AWS S3
Customers can call the fileX GenerateToken REST API by providing username and password. The REST API returns an access token containing a set of access keys, as described in the response JSON below, which should be used to send/receive files. The generated access token is valid for 1 hour and allows file transfer for the requested application only. If you want to transfer files to a different application, make another API call to request a new access token for that application.

HTTP Method: GET
GET token URI: /S3TransferTokens/(ORG_ID)/(APPLICATION)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required</th>
<th>Accepted Values</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG_ID</td>
<td>Y</td>
<td>Numerical values 0-9+</td>
<td>N/A</td>
<td>Number representing the account’s orgId provided by FINRA (e.g. 0001 or 888888)</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Y</td>
<td>Alphanumeric [a-zA-Z0-9]</td>
<td>Y</td>
<td>Name of the FINRA application (e.g. focus, crd, appX)</td>
</tr>
</tbody>
</table>

Response (JSON):
The request returns a JSON response containing the following:

<table>
<thead>
<tr>
<th>Element/Attribute Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>region</td>
<td>AWS region where S3 bucket is located</td>
</tr>
<tr>
<td>sessionName</td>
<td>Unique identifier generated by fileX for the request to generate the token</td>
</tr>
<tr>
<td>readPaths</td>
<td>List of application spaces available to the users to download file(s)</td>
</tr>
<tr>
<td>writePaths</td>
<td>List of application spaces available to the users to upload file(s)</td>
</tr>
<tr>
<td>accessKeyId</td>
<td>20 character alphanumeric string that identifies the temporary access token</td>
</tr>
<tr>
<td>secretAccessKey</td>
<td>40 character alphanumeric string used to sign the request</td>
</tr>
<tr>
<td>sessionToken</td>
<td>Token that users must pass to the service API to use the access token</td>
</tr>
<tr>
<td>expiration</td>
<td>Time at which current access token expire</td>
</tr>
</tbody>
</table>

Note: Token is valid for 1 hour only. Users will have to generate and use new tokens to upload/download additional file(s) to AWS S3 after the previous token is expired.
Sample Code:

cURL:
```bash
```

Python:
```python
import base64, requests, sys
username = '1234ftpl12'
password = '*******'
# Base64 encode the username and password
authorization = base64.b64encode(username + ':' + password)
# Prepare for GET header
requestHeaders = {
'Authorization': 'Basic ' + authorization,
'Accept': 'application/json'
}
# Make the request
response = requests.get('https://filex.finra.org/S3TransferTokens/0001/app1', headers=requestHeaders)
```

After getting the access token using fileX S3Token API, customers can use any of the AWS S3 APIs, AWS CLI or AWS SDK wrapper libraries to upload/download files. Here is a sample AWS CLI Code to upload a file to an application sub-space

```bash
export AWS_ACCESS_KEY_ID=AIJIA2022000000000000
export AWS_SECRET_ACCESS_KEY=gsbM6wKWNMXxK6wzaZyX6L8744dW2G2p
export AWS_SESSION_TOKEN=FopOgxTVYMsgjGoeDMSLP2oObRUA30jyik0RE/RA9VF9PB6/111p/0Fh89v88TBQ6dsMa2J18K5/yg0CVCQ3IC3fjw9yv8wFQ06BrcsBss93012C4BV8IAjJW8Njyb
#x53v52hj2i312niu=468ypppyjF2Dsp94ACbnH3sju6xj3i1o1jy8WLYvMrHt9DrHeRHS335q35e60gj/3y4k/KG9a/4My8Fg5d8cbe6hK6Kv78Q5E61s15608/EIE1wZ2a16Nh
Xi2QdpbAs8vM2Xw6b2Mz3q884t6s8179411c1ts8ilM1LQ3Jg3p0w0wznzOp3S0x4CQwP0w03w8196y6ne6nF68W77P0o0011KtC7T/A/ds50/Upap/31Te3CFaF0rPA6/sd
fjPLrvrW7iku3X9kxkVQcKFWp7eaeM/uQv0902Q3mM0hM6/s609Mg9FZT2QYyFg2G5b9y88DKi9kYo8y9q2q2fF6R8rjSfaroS5h3yK3dU194mblUP5zun0I8ame4rdw8tC7+4a8f91208d
Te3/M5h8c4t19y75cSeX8XB1r1wcN2oZvXw7y0nh6hAds5x8nSa4P12CFz
ejPF14er6SEsAyv=qQb80c7Jo6VbQb8a1Yy7p7LDR24h21x29f0mZn3j4M17u3Kwh8/7mpqW98xua6X9B/Cvck+S1r6GXXZdp0gw6CF2508/R/
cL8yLX954zdbqATle3ehyiGZ2XgfyfVuAM3BO39ykr2/Mp85W1jzjr/zj80==
aws s3 cp test.txt s3://bucket-filex/0001/app1/in/test.txt
```

Note: Latest documentation on upload/download using AWS S3 APIs or AWS CLI or AWS SDK wrapper libraries can be found here - [https://docs.aws.amazon.com/AmazonS3/latest/dev/MakingRequests.html](https://docs.aws.amazon.com/AmazonS3/latest/dev/MakingRequests.html)
7 Troubleshooting & FAQs

1. What are the supported and unsupported SFTP actions?

SFTP commands supported by fileX: put, get, cd, ls
SFTP commands not supported by fileX: mkdir, rmdir, ln, chgrp, chown, chmod, move, rename
fileX SFTP does not support put append or put resume.

2. What happens when a file is re-uploaded (uploaded twice)?

FINRA handles every uploaded file as a separate submission and delivers to the application that processes that submitted data. Please contact the FINRA support team for guidance in handling re-uploads in specific scenarios.

3. Can I do recursive calls to upload multiple files through fileX SFTP service?

fileX does not allow recursive PUT operations.

4. How do I view the files that I submitted?

fileX service keeps a copy of uploaded files in an archive sub-space, corresponding to the incoming application sub-space where file was originally uploaded. All files are retained in the archive sub-space for 30 calendar days. How to track a file’s progress?

File Tracking API allows users to track files uploaded through REST API. Please refer to section 5.4.6 for more details. For SFTP and S3 Direct, please contact the FINRA support to check the status of a submitted file.

5. Are there any restrictions on the file name?

fileX service allows all letters (a-z)(A-Z), numbers (0-9) and special characters (: ! @ , & = ' _). However file name should not contain ‘#’ as anything after this character in the filename would be ignored.

Each FINRA application may enforce a certain naming convention, please check with that application contacts for additional restrictions.

6. Are there any restrictions on the file size?

fileX service does not put any limit on the file size for SFTP. However it is recommended to keep the file size under 60GB to have better control over the file transfer process.

If you have a need to transfer very large files, please contact FINRA support to facilitate such transmissions.

7. Can I change the file immediately after it is uploaded?

fileX does not allow any changes/operations to the file like changing the owner (CHMOD) or renaming the file. If customers perform these tasks after uploading the file, it would become unusable and customers have to re-upload the file.

Some SFTP clients attempt these actions by default, so they should be disabled.
8. What could be the problem if the file is still in the upload directory and has not moved?

This may happen due to variety of reasons ranging from slow network connection to large file size. It is recommended to wait for few minutes for fileX service to pick up the file(s) before reaching out to FINRA support team.

9. I am not able to see the folder to upload/download file/s. What could be problem?

This could be due to lack of proper/required FINRA entitlements to the specific application you are trying to upload/download. Please contact FINRA support team.

10. I am not able to upload any file. What could be problem?

fileX allows upload operation only to specific directories for the respective FINRA application. Make sure you are trying to upload to the correct directory. See section 8 for FINRA Application specific directory information. In addition you need to make sure the account performing the upload has the proper entitlements for that application. Please contact FINRA support team for questions related to FINRA Entitlements.

11. Am I allowed to rename or delete file/s in download location?

fileX does not allow rename or delete operations on files at the download locations.

12. How many files can I transfer together using fileX service?

SFTP and AWS S3 Direct transfer methods do not have any limit on the number of files that could be transferred in a single operation but HTTPS REST method allows only ONE file per API call.

13. What happens when two sessions from the same firm log in with the same entitlements?

Both sessions will see the same directories and files. fileX service moves the file(s) immediately after the upload is complete, so a file that gets uploaded in session 'A' may "disappear" from view of session 'B'.

14. Is there a SFTP Client UI to exchange file(s) through fileX?

fileX service with FINRA is tested with some SFTP clients like FileZilla, SecureFX and WinSCP.

15. I am a new member/customer of FINRA. How do I request access to fileX services?

As mentioned in this document, fileX service access is controlled by credentials provided and permissioned by FINRA Entitlement services. Please contact FINRA support to request access. You may also check https://www.finra.org/industry/entitlement-program for information related to Entitlement process.

16. I am not able to connect. What should I do now?

Your account may not be active or locked out. Also check with FINRA support team to check the status of the account and it has correct privileges to use fileX services.

17. My account got locked out, how do I reset my account?

The account will be locked out if it connects with invalid credentials, please contact FINRA support for further help with the account.
18. Does fileX SFTP support SSH Keys?

No, SSH Key based authentication is not supported for SFTP at this time. It may be supported in future.

It is recommended to use the following options in the SFTP connection configuration so connection is made via password instead of attempting with public keys.

- PreferredAuthentications=password
- PubkeyAuthentication=no

19. My connection got disconnected while I was uploading the file, what should I do now?

You may still see the file in the folder but it is highly recommended to upload the file again. fileX must receive a successful upload complete status from client applications before it starts processing file(s). When re-uploading the same file, name sure the file name is not changed.

20. I am getting network connection errors while trying to connect to fileX and perform file transfer operations using SFTP. What could be the issue?

Network connection errors may occur because IP Address or DNS names are not whitelisted by either your network/firewall department or FINRA’s network/firewall department. Please ensure you have whitelisted fileX SFTP IP addresses as required and verify outflow of traffic at your end. Inform FINRA of your outgoing IP address (internet routable IP addresses) so it could be whitelisted on FINRA’s side (see also question 22) by contacting FINRA support team.

Network connection errors could also happen due to encryption key related issues. If the problem still persists after whitelisting IP addresses, please contact FINRA support team to troubleshoot.

21. I am currently transferring files through other FINRA SFTP systems and have provided IP’s to whitelist in the past. Do I need to request to whitelist IP Addresses again to use fileX?

No, FINRA will retain the previously whitelisted IP address for fileX service also.

22. How can I check the health of fileX service status?

You can check the status of the fileX service through the below health check URL: [https://filex.finra.org/health](https://filex.finra.org/health).

23. Why am I getting ‘Too Many Connections Error’ with SFTP method?

You may have too many concurrent connections opened to fileX. Make sure your connections are terminated gracefully after successful upload/download operations.

As a good practice avoid frequent connections to check for a file, only connect at the expected file availability time. Contact the respective FINRA Application to know the expected file availability time/s.

24. My SFTP session is timing out during file transfer. What could be the issue?

This could happen due to network related issues at your end, please check with your network support to ensure proper outbound data traffic flow. If you are still getting this error, please contact FINRA support team to troubleshoot.

25. Can I make a POST request to download the file?

No, fileX only supports GET method to download the file.

26. Which coding/scripting languages are supported when calling HTTPS REST API endpoints?

Any client language can be used to call fileX API endpoints as long as the requests are valid REST calls.
27. Can I pass authentication parameters in the URL instead of headers?
No. fileX only supports authentication parameters to be passed as headers to keep the information secure.

28. Do I need to provide authentication headers again when making call to pre-signed URL to download the file?
No. You do not have to provide the authentication details again to download the file. URL is pre-signed and valid for 1 minute following the GET request. Please make sure to initiate the download request within the 1 minute time limit. If you try to download after the expiration time, the download operation will fail with error message similar to below:

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Request has expired</Message>
  <X-Amz-Expires>59</X-Amz-Expires>
  <Expires>2018-12-11T19:58:13Z</Expires>
  <ServerTime>2018-12-11T23:38:49Z</ServerTime>
  <RequestId>CD51795F7323938B</RequestId>
  <HostId>GZmAO5Wk70cf2S+xxd47hM2oT2UYCs7z9If2y++C4qmR/cU5nM1paCih0LH7JmfrxTyRHdeqkNI=</HostId>
</Error>
```

29. Can some users within the same firm use SFTP and other APIs?
Yes. fileX service experience will be consistent across all the supported methods. Same files will be available in all the supported methods.

30. I am getting 302 response from the APIs instead of 401 for invalid credentials?
It's a known limitation and FINRA will address this in future release. Customers should handle 302 Error codes like 401 and check for credentials.

31. Why I am getting Not Found 404 Error Code when I make tracking API request?
It is a standard HTTP Response Code you get when the tracking ID provided in the API request is either invalid or older than 90 days.

32. Is tracking API supported for files uploaded through all the access methods?
Tracking API from fileX is only supported for upload requests made through HTTP REST APIs.

33. How can I renew the AWS S3 access token after it expires?
You have to call the S3TransferToken API from fileX again to get the new access token.

34. Can I use S3 multipart upload?
Yes. You can find the latest AWS documentation here - https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

35. Can I download files from archive sub-space?
Yes, a user with right entitlement can download file available in the archive sub-space

36. Is file archive supported for all the access methods?
Yes, files uploaded through any of the supported access methods, SFTP, REST APIs and S3 Direct, gets archived for 30 days.
37. Is it recommended to connect to the hostname or IP addresses directly for SFTP connectivity?

It is recommended to connect to the hostname referenced in Section 3: Environment and Connectivity.

38. File download is interrupted and ends up in a partial file. What could be the reason?

Some of the most common reasons are:

- Insufficient space at the location where the file is being downloaded to.
- Some SFTP client libraries are unable to handle packets out of order and the file download stops after a certain size. As a workaround, you can set the QueueDepth/queue_size to 1 which will force the packets to arrive in order. This may slowdown the overall file download operation when downloading very large files.
8 Contact Information

Please call FINRA support at 800-321-6273 or visit the web page at https://tools.finra.org/cc_support/ to open a support request. Please provide the following information when contacting support to help us troubleshoot issues faster:

1. Org ID
2. User account
3. Access method (SFTP, HTTPS REST or AWS S3 Direct)
4. Application space (where you are trying to transfer files)
5. File Name
6. Brief description of the error (include information on tool/language used)
9  Supported Applications and Relevant Parameters

This section lists the application sub-spaces and retention policies for the respective applications in fileX. This section will be updated as FINRA applications migrate to fileX service but if any application space you are trying to use is not listed below, please contact FINRA support to get details.

**Key:**

- **Immediately Moved** - these files are moved out of the indicated sub-space as soon as they are processed by the downstream applications. There should be no expectation that the files in these application sub-spaces will persist beyond the transfer itself.
- **N days** - Number of days for which files will remain in the indicated application sub-space. Files will be removed from the application sub-space after N days have passed.

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Application Sub-Spaces</th>
<th>Allowed Actions</th>
<th>File Retention duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>eFOCUS</td>
<td>{orgId}/focus/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/focus/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>ACATS</td>
<td>{orgId}/acats/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td>CCCS</td>
<td>{orgId}/cccs/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/cccs/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>CRD</td>
<td>{orgId}/crd/incoming_designations</td>
<td>Upload (Designating Authorities Only)</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/crd/incoming_filings</td>
<td>Upload (Firms Only)</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/crd/results</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td></td>
<td>{orgId}/crd/reports</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>Stock Record and allocations</td>
<td>{orgId}/stockrecord/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/stockrecord/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>Bluesheets</td>
<td>{orgId}/blshts/finra_in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/blshts/sec_in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td>Advertising</td>
<td>{orgId}/adv/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/adv/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>4530</td>
<td>{orgId}/r4530/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/r4530/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>INSITE</td>
<td>{orgId}/ifdf/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/ifdf/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>Short Interest Reporting</td>
<td>{orgId}/shorts/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/shorts/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>Regulatory Extensions (REX)</td>
<td>{orgId}/rex/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/rex/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
<tr>
<td>Regulation M Filings</td>
<td>{orgId}/regm/in</td>
<td>Upload</td>
<td>Immediately Moved</td>
</tr>
<tr>
<td></td>
<td>{orgId}/regm/out</td>
<td>Download</td>
<td>30 calendar days</td>
</tr>
</tbody>
</table>

Note: Every incoming application sub-space will have a corresponding <application sub-space>_arcv space. This sub-space will store files received within the last 30 days. The filenames will be prefixed with a timestamp yyyyymmddhh24missSSS_<filename>. Timestamp is in US Eastern. An example would be

```
/0001/app1/in_arcv/20190322190521330_file1.zip
```