CU*ANSWERS
A CREDIT UNION SERVICE ORGANIZATION

MOVEit Secure eMail/HTTPS Access Services
Outline and Policy

Rev 4/12

MOVEit is a secure HTTPS system developed to allow a secure and convenient method for CU*Answers clients and internal staff to exchange sensitive files via the Internet or WAN networks. MOVEit uses the industry-standard HTTP over SSL protocol (HTTPS) to secure data in transit between the client and the server. Following is a description of the overall purpose of this system, as well as a brief outline of its configuration and security parameters.

Purpose

CU*Answers has a secure HTTPS server to facilitate the exchange of sensitive financial information, such as check images. This private server is available to our clients as a method of exchanging sensitive information that is easier than using encrypted email. You must be an approved authorized user to use the CU*Answers secure HTTPS server.

Access Capacity

Access is via the public Internet or private-frame circuits. Private-frame circuits usually have less bandwidth than high-speed Internet access and thus are not always preferred over high-speed Internet access. Additionally, large HTTPS transmissions may interfere with CU*BASE® GOLD traffic on smaller bandwidth frames.

Access is facilitated by use of a standard web browser capable of making HTTPS connections. CU*Answers does not require any specific browser, other than one that meets the above requirement.

Available Access Time Periods

Typically, authorized users may access MOVEit at any time. However, CU*Answers does not guarantee the MOVEit server will be available at any given time. Additionally, CU*Answers reserves the right to restrict access to the server to specific times of day or days of the week. CU*Answers does not back up data on the MOVEit server. The server should not be used for storage of data, as data is automatically purged at least once every 30 days.

Network Accounts

In order for any user to gain remote access to MOVEit, Network management must create a MOVEit account with appropriate privileges. The account includes both a user name and a unique password. This network account will only allow the user access to the approved MOVEit folder(s) authorized by network management.

MOVEit access is controlled by one’s user name and password. Passwords will be determined by network management when the account is created. Passwords will adhere to the standards set by CU*Answers network password policies and will be changed on a periodic basis.

Requesting Access

Requests for access by clients and internal staff members will be tracked using the **MOVEit Secure HTTPS Access Services Request Form**, with an ongoing list of outstanding and implemented requests to be maintained by the Network Services team, overseen by the Network Services Manager.

Following is the basic timeline for request submission and approvals:

1. The request form is completed and submitted to the Network Services team.
2. The request is reviewed against current access policies and authorized user lists, then is routed for approval by the CEO, CIO, or Network Services Manager.
3. Copies of the "CU*Answers MOVEit Secure HTTPS Server Acceptable Use Agreement" and "Using CU*Answers' Secure File Transfer System Best Practices" are sent for signature to the requesting credit union.
4. Both the approved request form and the signed agreement are forwarded to Network Services.
5. Network Services will assign a systems technician to perform the following tasks:
    - The technician will contact the credit union to set up an initial test of the connection and verifying the purpose for the connection (i.e., loan applications, member transactions, etc.).
    - The credit union is provided current user materials showing setup and configuration requirements as well as step-by-step instructions for establishing a connection.
    - A MOVEit account is created and the credit union is contacted with the name and password. The controlled test is performed as scheduled, ensuring that all equipment and account settings work as expected.
    - Once the test has been completed, the technician makes any necessary changes to the account according to the approved request form and contacts the credit union with any final instructions.
6. The request form paperwork, including any notes regarding setup and test results, are returned to the Network Services Manager or designated Network Services team member to be filed.
7. On a daily basis, the designated Network Services team member or assigned technician will be responsible for reviewing access and usage logs.

Security and Monitoring

Network Services will keep a log of MOVEit accounts. In addition to this log, a log of daily remote-access activity will be reviewed on a daily basis by Network Services.

Fees and Charges

At this time this service is provided to CU*Answers clients free of charge.