FILE GATEWAY

EXTERNAL CLIENT BOARDING GUIDE

Version 6.0

Contents

Distribution 4

Author Contact Details 4

Document References 4

Version Control 4

Introduction 5

Document Purpose 5

Business Requirement Summary 5

Client Benefits 5

Client Technical Requirements 5

FIle Naming .... **Error! Bookmark not defined.**

File Naming Convention Standards 6

How the Filename is used in Fiserv File Gateway 6

What does the File Naming Standard give us? 6

How does the File Naming Standard affect clients? 7

User Account Naming Convention Standards 8

What do these usernames mean? 8

External User Names 8

Use of DNS names required 8

Multi-Factor Authentication 8

Connecting to Fiserv 9

Firewall Access 10

Authentication 100

Passwords 11

Public Key Authentication 11

SSL Certificate 11

Transmitting Files 11

Directory Layout 11

Uploading to Fiserv 12

Filename format 12

Encryption and Zip 12

Pass-Through Files 13

Receiving Files From Fiserv 13

Pulling files from Fiserv 13

Pushing Files To A Partner Server 133

Connect:Direct Push Information Needed 14

File Encryption 155

File Compression 15

File Content Limitations 155

MYFILEGATEWAY........15

Scheduled Maintenance 16

North America Production Support Help Desk (24x7) 166

BAMS Clients only 166

Card Clients only 166

Distribution

Name	Business Area/Role	Purpose

Author Contact Details

Name	Global Transmissions Team
Phone	
Email address	

Document References

Document Name	Document Version
FD_SFG_External_Boarding_v1.docx	V1.0

Version Control

	Status	Date	Author	Reason for Version
V1.0		4/18/2016	John Cutchin	Format modification
V1.1		5/5/2016	Todd Struthers	Content modification
V4.0		5/18/2016	Tim Allen	Content modification
V5.0		7/14/2016	Tim Allen	Content modification
V5.1		8/05/2016	Tim Allen	Content modification
V5.2		8/07/2016	Tim Allen	Content modification
V5.3		8/09/2016	Tim Allen	Content modification
V5.4		8/12/2016	Tim Allen	Content modification
V5.5		8/12/2016	Tim Allen	Content modification
V5.6		9/11/2018	Tim Allen	Content modification
V5.7		6/01/2019	Tim Allen	Content modification
V5.8		8/21/2019	Lynne Hannon	Content/Format/Name
V5.9		10/16/2019	Lynne Hannon	Content/Whitelisting
V6.0		11/4/2019	Lynne Hannon	Formatting/Directory

INTRODUCTION

DOCUMENT PURPOSE

This document summarizes the business and technical requirements for migration to Fiserv's new File Gateway platform. The document provides an overview of client impacting changes and requirements as well as general technical information for connecting to the new File Gateway platform.

BUSINESS REQUIREMENT SUMMARY

The Fiserv File Transmission Gateway is a multi-protocol file transfer system for transmitting files to/from Fiserv. Changes to the way a client connects to the File Gateway will be required as transmissions are moved to the new platform. The goals of this platform are to provide standardization and consolidation of existing file transmission systems for improved security and PCI standardization. Migration of file transmissions to the Fiserv global standard will help in improving time to repair and improved support services efficiency.

CLIENT BENEFITS

- Improved Security
  - Compliant with FDC and PCI security standards
  - Multi-Factor Authentication capability
  - TLS 1.2 communication protocol standard for HTTPS and FTPS protocols
- Improved Support Efficiency
  - Efficiencies from platform consolidation
  - Improved "Mean Time to Repair" capability
  - Robust diagnostic capability for improved problem resolution
- Client Benefits
  - Standardized global onboarding processes
  - "Follow the Sun" always available support model
  - Self-service transmission status capability

CLIENT TECHNICAL REQUIREMENTS

- New standard file transmission naming convention
- New standard user/system account name
- Use of DNS names required
- Client Firewall access to Production as well as Disaster Recovery is required
- Multi-Factor Authentication required for **external** transmission
- Use of TLS 1.2 (recommended) for HTTPS and FTPS protocols
- Protocol authentication with SSL certificate (HTTPS / FTPS) or SSH public key (SFTP) required

FILE NAMING

FILE NAMING CONVENTION STANDARDS

In moving towards a global enterprise model for File Transmissions, a common standard for file naming conventions is necessary. The file naming standard that has been defined for the Fiserv File Gateway is the following format.

Files Sent to Fiserv:	**[jobname].[filename].[ext]**
Files Sent From Fiserv:	**[jobname].[date].[time].[ext]**

[jobname]: The jobname is an 8 character all upper case identifier for the file transmission. This value will be provided by Fiserv.

[**filename]:** This section of the filename is optional. The filename can be anything the client or internal team wishes to identify the file on their end. This can include naming conventions required to include date, timestamps, sequence numbers etc. Additional sections, separated by periods, can be supported within this section of the filename.

[date]: The format of the date will be <mmddyyyy>

[time]: The format of the time will be <hhmmss> the [date] and [time] portions of the outgoing file name ensure that there are no collisions or files overwritten on the receiving system.

[ext]: The ext is the file extension for the file that is being transmitted. This can be anything that is necessary to support the format of the file.

NOTE: The total length of a filename cannot exceed 256 characters and spaces in the filename should be avoided and replaced with hyphens and/or underscores.

HOW THE FILENAME IS USED IN FISERV FILE GATEWAY

The standard file naming format is what allows for the file to be routed through Fiserv File Gateway and be delivered to the appropriate end point.

When a file is uploaded into Fiserv File Gateway, the “Consumer Lookup Business Process” determines who the producer (sender) of the file is, as well as captures the filename Regex pattern of the file. The Regex pattern is a unique pattern that is defined by the standard. The business process will determine who the “Producer” of the file is and will utilize the filename submitted to find the appropriate routing and deliverable actions to be taken. By having the jobname in the first position of the file, it serves as the query pattern used to search for the routing and deliverable actions that are stored in the applications database.

WHAT DOES THE FILE NAMING STANDARD GIVE US?

The file naming standard outlined above provides a standard method to route the file. One global enterprise standard gives Fiserv the ability to at any one time, identify, monitor, and provide metrics on all file transmissions globally. This standard streamlines the file transmission support process by providing a format which allows for an improved and efficient global support model to be attainable and realistic by reducing complexity.
The file jobname **[jobname],** is unique to every file transmission. It allows for no duplicate entries to be created which could cause a file to be delivered to an incorrect dataset or client. The filename, with the unique jobname prefixed at the beginning allows for metrics to be pulled at any time allowing Fiserv to quickly, efficiently, and accurately measure throughput performance.

HOW DOES THE FILE NAMING STANDARD AFFECT CLIENTS?

The file naming standard will require changes to be made by our clients. The changes required will vary based on the direction of the file transmission.

SENDING FILES TO THE NEW FISERV FILE GATEWAY

Clients will need to make changes to their system to allow for them to **send** to the new Fiserv File Gateway in the standard naming convention format. Sending users will also have a **new user ID**. The change to the file naming standard does not need to impact the file name that they create and use on their end. As an industry standard, the file transmission sender always provides the ability for the receiving party to dictate the name of the file that they are receiving.

Example:

Using an SFTP transmission as an example. A sender may use a "PUT" statement as follows:

Mput [source filename] [destination filename]

This statement allows for the client to utilize any filename on their source side they wish, but the destination filename is what Fiserv will be needing it to be received as. The client just needs to provide the destination filename **[destination filename]** as in our required standard.
In the case where the client has custom developed and hard coded fine naming in their scripting, changes will need to be made to provide the new receipt format.

RECEIVING FILES FROM THE FISERV GATEWAY

Clients that will be receiving files from Fiserv, **do not** have to receive their files in Fiserv's file naming standard. The Fiserv File Gateway allows for file name masking to take place in the last processing step where the file can be renamed prior to sending to the client.

Example:

A file is uploaded to Fiserv File Gateway named:

ABCDBANK.february_12_2016_Report.txt.

If the client cannot accept the file to be delivered to them in this naming fashion, but prefers the file delivered to them to be:

Settlement_Report_12022016.txt.

This file name change can be completed through the Fiserv File Gateway Delivery Params process.

USER ACCOUNT NAMING CONVENTION STANDARDS

User account naming standards will, just like file naming standards, be a standard that is identifiable from a global enterprise perspective. By utilizing a standard, Fiserv will align with security requirements that will improve the safety and integrity of the data as well as provide for a common support model for all users improving support efficiency. The same credentials (username and password) are utilized on the Client Acceptance Testing (CAT) environment and the Production environment.

Example: **External Users:**

North America: NAGW-ABCDE001

What do these usernames mean?

EXTERNAL USER NAMES

External user names are prefixed with a four letter identifier, this identifier signifies the region (NA, EM, LA, AP) as well as Gateway (GW) for Fiserv File Gateway. With Fiserv File Gateway we are utilizing an Active Directory LDAP that allows us to have single sign-on for the application which is utilized globally.

An easily identifiable way of determining which application the user account is for is necessary. The above naming format for external users allows for support and Active Directory teams to quickly identify that a user is requesting access to the Fiserv File Gateway, and for which region. The ABCDE001 following the region and file gateway identifier prefix, allows for a unique identifier for each client that is non-identifiable while allowing for multiple potential ID's being created for a client should they be needed. By having a random alpha first 5 positions (ABCDE) we are in compliance with Information

Security standards and global security regulations. These 5 characters will be unique to the client, allowing for over 11 million unique combinations. The 001 of the username is a sequence number and every client will have a 001. Should they need to have more user ID's created for other divisions within their company, this number can be increased up to 999.

USE OF DNS NAMES REQUIRED

It will be necessary for client's to use DNS for inbound connections rather than IP address. This is necessary to support multi-site load balancing and disaster recovery situations.

MULTI-FACTOR AUTHENTICATION

Fiserv File Gateway will support MFA (Multi Factor Authentication) and this will require clients to authenticate with 2 forms of authentication.

Multi Factor Authentication requires both items below.

1. Password Authentication *(Non Expiring password on service type accounts)
2. FTPS Certificate or SFTP Key Authentication

TLS 1.2 will be required for HTTPS and FTPS protocols as the Fiserv File Gateway secure protocol. The File Gateway will not be configured for any version of SSL. Browser (HTTPS) based internet access will require User/password and public key certificates for authentication.

CONNECTING TO FISERV

Fiserv provides a highly redundant environment for securely transmitting files with select protocols. Fiserv supports SFTP, FTPS (Explicit only) and Connect:Direct connections and provide access to a secure web interface. The table below shows each supported protocol, the type of transmission available, and the connection types supported.

Protocol	Receive Files From FD	Send Files To FD	Network Type
SFTP	Push Client Pick up	Push	Internet Dedicated
FTPS (Explicit)	Push Client Pick up	Push	Internet Dedicated
Connect:Direct	Push	Push	Internet Dedicated
Web	Client Pick up	Push	Internet

Fiserv provides two public environments: CAT and Production for North America

NORTH AMERICA CONNECTION DATA			
Access Method		CAT	Production
Dynamic Internet	Domain Name	test2-gw-na.firstdataclients.com	prod2-gw-na.firstdataclients.com
	SFTP Port	6522	6522
	FTPS Ports	6521/20000-20100	6521/20000-20100
	C:D Ports	1364	1364
	Web	443	443
Dedicated	Domain Name	test-gw-na.firstdataapps.com	prod-gw-na.firstdataapps.com
	SFTP Port	6522	6522
	FTPS Ports	6521/20000-20100	6521/20000-20100
	C:D Ports	1364	1364

All configurations are built in the CAT environment and tested prior to promotion to the production environment. Once successful testing in the CAT environment has been completed, subsequent transmissions should be routed through the production environment. The intent of the CAT environment is for initial or changed configuration testing only.

FIREWALL ACCESS

Fiserv provides a secure file gateway service that is a public service for all Fiserv customers as an internet service. Fiserv is discontinuing the use of whitelisting source IP address restrictions and is standardizing on modern security measures for its internet based products. Fiserv utilizes blacklisting along with a combination of Certificate based authentication and multi-factor authentication to limit access to this service and keep the service highly available. The File Gateway services are protected by always on DDOS and Next Generations firewalls leveraging IPS protections. Using the whitelisting method causes delays in onboarding clients as well as outages in the client's service with any client IP changes.

FISERV NORTH AMERICA –

Primary IP addresses are:

Static Internet 216.66.218.146 and DR Static 208.72.249.199

Dynamic Internet 216.66.218.161 and DR Dynamic 208.72.249.221

Dedicated connectivity 204.194.139.35 and DR 204.194.127.150

CAT IP addresses are:

Static Internet 216.66.218.147 and Static DR CAT 208.72.249.200

Dynamic Internet 216.66.218.162 and Dynamic DR 208.72.249.222

Dedicated connectivity 204.194.139.36 and DR 204.194.127.151

All IP's need to be added as we will switch over to Disaster Recovery at certain periods to validate our Disaster Recovery

AUTHENTICATION

Access to the Fiserv File Gateway requires the use of multi-factor authentication. You will be provided a username and password. You will need to provide the second authentication factor to Fiserv, dependent on the protocol chosen. **We do not encourage the use of self-signed certificates. Please use a provider that can provide a Public SSL certificate that will work with the File Gateway service. (E.g. DigiCert)**

Protocol	2nd Factor	Minimum Bit Strength
HTTPS	Public SSL certificate (TLS 1.2)	2048
FTPS	Public SSL certificate (TLS 1.2)	2048
SFTP	SSH Public Key	2048
C:D	Secure+ SSL Certificate	2048

PASSWORDS

Passwords are required to adhere to Fiserv Security requirements. Users will be provided a temporary password when the user account is created. The temporary password must be changed to one meeting the following requirements:

- Passwords must be a minimum length of eight (8) characters
- Passwords must be a combination of alpha, numeric or special characters
- Passwords must use, at a minimum, at least one number, one upper case alpha character, one lower case character and a special character

Fiserv security policy supports non-expiring passwords for automated service type accounts. If you need to change your pass it will be supported by Identity Minder solution that will allow the client to reset their own password.

PUBLIC KEY AUTHENTICATION

Partners connecting to Fiserv using SFTP must utilize SSH Public Key authentication in conjunction with a password. If you need to add or change your public key at any time, please contact your Fiserv Account Manager or Relationship Manager to initiate a request.

SSL CERTIFICATE

Partners using FTPS or connecting to our web interface using HTTPS will need to provide a valid, Public SSL certificate to connect to our system. We do not encourage the use of self-signed certificates. **Please use a provider that can provide a Public SSL certificate that will work with the File Gateway service. (E.g. DigiCert) Should you wish to use SFTP Pick Up or SFTP Push AND MyFileGateway, two mailboxes will be created for you.**

If you need to change your public certificate at any time, please contact your Fiserv Account Manager or Relationship Manager to initiate a request.

TRANSMITTING FILES

DIRECTORY LAYOUT

When connecting to the Fiserv File Gateway, the file directory layout is dependent on the transmission method and direction of the file:

Directory	Use	Note
/	Upload Directory	Upload directory for SFTP/FTPS
/mailbox/	Connect:Direct upload directory	Upload directory for Connect:Direct only
/available	New files available to download	Used for pulling new files. Only visible when pulling files from Fiserv
/downloaded	Archive of previously downloaded files	For pulling files you have pulled previously. Only visible when pulling files from Fiserv

UPLOADING TO FISERV

The push method of file delivery is the standard method of delivery for files to the Sterling File Gateway as this provides for direct alerting on failure. The reason for this is a "pull" does not provide for an appropriate method of alerting on delivery.

FILENAME FORMAT

All files submitted to Fiserv will be prefixed with a job name identifier supplied to you by the file transmission representative creating your account. The job name is eight (8) uppercase alpha-numeric characters followed by a period.

SFTP/FTPS

Example:

Your local file is called '***SettlementFile.txt***'

Your transmission representative provides you with the job name ***AB9TQXY1***

You will upload a file with the name ***AB9TQXY1.SettlementFile.txt***

CONNECT:DIRECT

Connect:Direct example:

Your local file is called '***SettlementFile.txt***'

Your transmission representative provides you with the job name ***AB9TQXY1***

You will upload a file with the name ***AB9TQXY1.SettlementFile.txt***

When uploading files to Fiserv using Connect:Direct, all files are uploaded to:

/mailbox/NAGW-USRID001.{filename}

ENCRYPTION AND ZIP

Fiserv supports incoming files in text, compressed (Zip or GZip), or PGP/GPG encrypted (unsigned).

PGP/GPG:

If you require the use of PGP/GPG, your transmission representative will provide the Fiserv public PGP/GPG key. Due to the use of secure transmission protocols, PGP/GPG is not required.

Zipped Files:

- Fiserv *does not* support password-protected Zip files.
- Only one (1) file should be contained in a zip file.

All files uploaded to the Fiserv File Gateway will be uploaded to the home directory (the default directory after logging in)

PASS-THROUGH FILES

If your zip file contains multiple files or your PGP/GPG encrypted file must remain encrypted for the intended recipient, please notify the transmission representative assigned to your project to have the files passed through without additional processing.

RECEIVING FILES FROM FISERV

Partners can choose to either pull files from the Fiserv File Gateway or have files pushed to a server using supported protocols. Your file transmission representative will provide documentation containing a job name for each file you will receive. Fiserv uses the following standard file name format described above:

{JOBNAME}.{Date}.{Timestamp}.{Extension}

Example:

CB9TQXY2.20150922.122312.TXT

PULLING FILES FROM FISERV

For partners pulling files from the Fiserv File Gateway, newly available files are available in a sub-directory of the user's home directory called "available". Once a file has been downloaded one (1) time, a backup copy is available in the "downloaded" sub-directory.

If you need to have a file re-transmitted, please check the 'downloaded' directory for a copy prior to escalating.

PUSHING FILES TO A PARTNER SERVER

For partners who wish to have files pushed to their server, additional information must be provided:

SFTP (SSH) INFORMATION NEEDED

Value	Description
Host	The URL or DNS name of the server
Port	Port number to connect to
Username	Username assigned for the file transmission
Authentication Type	Non-expiring Password and/or SSH Public Key authentication
Password	If not using SSH Public Key authentication
Temp Path	Initial upload path if required
File Path	Final path to where the transmitted file is delivered
File Mask	A mask can be used to make limited changes to the received filename. If none is provided, Fiserv will use the standard file name format mentioned above.
SSH Host Key	Fiserv will supply the SSH public key if files are pushed via SFTP

FTPS PUSH INFORMATION NEEDED

Value	Description
Host	The URL or DNS name of the server
Port(s)	Port number to connect to as well as the data port range
Username	Username assigned for the file transmission
Password	Password assigned to the user
Temp Path	Initial upload path if required
File Path	Final path to where the transmitted file is delivered
File Mask	A mask can be used to make limited changes to the received filename. If none is provided, Fiserv will use the standard file name format mentioned above.
Data Connection	Passive or Active
Server Type	Explicit or Implicit
Server Fingerprint	Used to validate the remote server instead of a full certificate

CONNECT:DIRECT PUSH INFORMATION NEEDED

Value	Description
Node Name	Name of the node we will push files to
Host	The URL or DNS name of the server
Alternate Host	Alternate IP or DNS name if used
Port	Port number to connect to
Username	Username assigned for the file transmission if not using Secure Point of Entry (SPOE)
Password	If not using SPOE
File Path	Final path to where the transmitted file is delivered if needed
Remote Filename	File name to write to. If none is provided, Fiserv will use the standard file name format mentioned above.
Runtask	Runtask information if required (maximum of 5 can be supported)
Run Job	Run job information if required (maximum of 5 can be supported)
Secure+ Certificate	Share certificates for secure+ builds.

FILE ENCRYPTION

Fiserv supports PGP/GPG encryption as an optional feature for an additional layer of security.

If a Partner chooses to use PGP/GPG encryption and receives files from Fiserv, the Partner must provide a PGP/GPG key to the Fiserv transmission representative assigned to the project. If your key has an expiration date, you'll need to contact your Fiserv Account Manager or Relationship Manager to initiate a request prior to the expiration date. Fiserv recommends a minimum of 2048 bit RSA keys for security reasons.

If a Partner chooses to send files to Fiserv using PGP/GPG encryption, the Fiserv transmission representative setting up the file transmission will provide the Partner with the Fiserv Public PGP key. Fiserv's key is a 2048 bit RSA key.

The following algorithms are supported:

Property	Value
Pubkey	RSA, RSA-E, RSA-S, ELG-E, DSA
Cipher	3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash	MD5, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression	Uncompressed, ZIP, ZLIB, BZIP2

FILE COMPRESSION

Fiserv supports the Zip and GZip file compression formats. If compression is requested, please indicate the preferred file compression format to the Fiserv transmission representative implementing your file transmissions.

FILE CONTENT LIMITATIONS

For security purposes, no *production* data should be submitted to the *test* environment

MYFILEGATEWAY

MyFileGateway is a web based site to support the client activities. Clients can upload or download files, run reports, and view the complete process from arrival to delivery of files. **Please use a provider that can provide a Public SSL certificate that will work with the MyFileGateway service. (E.g. DigiCert) Should you wish to use SFTP Pick Up or SFTP Push AND MyFileGateway, two mailboxes will be created for you.**

MyFileGateway will require a separate account if you are using the service account non-expiring password setup. Passwords on MyFileGateway will expire every 60 days.

Subscribe to notifications to receive email about Fiserv File Gateway activity.

Procedure

1. From the main menu, select **Profile**.
2. Select the **Notifications** tab.
3. Drag an event from the left pane to the right pane to enable notifications.

Results: When an event occurs, an email notification is sent to the email address in your user account.

SCHEDULED MAINTENANCE

Fiserv has established a scheduled maintenance window for the Fiserv File Gateway environment.

Maintenance Windows:

Every Saturday of the month between 20:00 - 02:00 Eastern.

The Fiserv File Gateway environment may be unavailable during this time.

NORTH AMERICA PRODUCTION SUPPORT HELP DESK (24X7)

After file transmissions are promoted to production, the initial point of contact for any file transmission issues in production will be the appropriate Help Desk:

BAMS CLIENTS ONLY

Please contact:

BAMS IOCC number	**(866) 934-9423 Opt 1-2**

CARD CLIENTS ONLY

Please contact:

Fiserv Response Center	**(800) 337-1222**

APPLICATION PLATFORMS OTHER THAN CARD OR BAMS

Please contact:

Fiserv Customer Support Center	**(800) 555-9966**

Please contact the Fiserv Customer Support Center at for any assistance at the above help desk numbers regarding your production files and to initiate a ticket. Please identify yourself as a Fiserv File Gateway client and have your JOBNAME/Class ID available with any other pertinent information to help expedite your inquiry.