Sterling File Gateway

EBICS System Administrator Help

Version 2.0

Contents

Install and Set Up

Create User Accounts

Create user accounts in the B2B Console.

To create a user account:

1. From Sterling File Gateway, select **Tools** > **B2B Console**.
2. From within Sterling Integrator, Select **Accounts** > **User Accounts** > **Create a new Account**.
3. Complete the steps in the wizard.

   Supply the following information about the user:

   - Authentication type (Local or external)
   - User ID - by default, the User ID must be at least five characters. To enable shorter or require longer User IDs, modify the following property in customer_overrides.properties:

     ```
     userIdMinLength.ui=(# of characters)
     ```

     The value of # of characters must be greater than zero. To implement single sign-on, this value must match the value set in Sterling Integrator.
   - Password
   - Confirm Password
   - Policy - choose from:
     - [blank] (default)
     - Default User Policy - For the default user policy, the password must be at least six characters and is required to contain at least two of the following characters. (numeral, capital letter, !, @, #, $, %, ^, &, *)
     - You can create a different policy for your system. Create the policy in Sterling Integrator first, then select it from the list when you create a user.
   - SSH Authorized User Key
   - Session Timeout (in minutes)
   - Accessibility
   - Dashboard Theme

   See *Managing User Accounts.*

4. Select one or more groups from the following list:

   • File Gateway Integration Architects - can only access File Gateway, not *myFileGateway*
   • File Gateway Operators - can only access File Gateway, not *myFileGateway*
   • File Gateway Partner Users - can only access *myFileGateway*
   • File Gateway Route Provisioners - can only access File Gateway, not *myFileGateway*
   • File Gateway System Administrators - can only access File Gateway, not *myFileGateway*

   Note: For full Sterling File Gateway functionality, each of these groups must have at least one user. By default, the following users are created during installation of Sterling File Gateway:

   • fg_sysadmin - belongs to all File Gateway groups except File Gateway Partner Users. Also belongs to Sterling Integrator Admin group.
   • fg_architect - belongs to File Gateway Integration Architects group
   • fg_provisioner - belongs to File Gateway Route Provisioners group
   • fg_operator - belongs to File Gateway Operators group

   A user can belong to multiple groups, but cannot belong to File Gateway Partner Users group while a member of any other group.

   Note: To protect the security of your system, delete the default users or change the default passwords.

   Note: To create an independent user that is the equivalent of fg_sysadmin, assign the Sterling Integrator Admin group and all File Gateway groups except File Gateway Partner Users group to that user.

5. Select the permissions for the user. (Optional.) The group assignments include the standard permissions for users of each group.
6. Supply the following information for the user:

   • First Name
   • Last Name
   • E-mail
   • Pager
   • Preferred Language (English, Japanese)
   • Manager ID
   • Identity

7. Review and confirm to create the new user account.

User Interface Access

Access to each page of the user interface is authorized based on permission groups assigned when the user is created.

The following table describes which screens and functions each persona can access:

Page	System Admin	Integration Architect	Route Provisioner	Operator	Partner
Routes > **Activity**	(Default page.) Can search and	Can search and view events, but	Can search and view events, but	(Default page.) Can search and view	No access.

Page	System Admin	Integration Architect	Route Provisioner	Operator	Partner
	view details and links to details in B2B Console. Can mark routes as reviewed or not reviewed. Can replay and redeliver.	cannot view linked details. Can mark routes as reviewed or not reviewed. Cannot replay or redeliver.	cannot view linked details. Can mark routes as reviewed or not reviewed. Cannot replay or redeliver.	details and links to details in B2B Console. Can mark routes as reviewed or not reviewed. Can replay and redeliver.	
Routes > **Channels**	Can view and edit.	No access.	(Default page.) Can view and edit.	No access.	No access.
Routes > **Templates**	Can view and edit.	(Default page.) Can view and edit.	No access.	No access.	No access.
Participants > **Groups**	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
Participants > **Partners**	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
Participants > **Communities**	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
Tools > **Reports**	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
Tools > Activity Snapshot	Can view and get events and complete details.	Can view and get events, but not details.	Can view and get events, but not details.	Can view and get events and complete details.	No access.
Tools > **B2B Console**	Can view and edit complete Admin menu.	Can only view and edit Accounts > My Account.	Can only view and edit Accounts > My Account.	Can view and edit Business Processes and Operations menus, and Accounts > My Account.	No access.
Tools > **Logs**	Complete access to all logs.	No access.	No access.	Complete access to all logs.	No access.
Profile > **Notifications**	Can subscribe and delete.	Can subscribe and delete.	Can subscribe and delete.	Can subscribe and delete.	No access.
Profile > **Password**	Can change own password, unless external user. Can change other users passwords.	Can change own password, unless external user.	Can change own password, unless external user.	Can change own password, unless external user.	No access.
myFileGateway > **Activity** > **Upload Files**	No access.	No access.	No access.	No access.	(Default page.) Complete access to search, generate reports, upload files,

Page	System Admin	Integration Architect	Route Provisioner	Operator	Partner
> **Download Files** > **Reports** > **Profile**					and download files when Partner is producer or consumer. Can subscribe and unsubscribe to notifications and can change own password.
Help	Can view all Help libraries.	Can view all Help libraries.	Can view all Help libraries.	Can view all Help libraries.	Can only view myFileGateway Help, not the other persona libraries.

Use Preconfigured User Groups to Assign Permissions

To assign permissions to users, you can assign user accounts the groups that come preconfigured with Sterling Integrator. Users inherit all permissions associated with the groups.

Permissions Inherited from Groups

These groups are preinstalled with Sterling Integrator and the permissions are inherited when the group is assigned to a user account. The same permissions are inherited when a group is assigned as a subgroup.

Group	Permissions Inherited from the Group
File Gateway Integration Architects	Dash AFT Theme
File Gateway Operators	Dash AFT Theme, UI BP Manager, UI BP Monitor, UI Business Process, UI Lock Manager, UI Logs, UI Operations, UI reports Plus, permissions inherited from subgroups: Subgroup BPMONITOR - BPSSCorrelation, BusinessProcesses, CentralSearch, CommunicationSessions, Correlation, CurrentActivities, CurrentDocuments, CurrentProcesses, DataFlows, Documents, EBXMLCorrelation, EDICorrelation, EDIINT, GentranServerforUnix, Message Entry Workstation Home, SWIFTNETCorrelation, UI BP Monitor Subgroup OPERATIONS - JDBCMonitor, MessageMonitor, Perfdumps, SequenceManager, Statistics, ThreadMonitor, Troubleshooter, Tuning, UI Federated Systems, UI Operations
File Gateway Partner Users	myFilegateway Login myFilegateway Logout myFilegateway User Name myFilegateway File Activity myFilegateway File Upload myFilegateway File Download

Group	Permissions Inherited from the Group
	myFilegateway Reports myFilegateway Event Subscription myFilegateway Change Password myFilegateway Help myFileGateway Upload Applet myFileGateway Download Applet File Gateway Auto-grant Mailbox Permissions
File Gateway Route Provisioners	Dash AFT Theme
File Gateway System Administrators	None. System Administrators have unlimited access to all resources.

Modify Group Permissions

System Administrators can edit group permissions, or create new groups with different permissions. For example, to create a group of operators that can view and edit troubleshooting menus, but do not have permission to view or edit tuning menus:

1. Select **Tools** > **B2B Console**.
2. From the Admin menu, select **Accounts** > **Groups**.
3. Next to **Create a New Group**, click **Go!**
4. Type a **Group ID** and **Group Name**. Click **Next**.
5. On the **Assign Subgroups** page, select BPMONITOR. Click **Next**.
6. On the **Assign Permissions** page, select the following:

   • **Dash AFT Theme**
   • **UI BP Manager**
   • **UI BP Monitor**
   • **UI Business Process**
   • **UI Lock Manager**
   • **UI Logs**
   • **UI Operations**
   • **UI reports**
   • **Troubleshooter**

   Click **Next**.
7. Click **Finish** and **Return**.
8. Create or edit users, assigning them to the group you just created. These users will have access to the **Operations** > **Troubleshooter** menu, without access to the **Operations** > **System** menu and submenus.

Migrate from Advanced File Transfer to Sterling File Gateway

If you have an existing installation of Advanced File Transfer (AFT), you can migrate the partner configurations to Sterling File Gateway.

To migrate partner configurations from AFT:

1. Run the following script:

<install_dir >/tp_import/aft2fg.sh (for UNIX) or aft2fg.cmd (for Windows)

2. The script performs the migration and displays details of the migration.

   The following operations are performed:

   - Static and dynamic routing channels are created, based on the consumer identification policies in effect for the migrated producers.
   - AFT routing rules are replaced with a single automatic evaluation Sterling File Gateway routing rule.
   - AFT Route Business Process is disabled.
   - If a consumer identification policy of Use Map was utilized in AFT, a routing channel template is created so that the map will continue to drive the consumer identification. After conversion the name of the map used in the routing cannot be changed in Sterling File Gateway. The name of the map used is visible from the Data Session details window only.
   - PGP settings remain in effect.
   - The Advanced File Transfer tab in Sterling Integrator will be available, but limited to offer AFT Route Activity and Reporting links so that a legacy AFT user can still view old AFT data for as long as it exists in the system.

3. If the migration fails, an error message is displayed. The migration report states what changes were successfully completed. Correct the error conditions and proceed. It is safe to run the script again.
4. The imported partners will automatically be associated with the "All Partners" partner group. You can also associate the newly migrated Partner with other Sterling File Gateway partner groups to make them work with routing channel templates that have specified these partner groups.
5. Turn off the AFTPurgeArchiveMailboxes business process in Sterling Integrator.

About Export and Import

The Import/Export feature enables you to save time and increase the accuracy of duplicating supported resources on different Sterling Integrator or Sterling File Gateway environments that are set up for unique purposes. Specifically, the Import and Export options enable you to:

- Move resources such as adapters, communities, partners, mailboxes, routing channels, routing channel templates, and users from a Sterling Integrator instance to a Sterling File Gateway instance or from one Sterling File Gateway instance to another.
- Move resources from a test environment into a staging or production environment.

Export and Import Resources

If you want to use the same configurations of partners, communities, partner groups, routing channels, routing channel templates, or custom file layers in multiple Sterling File Gateway installations, you can create them in one installation, export them from there, and import them into other installations. This is useful for first creating a test system and then moving the successful configurations to a production system.

It is a good practice to fully implement Sterling File Gateway in a test environment. You can configure the required resources, test to confirm that everything is functioning as you require, and then move to a production environment. You may want to use a staging environment as another step in the process. Use the export and import capabilities to move any or all of the following:

- Communities
- Partners
- Partner groups
- Routing channels
- Routing channel templates
- Producer custom file layers
- Consumer custom file layers
- Adapters
- SSH keys
- PGP profiles
- Mailboxes
- Mailbox routing rule named FileGatewayRoutingRule

The following constraints apply to exporting:

- You can only export one community at a time and each goes into its own file. This is because each community is associated with a unique resource tag that is applied to every partner belonging to the community (and to all resources that belong to each partner). Partners cannot be exported individually. Partners are exported by exporting the community the partners belong to, which exports all partners in the community at once.
- Although you can export only one community at a time, you can update the community resource tag to associate related resources and then export the resource tag. This ensures that related resources are exported together and then imported as a single unit. When resources are exported and imported individually, there is a risk of incorrectly ordering the files on import, which could cause the import of resources to fail.
- When a Routing Channel is selected for export, the export file will also include the Routing Channel Template referenced by the Routing Channel.
- When a Routing Channel Template is selected for export, the export file will also include the Partner Groups, Producer Custom File Layers and Consumer Custom File Layers referenced by the Routing Channel Template.
- When Producer and Consumer Custom File Layers are selected for export, the associated container Producer and Consumer File Layer Translations are also included in the export file. Non-container Custom File Layer Translations are included in an export file when the Custom File Layers involved in the translation have been selected for export, including cases where the Translation involves a System File Layer.
- When a Routing Channel is imported, the referenced Routing Channel Template must either already exist on the target system or be included in the current import file. If the referenced Routing Channel Template already exists on the target system, it must have been created there using an export file taken from the same system as the Routing Channel. If two identically named Routing Channel Templates were independently created on the source and target systems, then Routing Channels referencing the Routing Channel Template cannot be exported and imported across the two systems.
- You can create partners in a test system and migrate them to a production system using Export and Import, or you can create partners directly in a production system. To avoid conflicts between systems, you should create partners in either the source or target system of Export/Import, not both.

To export and import resources:

1. To export and import from Sterling File Gateway, select **Tools** > **B2B Console** > **Deployment** > **Resource Manager** > **Resource Tags**.
2. Search for or select from the list the resource tag name (same as the community name). When selecting a large number of resources to associate with a resource tag, you may need to use the Tab key three times to view the **Finish** button.
3. Click **Edit** next to the Resource Tag.
4. Edit the community resource tag to add partner groups, routing channel templates, custom file layers, routing channels, business processes, maps, service configurations, SSH resources, and any other relevant resources.

5. Select from the following according to your needs:
   - Accounts (if created outside regular partner creation)
   - Service Configurations
   - Digital Certificates
   - SSH Resources
   - PGP Profiles
   - Perimeter Servers
   - Business Processes (if created for dynamic routing channel templates, custom file layers, or other extensibility)
   - Schedules
   - Mailboxes (if created outside regular partner creation or regular routing channel creation)
   - Maps (if created for extensibility)
6. Select **File Gateway Configurations** to access selections of the following:
   - Routing Channel Templates
   - Consumer Custom File Layers
   - Producer Custom File Layers
   - Partner Groups
   - Routing Channels

   Note: A partner group is the only File Gateway object that is updated upon import. All other File Gateway objects are not updated, regardless of the specification for the "Update Existing Object" value. To update any File Gateway object other than a group on the target system upon import, you must first delete it from target system.
7. Continue through the wizard, using the right and left arrows to select the components to include in the resource tag.
8. Click **Finish** to confirm the edits to the resource tag.

   Note: When selecting a large number of resources to associate with a resource tag, you may need to use the Tab key three times to view the **Finish** button.
9. From the Administration menu, select **Deployment** > **Resource Manager** > **Import/Export**.
10. Click **Go!** next to **Export Resources**.
11. Choose **XML Document** for the type of format.
12. Select **Yes** for tag name.
13. Choose the resource tag with the name of the community name you want to export from the list.
14. Select whether to export private certificates.
15. Click **Finish** to confirm the report. The export file is created. Examine the export report to confirm that there are no errors.
16. Save the export file to an accessible directory.
17. In the target system, import the resources by selecting **Tools** > **B2B Console** > **Deployment** > **Resource Manager** > **Import/Export**.

    When importing a community, a page is presented for each kind of resource in the export file. Choose all the objects for each kind of resource so all objects are imported. You cannot specify individual partners for

import; all the partners in the exported community are imported at once. Do not change the name of the resource tag. When importing routing rules, do not import any routing rules with a suffix of "_AFTRouter".

18. After importing, review the Import Report to verify a status of **Success** for each resource. Correct any conditions noted in the report that did not result in success.

Use Audit Records to Trace Administrative Actions

Audit records are helpful for proving that activities occurred at a stated time between partners. Audit records enable tracing creations and deletions to routing channel templates and routing channels. The records indicate when and what changed and who made the changes. By default, audit records are turned on. To view and use audit records:

1. Select **Tools** > **B2B Console** > **Admin** > **Operations** > **System** > **Support Tools** > **SQL Manager**.
2. Type the following:

```
select * from YFS_AUDIT
```

3. Click **Execute** to view all audit records.
4. Or, select the tables and columns you are interested in, for example:

```
select TABLE_NAME, OPERATION, AUDIT_XML, CREATETS,
CREATEUSERID, MODIFYTS, MODIFYUSERID from YFS_AUDIT where
TABLE_NAME = 'FG_ROUTCHAN_TMPL' or TABLE_NAME = 'FG_ROUTCHAN'
```

Set Up HTTPS for myFileGateway

To run *myFileGateway* inside your secure network, no configuration is required. An HTTP Server adapter configuration (named Http Server Adapter) comes with Sterling File Gateway that enables the clients on the same network as Sterling File Gateway to access *myFileGateway*.

To run *myFileGateway* in a DMZ, an HTTP Server adapter must be configured that uses a remote perimeter server.

After a Perimeter Server has been configured in Sterling Integrator, its name is available to the HTTP Server adapter configuration, in the Perimeter Server Name list on the HTTP Connection Properties page.

To configure *myFileGateway* to run in the DMZ:

1. Set up a perimeter server in the DMZ.
2. Configure a new Perimeter Server in Sterling Integrator.

   The port specified in the Perimeter Server configuration must *not* be the HTTP listen port (to which trading partners are expected to connect), which is specified in a subsequent stage.
3. Ensure that the remote perimeter server is running.
4. Create a new instance of the HTTP Server Adapter configuration.
   a) Log into Sterling File Gateway as a system administrator.
   b) Select **Tools** > **B2B Console**.
   c) From the Sterling Integrator Admin menu, select **Deployment** > **Services** > **Configuration**.

d) Under **Create**, next to **New Service**, click **Go!**
e) For **Service Type**, open the List View, select **HTTP Server Adapter** and click **Save**, then **Next**.
f) Give the adapter a new unique name and description. If you are using a clustered environment, from the **Environment** list, select the node where the remote perimeter server is to be assigned. Click **Next**.
g) For the **HTTP Listen Port**, specify the port that the Partner is expected to connect to. This port must not be used by a different application on the computer that the remote perimeter server is installed on. No two HTTP Server adapter configurations can listen on the same port on the same remote perimeter server computer. The default port for Sterling File Gateway is 33, so select a different port number.
h) From the **Perimeter Server Name** list, select the name of the Perimeter Server (previously configured) that corresponds to the specific remote perimeter server to be used. The name is in the format *node & name*, where name is what you specified.
i) For **Total Business Process queue depth threshold**, enter a number of business processes to allow in queue. The value of this setting has no effect if Sterling File Gateway is the only application hosted on this HTTP Server adapter, because Sterling File Gateway does not initiate business processes.
j) For **Document Storage** and **User Authentication Required**, you can accept the default or change to match your system.
k) For **Use SSL**, select **Must** to implement stronger security. Click **Next**. See *Implementing SSL* for more information about settings for the SSL Settings page. Click **Next**.
l) On the Services Configuration page, click **add**, type the URI /myfilegateway.
m) Select **War File**. Click **Next**.
n) **Enter the War File Path**. The *myFileGateway* War file is located at <*install dir*>\SI\container\Applications\myfilegateway.war. (For UNIX, <*install dir*>/container/Applications/myfilegateway.war.)
o) Click **Save**.
p) In the **Confirm** page, verify that all parameters are as specified.
q) Ensure the **Enable Service for Business Process** check box enabled.
r) Click **Finish**.

5. If you have access to the computer on which the remote perimeter server is running, log in to that computer and run the following command:

```
netstat -an | grep <httpListenPort>
```

where <*httpListenPort*> is the port previously specified. If a row is found that reads, LISTEN, the HTTP Server adapter is ready to handle requests from external clients.

6. Verify that the HTTP Server adapter is listening and that *myFileGateway* is configured correctly by pointing an HTTP browser to the following URL:

```
https://<host>:<httpListenPort>/myfilegateway
```

where <*host*> is the IP address or host name of the computer where the remote perimeter server is running and <*httpListenPort*> is the port previously specified. Set your browser options to select TLS 1.0 (in the Advanced tab). A dialog opens, requesting the user name and password to use with *myFileGateway*. If instead the browser encounters an error, verify that <*httpListenPort*> is being listened on. If it is listening, verify that some other application has not reserved this port. To do this, disable the HTTP Server adapter and verify that this port is not being listened on. If it is, find the application that has the port bound and shut it down. Alternately, select a different HTTP Listen Port and try again.

Note: If you have many concurrent users, you may find some degradation of performance. All HTTP server adapters in your Sterling Integrator installation share the setting for maximum number of threads. To increase

the maximum number of threads running at the same time, edit customer_overrides.properties to modify the following property:

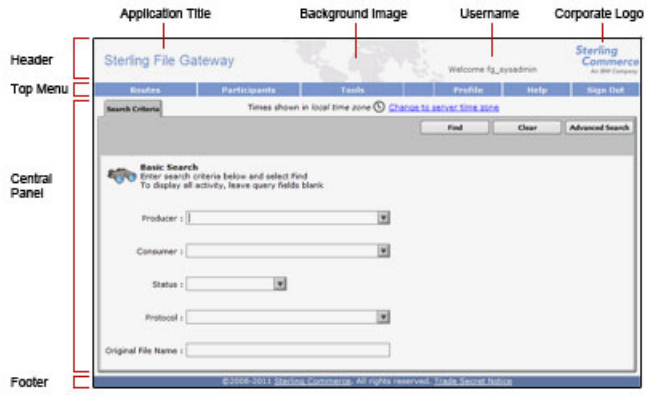
```
http.numOfmaxThread = X
```

where is *X* is the number of threads. The default value is 10. If your users are experiencing slow response when many concurrent connections have been made to the same port, increase this value to 50. Continue tuning this value until the system response is acceptable for the number of concurrent connections that must be supported. Setting this value to a value that is too high could be detrimental to system stability when too many concurrent connections are made.

Rebrand Sterling File Gateway and *myFileGateway*

You can rebrand Sterling File Gateway and *myFileGateway* to use your company's logo or other special content. To customize the look of Sterling File Gateway and *myFileGateway*, you create a skin, reference this new skin, and restart your system. You can use the same or different skins for Sterling File Gateway and *myFileGateway*.

The following figure shows the location of the portions of the screens you can rebrand:



The corresponding file names are:

- Header:
  - [skin]/brandingcontent/header.txt
  - [skin]/brandingcontent/myFgHeader.txt
  - [skin]/load_skin.js
  - [skin]/images/FGimages/brandingimages/...
- Top Menu: [skin]/skin_styles.css
- Central Panel:

- [skin]/skin_styles.css
- [skin]/load_skin.js
- [skin]/images/…

- Footer: [skin]/brandingcontent/footer.txt

Note: If you rebranded Sterling File Gateway in a previous version, you must make an additional change after you install Build 5006. Add the .menuBackground property to the custom skin .css file as in the following:

```
/* --- menu background color for main navigation bar;
default is #7896CF --- */
.menuBackground {
background-color: #7896CF;
}
```

To rebrand Sterling File Gateway:

1. Locate files in the following directories for the default skins:

   `<install_dir>/container/Applications/filegateway/isomorphic/skins/FileGateway`

   and

   `<install_dir>/container/Applications/myfilegateway/isomorphic/skins/FileGateway`

2. Copy and rename the “FileGateway” directory in path:
   `<install_dir>/container/Applications/filegateway/isomorphic/skins/FileGateway`

   You can use any valid directory name. In the next steps, the renamed directory is referred to as [skin].

3. To customize the header, you can change the following elements:

   - Application Title
   - Background Image
   - Corporate Logo
   - Position of the user name
   - HeaderALT

4. To change the Application Title:
   a) Open the following file:

      `[skin]/brandingcontent/header.txt`

   b) Change line 15 to refer to your company name (padding-left: 15px" nowrap="nowrap">My Company</td>)
   c) Open [skin]/brandingcontent/myFgHeader.txt
   d) Change line 15 to refer to your company name (or another name) (padding-left: 15px" nowrap="nowrap">My Company</td>)

5. To change the browser title text, which appears up in the top left-hand side of the browser (if different from Application Title, mentioned in the graphic, above) set the variables:

   - fgWindowTitle (for Sterling File Gateway)
   - myfgWindowTitle (for myFileGateway)

   in customer_overrides.properties as

   ```
   filegateway_ui.fgWindowTitle=xxx
   ```

and

```
filegateway_ui.myfgWindowTitle=xxx
```

6. To change the Background Image:
   a) Create a new Background Image GIF image, 66 pixels high by 800 pixels wide and named "MastheadBkgd_Map.gif"
   b) Place this GIF in the following directory:`[skin]/images/FGimages/brandingimages/`
   c) Open the following file: [skin]/brandingcontent/header.txt
   d) Change line 3 to refer to your skin's directory where the background image (from step 5) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ MastheadBkgd_Map.gif)
   e) Open [skin]/brandingcontent/myFgHeader.txt
   f) Change line 3 to refer to your skin's directory where the background image (from step 5a) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ MastheadBkgd_Map.gif)
7. To change the Corporate Logo:
   a) Create a new Corporate Logo GIF image, which should be 66 pixels high by 93 pixels wide and named "hdr_logo.gif"
   b) Place this GIF in the following directory:`[skin]/images/FGimages/brandingimages/`
   c) Open the following file: [skin]/brandingcontent/header.txt
   d) Change line 18 to refer to your skin's directory where the corporate logo image (from step 6a) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ hdr_logo.gif)
   e) Open [skin]/brandingcontent/myFgHeader.txt
   f) Change line 18 to refer to your skin's directory where the corporate logo image (from step 6a) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ hdr_logo.gif)
8. To change the position of the user name:
   a) Open the following file:`[skin]/load_skin.js`
   b) Change the two variables on Lines 14 and 15 to position the name label where you desire:
      • headerUserNameTop (expressed in absolute pixels from the top)
      • headerUserNameLeft (expressed as a percentage of page width, from the left side)
9. To change the headerALT, which is displayed while the header is loading:
   a) Open the following file:`[skin]/load_skin.js`
   b) Change the variable on Line 13 (headerALT) to your company name (e.g. "My Company").
10. To change the footer:
    a) Open the following file: `[skin]/brandingcontent/footer.txt`
    b) Modify the first line to refer to your company name as well as the link to your corporate Web site, if desired: …href='http://www.MyCompany.com' target ='_blank'>My Company…
11. To reference the new [skin], create or open customer_overrides.properties in a text editor. Add the following line:

```
filegateway_ui.fgSkinName=[skin]
```

where [skin] is your new skin name for Sterling File Gateway and

```
filegateway_ui.myfgSkinName=[skin]
```

where [skin] is your new skin name for myFileGateway. The values for [skin] can be different for Sterling File Gateway and myFileGateway.

12. To change the header only for myFileGateway:
    - Modify only the two files, header.txt and myFgHeader.txt in the new directory at:(<install_dir>/container/Applications/myfilegateway/isomorphic/skins/[skin]/brandingcontent

13. Run the following scripts:
    - <install_dir>/bin/hardstop.sh
    - <install_dir >/bin/deployer.sh
    - <install_dir >/bin/run.sh

14. Refresh your browser cache.

When you launch Sterling File Gateway, the new branding is shown in the header and footer. When your Partner users launch *myFileGateway*, the new branding is shown in the header.

Change Purge Settings

Sterling File Gateway activity is purged, not archived. Data that is purged is unrecoverable. Depending on your file transfer usage patterns, you may want to change the frequency in which Sterling File Gateway activity is purged. System Administrators can change the frequency for purging. Purging behavior is governed by the following settings in the visibility.properties file:

- lifespan_dataflow - length of time, in hours, before dataflow records are purged. Default is 336 hours (14 days).
- lifespan_adminaudit - length of time, in hours, before administrative change records, such as deleting a user are purged. Default is 336 hours (14 days). If a partner is deleted, the user who deleted it is recorded until the record is purged according to the value for the lifespan_adminaudit property.
- lifespan_session - length of time, in hours, before communication session records are purged. Default is 336 hours (14 days).

Note: To avoid conflicts, lifespan_dataflow and lifespan_session should be set to the same length of time.

Values for these settings are used in the schedule for the Purge Service. Changing either the settings or the schedule will result in a change in purge behavior for new activity records. Activity that has already occurred is governed by lifespan settings at the time they occurred.

Note: Changes made to this file affect the behavior of all tables in Sterling Integrator with a prefix of ACT_.

Once activity is purged, it is no longer available in the system and will not be found in a search that matches the criteria for it.

The tables in Sterling File Gateway that are purged are:

- FG_ARRIVEDFILE
- FG_ROUTE
- FG_DELIVERY
- FG_EVENT_ATTR
- FG_ROUTE_EVENT

To change settings for purge:

1. Open or create the following file:
   `<install_dir>/properties/customer_overrides.properties`
2. Add the following properties:
   `dmivisibility.lifespan_dataflow=Value`
   `dmivisibility.lifespan_adminaudit=Value`
   `dmivisibility.lifespan_session=Value`
   where Value is the number of hours before an item is purged.
3. Save the customer_overrides.properties file.
   See *Using Property Files*.
4. Restart Sterling File Gateway for the settings to take effect.

> **Purge Messages from Mailboxes**
>
> Messages in consumer mailboxes are not automatically purged, and over time could affect system performance. To avoid this, configure the Mailbox Scheduled Delete service to delete messages from one, many, or all mailboxes. You cannot replay or redeliver messages that have been purged. See *Mailbox Scheduled Delete Service*.

filegateway.properties

The filegateway.properties file contains properties which control the operation of Sterling File Gateway.

The following table describes properties in the filegateway.properties file:

Note: Do not edit the filegateway.properties file. Make all changes in the customer_overrides.properties file. For example, to change the pgpCmdline2svcname property, enter the following line into customer_overrides.properties:

```
filegateway.pgpCmdline2svcname=CUSTOM
```

substituting CUSTOM with the name of your Command Line 2 adapter. See *Using Property Files*.

Property	Description
ignoreFilenamex	Setting a regex pattern for this will cause any arrived file that matches your regex pattern to be ignored by Sterling File Gateway. This is useful for recognizing and ignoring temporary files sent by producers before they are renamed to the expected name. These will not be routed and are not considered failures. Specify one or more file name patterns to ignore in the following format: • filegateway.ignoreFilename1=<regex expression> • filegateway.ignoreFilename2=<regex expression> • filegateway.ignoreFilename3=<regex expression> • filegateway.ignoreFilenamex=<regex expression> For example: `filegateway.ignoreFilename1=.+[.]tmp$` would have the effect of ignoring all files with an extension of .tmp.

Property	Description
	Note: The regex pattern must match the file name in its entirety. Partial matches are not recognized.
ftpClientAdapterName	The FTP Client Adapter instance or service group that the FileGatewayDeliverFTP business process will use. Override this property in customer_overrides.properties if a custom FTP Client Adapter instance must be used to contact trading partners. You can also specify an adapter group name to load-balance outbound FTP sessions across multiple adapter instances. Default is: `ftpClientAdapterName=FTPClientAdapter`

bpCompletionProbes.1
bpCompletionSleepMsec.1
bpCompletionProbes.2
bpCompletionSleepMsec.2
	Timeouts and sleep intervals that control how long Sterling File Gateway waits for every sub-business process it invokes. These control the timeouts when a business process is executed synchronously during routing. Used for consumer identification business processes and for PGP processing. Enables one set of relatively quick probes followed by a second set of slower probes. The first set will be very reactive, but consume more processor. The second set will activate for longer-running processes and will consume less processor.
	First probe 120 times with 100 Milliseconds between, for a total of 12 seconds. Default is:
	`bpCompletionProbes.1=120 and bpCompletionSleepMsec.1=100`
	Then probe 600 times with 2000 Milliseconds between, for a total of 1200 seconds (20 minutes). Default is:
	`bpCompletionProbes.2=600 and bpCompletionSleepMsec.2=2000`

pgpCmdline2svcname	The name of the Command Line 2 adapter to be used for PGP packaging and unpackaging. Override this property in customer_overrides.properties if a custom Command Line 2 adapter must be used for PGP operations. You can also specify an adapter group name to load-balance outbound PGP sessions across multiple adapter instances. Default is: `pgpCmdline2svcname=PGPCmdlineService`
fgRoutePGPCmdLineSocketTimeout	Timeout value, in milliseconds, for PGP package and unpackage operations invoked by Sterling File Gateway. Default value is 240000 milliseconds (4 minutes)
fgRouteConcurrentSessionLimit	Limits the number of File Gateway services that can be running concurrently. The services are split into two groups, and each group has this value as a limit. Therefore, there will be a maximum of two times the value of this property services running. It is best to set this somewhat (but not too much) higher than the number of business process threads in queues 4 and 6 (these are the queues where the File Gateway Services run.) The default is 8. To change this value, use the customer_overrides.properties file to set: `filegateway.fgRouteConcurrentSessionLimit=(# of limit)`

Property	Description
required_si_build_ver	The build number (version) of Sterling Integrator that Sterling File Gateway requires. This is checked at system start up. If the current version of Sterling Integrator does not equal the required_si_build_ver, a warning is issued and the system is shut down. Required. Do not change or override this property.
fgOnboardingDefaultUserGroupId	The group partner users are automatically assigned to when they are created as a result of creating a partner in Sterling File Gateway, migrated from AFT, or the partner's identity is associated with a File Gateway partner group. Required. Default is File Gateway Partners Users Group.
userIdMinLength	Minimum number of characters in the user ID. The default is 5. To enable shorter or require longer User IDs, modify the following property in customer_overrides.properties: `userIdMinLength.ui=(# of characters)` The value of # of characters must be greater than zero. To implement single sign-on, this value must match the value set in Sterling Integrator.
FGConsecFailedAttempts	Number of consecutive failed login attempts that are allowed before a user is locked out of the application. Default is 0, which means users are never locked out.
FGLockInterval	Length of time, in minutes, that the lock is applied after the number of failed login attempts is exceeded. Default is 30.

filegateway_ui.properties

The filegateway_ui.properties file contains properties which control the location of the Help systems for Sterling File Gateway and *myFileGateway*, as well as several other user interface settings.

The following table describes properties in the filegateway_ui.properties file:

Note: Do not edit the filegateway_ui.properties file. Make all changes in the customer_overrides.properties file. For example, to change the URL for the Help system, enter the following line into customer_overrides.properties:

```
filegateway_ui.help.uri=http://CUSTOM
```

substituting CUSTOM with your preferred URL.

Property	Description
reportingdirectory	Location of the reports templates. Default - reportingdirectory=&INSTALL_DIR/reporting Required. Do not modify or override.
help.uri	Specifies the URL for the Help used by Sterling File Gateway. Required. The default is: `http://help.sterlingcommerce.com/SFG20/index.jsp` This site is hosted by IBM.

Property	Description
myFghelp.uri	Specifies the URL for the help used by *myFileGateway*. Required. The default is: `http://help.sterlingcommerce.com/mySFG20/index.jsp` This site is hosted by IBM.
notification.partner.url	Login URL for partner users to access *myFileGateway*. Required. The default is: `notification.partner.url=http://&HOST_ADDR;:&PORT1;/myfilegateway` **Note:** The specified URL will be included in email messages generated to partner users. If you implement Sterling Secure Proxy (SSP), it is imperative that you change this property to remove the original server details and replace with the SSP-designated URL.
notification.admin.url	Login URL for administrative users to access Sterling File Gateway. Required. The default is: `notification.admin.url=http://&HOST_ADDR;:&PORT1 /filegateway` **Note:** The specified URL will be included in email messages generated to administrative users.
fgMaxRoutingChannelRecords	Limits the total number of routing channel records returned by a search. Required. Default is 1000. You can change this to fine tune performance by editing the customer_overrides.properties file.
myFgStoragetype	Storage type to use for new documents sent through myFileGateway. Possible values are: • default - use the system default • db - store documents in database • file - store documents in file system The default is default. To change this value, use the customer_overrides.properties file. For example to set it to database: `filegateway_ui.myFgStoragetype=db`
fgMaxActivityRecords	Limits the total number of Activity Records that will be returned in activity search. This can be edited to fine tune performance. The default is: `fgMaxActivityRecords=1000`
fgWindowTitle	The title of the window that displays in the top browser bar for Sterling File Gateway. Required. Default is Welcome to Sterling File Gateway.
myfgWindowTitle	The title of the window that displays in the top browser bar for *myFileGateway*. Default is Welcome to Sterling File Gateway.
fgSkinName	The file that contains the branding information for Sterling File Gateway. Required. Default is FileGateway.
myfgSkinName	The file that contains the branding information for *myFileGateway*. Required. Default is FileGateway.

Property	Description
fgOnboardingDefaultSessionTimeout	The default session timeout in minutes for a Partner User created using the Sterling File Gateway onboarding. The default is: `fgOnboardingDefaultSessionTimeoutInMinutes=15`
fgOnboardingDefaultUserGroupId	The group partner users are automatically assigned to when they are created as a result of creating a partner in Sterling File Gateway, migrated from AFT, or the partner's identity is associated with a File Gateway partner group. Required. Default is File Gateway Partners Users Group.
FGConsecFailedAttempts	Number of consecutive failed login attempts that are allowed before a user is locked out of the application. Default is 0, which means users are never locked out.
FGLockInterval	Length of time, in minutes, that the lock is applied after the number of failed login atttempts, FGConsecFailedAttempts, is exceeded. Default is 30.

About Event Codes

Each activity during the progress of a file transfer generates an event code. These codes are displayed in the activity details to enable Partners and Operators to see the progress and navigate to more details. System Administrators can create custom event codes and modify the permissions for standard event codes.

Some event codes trigger notifications to subscribers. System Administrators can change the permissions for an event code by using the customer_overrides.properties file to override values in the FGEventCodes.properties file. The default subscription settings are provided in the table below:

Event Code	Name	Description	Default Subscription Settings
FG_0050	MailboxAuthorizationFailure	When a user fails to access a mailbox that is monitored	Operators
FG_0201	BusinessProcessStarting	When a business process is started, with the reason for starting it stored in context.	Only in activity details.
FG_0202	BusinessProcessSuccess	When a business process is successfully completed, with a link to the business process.	Only in activity details.
FG_0203	SendMessageBusinessProcessStarted	When a business process is successfully started, with a link to the business process.	Only in activity details.
FG_0250	BusinessProcessFailure	When a business process fails, with a link to the business process	Operators
FG_0401	FactDiscovery	When a fact is discovered by the route, for example, matching a pattern on the file name.	Only in activity details.
FG_0404	ProducerFound	When a producer and user are identified based on the arrived file.	Only in activity details.
FG_0407	ConsumerFound	When a consumer is identified based on the route plan.	Only in activity details.

Event Code	Name	Description	Default Subscription Settings
FG_0408	ArrivedFileStarted	When a file arrives to be routed	Operators, producers, and consumers
FG_0409	ArrivedFileDeterminingRoutes	When an arrived file starts determining routes.	Only in activity details.
FG_0410	ArrivedFileRouting	When an arrived file starts processing routes.	Only in activity details.
FG_0411	ArrivedFileRouted	When an arrived file completes all its routes	Operators, producers, and consumers
FG_0412	RouteStarted	When a route is started from an arrived file.	Only in activity details.
FG_0413	RouteDeterminingDeliveries	When a route starts determining deliveries.	Only in activity details.
FG_0414	RouteDelivering	When a route starts processing deliveries.	Only in activity details.
FG_0415	RouteComplete	When a route completes all its deliveries	Operators, producers, and consumers
FG_0416	DeliveryStarted	When a delivery is started from a route.	Only in activity details.
FG_0417	DeliveryTransforming	When a delivery starts to transform the consumer file.	Only in activity details.
FG_0418	DeliveryDelivering	When a delivery starts delivering the consumer file to the consumer.	Only in activity details.
FG_0419	DeliveryComplete	When a delivery is complete	Operators, producers, and consumers
FG_0420	ArrivedFileReplayed	When an arrived file is replayed, with a link to the replay	Operators, producers, and consumers
FG_0421	ArrivedFileReplayOf	When an arrived file is a replay of an original arrived file, with a link to the original file.	Only in activity details.
FG_0422	Redeliver	When a redelivery is requested by a user	Operators, producers, and consumers
FG_0423	DeliverRedelivering	When a delivery starts redelivering the consumer file to the consumer.	Only in activity details.
FG_0424	ArrivedFileIgnored	When an arrived file is ignored due to a configured pattern for ignoring files	Operators, producers
FG_0425	ArrivedFileDescription	The description of the Arrived File	Operators, producers
FG_0450	ProducerMessageNotFound	When a producer message is invalid or cannot be found	Operators, producers
FG_0451	ProducerDocumentNotFound	When a producer document is invalid or cannot be found	Operators, producers
FG_0455	ArrivedFileFailed	When an arrived file fails	Operators, producers
FG_0456	RouteFailed	When a route file fails	Operators, producers, and consumers
FG_0457	DeliveryFailed	When a delivery fails	Operators, producers, and consumers

Event Code	Name	Description	Default Subscription Settings
FG_0458	FileGatewayServiceVersionMismatch	When a newer version of a system business process is installed, but is not the default chosen version.	Operators
FG_0501	ProducerMailboxRouteCandidatesFound	When route candidates are found for an arrived file based on the producer and the mailbox of the message.	Only in activity details.
FG_0502	RouteCandidatesFound	When route plan candidates are found for an arrived file.	Only in activity details.
FG_0503	RouteCandidate	A route plan candidate for an arrived file.	Only in activity details.
FG_0504	Route	When one or more routes are chosen from the candidates.	Only in activity details.
FG_0505	RoutesFound	The number of routes that will be executed.	Only in activity details.
FG_0506	Route Candidate Does Not Match	When a routing channel template contains no matching producer file structure for an arrived file.	Only in activity details.
FG_0550	ZeroRouteCandidatesFound	When no route candidates are found for an arrived file	Operators, producers
FG_0551	ZeroRouteChannelsFound	When no route channels are chosen from the list of candidates for an arrived file	Operators, producers
FG_0552	InvalidRoute	When a route is invalid	Operators, producers
FG_0601	TransformedMessage	When a message is transformed to the final format for the consumer.	Only in activity details.
FG_0602	ProducerPayloadExtracting	When the router begins to extract a producer payload file.	Only in activity details.
FG_0603	ConsumerPayloadConstructing	When the router begins to construct a consumer payload file for delivery.	Only in activity details.
FG_0604	ConstructedLayer	When a single layer in the consumer payload file gets constructed.	Only in activity details.
FG_0605	ExtractedLayer	When a single layer in the producer payload file gets extracted.	Only in activity details.
FG_0606	LayerOptions	When options are passed to a business process to process a layer.	Only in activity details.
FG_0607	PGPConstructSkipped	When the PGP Construct layer is skipped because the consumer does not handle PGP and it is optional on the Routing Channel Template	Operators, consumers
FG_0650	ExtractLayerFailed	When extraction of a layer fails	Operators, producers
FG_0651	ConstructLayerFailed	When construction of a layer fails	Operators, consumers
FG_0701	DeliveredMailboxMessage	When a message is delivered to a mailbox (either a consumer mailbox or a mailbox for sending to a listening consumer).	Only in activity details.
FG_0702	DeliveredListeningPartnerMessage	When the file transfer is complete.	Only in activity details.
FG_0703	ChangeDirectory	When the supported protocol changes directory on the listening consumer's server to transfer the file.	Only in activity details.

Event Code	Name	Description	Default Subscription Settings
FG_0704	ConsumerDestinationMailboxFound	When the destination mailbox for the consumer is discovered.	Only in activity details.

filegateway_eventcodes.properties

The filegateway_eventcodes.properties file contains properties that control the operation of event codes in Sterling File Gateway.

There are multiple properties in the filegateway_eventcodes.properties file for each event, in the format:

```
FG_<EVENT_CATEGORY><EVENT_CODE>.<PROPERTY_NAME>=<REPLACEABLE_TEXT>
```

where:

• <PROPERTY_NAME>is the parameter being defined for the particular event
• <REPLACEABLE_TEXT> is the value of the parameter for the particular event
• and the values used by Sterling File Gateway for <EVENT_CATEGORY> are:

Code	Category
00	Producer File Transfer
02	Routing Business Process
04	File Gateway General
05	Route Plan Determination
06	File Transformation
07	Consumer File Transfer

<EVENT_CODE> is a unique code (within the category) to identify this event. Check the other properties (or the FileGatewayEvent enumeration) to ensure no duplication.

<REPLACEABLE_TEXT> is text that displayed in the route details so users can monitor progress of the route.

The following information is provideded for each event:

Property	Description	Example
Name	Name of the event. Displayed in the subscription UI (**Profile** > **Notifications**). Required.	XX_0050.name=MyCustomEventFailure
Attributes	Comma delimited list of named attributes to the event. Used in the text field and must correspond to the order listed in the text field. For example, UserId attribute corresponds to {0} below. All attributes need not appear in the text field. Required, but can be empty.	XX_0050.attributes=UserId,ErrorMessage

Property	Description	Example
Text	Event description displayed in the route activity UI for a specific occurrence of this event. Required.	XX_0050.text=User {0} encountered failure {1}
Description	A generic event description that does not use attributes. Displayed in the subscription UI (**Profile** > **Notifications**). Required.	XX_0050.description=When a user encounters this custom event failure
Permissions	Comma delimited list that indicates who can be notified and who can view this event. Possible values are: • subscription - available for subscription to notifications • producer - producers can see in route activity events list and receive notifications • consumer - consumers can see in route activity events list and receive notifications Optional.	XX_0050.permissions=subscription

filegateway_eventcodes.properties includes only standard events shipped with Sterling File Gateway. Custom events you create are entered and configured in customer_overrides.properties.

Note: Do not edit the filegateway_eventcodes.properties file. Make all changes in the customer_overrides.properties file. For example, to change the name property, enter the following line into customer_overrides.properties:

```
filegatewayeventcodes.name=CUSTOM
```

substituting CUSTOM with the name of your event code. See *Add Custom Event Codes*.

Get Started

Prepare Communications Adapters for Use with Sterling File Gateway

Sterling File Gateway uses the communications adapters in Sterling Integrator to receive connections from and make connections to Partners for the purpose of transferring files. These connections can use various Internet protocols, including FTP, FTPS, SFTP, SCP, Connect:Direct, HTTP, HTTPS, and WebDAV. Before using Sterling File Gateway to route files, configure the communications adapters in Sterling Integrator.

To configure communications adapters:

1. Determine the communication adapters you require.
2. Review the information needed to configure the adapters you require.

   The following adapters can be used with Sterling File Gateway:

Protocol	Adapter
FTP, FTPS	FTP Server adapter
FTP, FTPS	FTP Client adapter and services
SSH/SFTP, SSH/SCP	SFTP Server adapter
SSH/SFTP	SFTP Client adapter and services
Connect:Direct	Connect:Direct Server adapter
PGP	Command Line Adapter 2
HTTP, HTTPS, WebDAV (Requires extensibility. See *Add Custom Protocols*.)	HTTP Server adapter
HTTP, HTTPS, WebDAV (Requires extensibility. See *Add Custom Protocols*.)	HTTP Client adapter and services

3. Gather the information needed for the adapters.
4. From the main menu, select **Tools** > **B2B Console**.
5. Select **Deployment** > **Services** > **Configuration**.
6. Select and configure the adapters you require.

Sterling File Gateway System Business Processes

There are several business processes delivered with Sterling File Gateway to perform basic tasks. Do not alter these business processes.

In Sterling Integrator, a business process is a series of linked software and possibly human activities that accomplishes a business goal. The activities in a business process are primarily performed by components known as services and adapters, and are orchestrated by Sterling Integrator integration engine.

The integration engine runs business processes according to the instructions that comprise your business process models. Technically, a business process model is defined by a single, unique BPML document, a .BPML file. BPML is an XML-based language used to describe (model) and run business processes.

The following table contains a list of the system business processes used for Sterling File Gateway operations:

System Business Process	Function
FileGatewayDeliverFTP	Delivers files to consumers using the FTP protocol.
FileGatewayMailboxRoute	Gathers all mailbox messages available for routing.
FileGatewayMailboxRouteArrivedFile	Routes individual messages identified by FileGatewayMailboxRoute as available for routing.
FileGatewayRoutePGPPackageDocument	Routes PGP packaged documents.
FileGatewayRoutePGPUnpackageDocument	Routes PGP unpackaged documents.
FileGatewaySendMessage	Sends messages from File Gateway.

Set Up and View Logs

To troubleshoot problems with file transfers that cannot be analyzed using the Sterling File Gateway user interface, view the activity log. Only Operators and System Administrators can edit log settings and view logs.

New log files are created at midnight each day. If the maximum log file size is exceeded during the same day, additional log files are created. Old logs are automatically deleted after the pre-determined maximum number of logs is reached. The default maximum number is ten, which can be changed in the customer_overrides.properties file (logService.filegatewaylogger.maxnumlogs=10)

To set up logging:

1. From the main menu, select **Tools** > **Logs**.
2. Scroll down to locate **File Gateway**.
3. Click on the **edit** icon next to **File Gateway**.
4. Select **Logging Level On**.

   Note: Logging can affect performance, so should only be turned on while troubleshooting problems.

5. Click **Save**.
6. View the log at **Tools** > **Logs**, **File Gateway**.

Prepare to Use the Connect:Direct Protocol

Prior to creating partners to use the Connect:Direct protocol for file transfer, you must:

1. Create a node by selecting **B2B Console** > **Deployment** > **Adapter Utilities** > **C:D Netmaps** > **C:D Nodes**.
2. Create a netmap by selecting **B2B Console** > **Deployment** > **Adapter Utilities** > **C:D Netmaps** > **C:D Netmaps**.
3. Create a cross-reference between the node and netmap by selecting **B2B Console** > **Deployment** > **Adapter Utilities** > **C:D Netmaps** > **C:D Netmap X-REF**.
4. Set up the Connect:Direct Server adapter.
5. Select the netmap you created in the Connect:Direct Server adapter configuration. For consumers, the Connect:Direct node that the Partner hosts is the SNODE.
6. Proceed with creating partners. When you onboard a listening consumer, specify the netmap information for the Connect:Direct specific parameters.

Prepare to Use PGP

PGP encryption is supported by Sterling File Gateway, in combination with FTP and other protocols.

For producers sending PGP packaged files, files are processed in accordance with the routing channels and their templates when a partner is the producer for the channel. Encrypted files will be decrypted using the router's secret PGP key and signed files will be verified using the producer's public key if it is present in the Public Key Ring.

For consumers, you specify in the Create Partner wizard that messages sent to the consumer must be encrypted, signed, or both. The PGP options of compression, text mode and ASCII armor can also be specified for each consumer.

The settings for the producer are independent of the settings for the consumers. If the producer is set to Encryption, regardless of whether the consumer is or is not, only encrypted files can be sent by the producer. If the producer is set to No Encryption, and the consumer is set to Encryption, unencrypted files are sent by the producer and the Router encrypts them before sending to the consumer.

Producers may unilaterally (without prior negotiation) choose to use PGP compression for their files. Consumers may be configured such that Sterling File Gateway also performs compression while it is packaging the PGP file before sending to them.

Prior to creating a community with partners to use PGP, you must do the following:

1. Install one of the supported PGP vendor’s products.
2. Start a <install_dir>/client/cmdline2/CLA2Client.jar process on the machine that the PGP vendor's product runs on.
3. Edit the PGPCmdlineService (which is a configuration of the Command Line 2 adapter) in Sterling Integrator, or create a new configuration of the Command Line 2 adapter. Set the following parameters:
   - Remote Name - IP address or machine name for the machine where the PGP server is running
   - Remote Port - the port number on the PGP server machine that the CLA2Client.jar is listening on
   - Working directory (optional)

4. If you create a new configuration of the Command Line 2 adapter, edit the customer_overrides.properties file to override the default setting for the pgpCmdline2svcname parameter in the filegateway.properties file to point to the new configuration.
5. Create a PGP profile in Sterling Integrator. Name the profile AFTPGPProfile. The Sterling File Gateway Router can only work with a profile that has this name and cannot use any other PGP profiles defined in Sterling Integrator.

Prepare to Use SSH/SFTP

Prior to creating a community with Partners to use the SSH/SFTP or SSH/SCP protocol for file transfer, you must:

1. For an SFTP listening consumer, you must first create their remote profile. Select **Trading Partner** > **SSH** > **Remote Profile**. Assign this SSH remote profile when you create a listening consumer Partner.
2. For an SSH/SFTP or SSH/SCP producer or initiating consumer an Authorized User Key may be required of them before they can connect. This key can be imported before configuration and selected when creating the Partner or imported during the Partner creation.
3. The SFTP Server adapter cannot be enabled until an SSH Host Identity Key is created or imported. Select **Deployment** > **SSH Host Identity Key**. This key must be assigned before the adapter is enabled.
4. Configure the SFTP Server adapter.

Exchange Information with Partners

For the FTP, FTPS, and Mailbox protocols, the user name and password, established during the Partner creation, is sufficient to begin exchanging files. For other protocols, additional steps are necessary as follows:

1. The specific details for how a Partner must configure their system, such as the host IP address, port number, certificates, and other specifics, must be communicated to the partners outside of Sterling File Gateway, such as by e-mail.
2. If a particular protocol requires extra parameters specific to the Partner, such as SFTP requiring user keys, set these up in the Sterling Integrator Administration menu after creating the partner.

Note: SFTP Authorized User Key can be added before or during Partner creation. Remote profiles must be added before an SFTP listening consumer can be created. These profiles contain a Known Host Key and the User Identity Key. The SSH Host Identify Key (public and private keys) is created or imported before Partner creation. The public part of this key may be exported and can become a Known Host Key for a Remote Profile for a remote server.

Authentication Outside Sterling File Gateway

About Authenticating Users Outside Sterling File Gateway

There are two supported methods of authenticating users outside Sterling File Gateway and Sterling Integrator:

- Single Sign-On (SSO) - a method of access control that enables a user to log in once to a company network or portal site to gain access to multiple software systems without logging in again. SSO bypasses the built-in authentication process in Sterling File Gateway and instead trusts that a user has been authenticated by a third-party software.
- Lightweight Directory Access Protocol (LDAP) - a network protocol for accessing directories where user credentials are authenticated against an external LDAP directory instead of against the Sterling Integrator database user table for access to Sterling File Gateway.

Implementing Single Sign-On in Sterling File Gateway

Single Sign-On (SSO) in Sterling File Gateway requires authentication using a third-party external Access Management System (AMS).

To enable SSO:

1. Configure an external Access Management System (AMS) to access a repository for user information.
2. For each AMS user who requires access to Sterling File Gateway, create an account in your AMS.
3. For each AMS user who requires access to Sterling File Gateway, create an external user account in Sterling Integrator that matches the AMS account created in step 2. For users created using Sterling File Gateway partner onboarding, edit the user account in the B2B Console (**Accounts** > **User Accounts**) to specify the user as an external user.

   Note: Users who are set up as external users cannot view the Change Password page in Sterling File Gateway (**Profile** > **Password**).

4. For third-party software integration, you must provide a custom plug-in that enables Sterling File Gateway to interface with the third-party software. Specify the name of this Java class plug-in:

   ```
   SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.fg.security.SSOProviderFilegatewayDefault
   ```

replacing `com.sterlingcommerce.fg.security.SSOProviderFilegatewayDefault` with the name of your repository.

See *Using Single Sign-On*.

5. Create or modify the customer_overrides.properties file to modify the authentication_policy.properties. Enable SSO by setting the property:

```
authentication_policy.SSO_AUTHENTICATION_ENABLED=true
```

Note: Do not edit the authentication_policy.properties file. Make all changes in the customer_overrides.properties file. See *Using Property Files*.

6. In the customer_overrides.properties file, configure a custom log out page to specify where the user is taken when Log Out is selected. For example:

```
security.SSO_FORWARD_URL.FILEGATEWAY.LOGOUT=http://www.google.com/search?q=logout
security.SSO_FORWARD_URL.MYFILEGATEWAY.LOGOUT=http://www.google.com/search?q=logout
```

7. In the customer_overrides.properties file, configure a custom time out page to specify where the user is taken when the session times out. For example:

```
security.SSO_FORWARD_URL.FILEGATEWAY.TIMEOUT=http://www.google.com/search?q=timeout
security.SSO_FORWARD_URL.MYFILEGATEWAY.TIMEOUT=http://www.google.com?q=timeout
```

8. In the customer_overrides.properties file, specify the HTTP Header name that will contain the user name being passed into Sterling File Gateway by editing the value:

```
## http header variable that contains externally authenticated
userid
authentication_policy.SSO_USER_HEADER=SM_USER
```

9. Configure the AMS to pass in the user name of the external user created in Sterling Integrator using an HTTP Header. Refer to the third-party software documentation for how to do this.

When a user that has previously been authenticated by the AMS requests access to Sterling File Gateway or *myFileGateway*, the user bypasses the login page, and is taken to the home page respective of that user's role. For example, a user belonging to the fg_architect group is taken directly the Routing Channel Template page, and a fg_operator user is taken to the Route Activity Page.

Implementing Lightweight Directory Access Protocol (LDAP) in Sterling File Gateway

Sterling File Gateway can be configured to authenticate user credentials against an LDAP directory.

To configure Sterling File Gateway for LDAP:

1. Create external users in Sterling Integrator.
2. For each external user created in Sterling Integrator, create a matching record in an LDAP Directory.

3. Create or modify the customer_overrides.properties file to modify the authentication_policy.properties. as in the following example:

```
authentication_policy.LDAP_AUTHENTICATION_ENABLED=true
 ############################################################
# LDAP Server <1> Authentication Configuration
############################################################
#
authentication_policy.authentication_1.className=
com.sterlingcommerce.SERVER!.security.LDAPAuthentication
 authentication_policy.authentication_1.display_name
=OPenLDAP Server localhost
## enable ldap authentication (true, false)
default=false
 authentication_policy.authentication_1.enabled=true
## jndi parameters for ldap
connections
authentication_policy.authentication_1.jndi_factory=
com.sun.jndi.ldap.LdapCtxFactory
authentication_policy.authentication_1.server=localhost
authentication_policy.authentication_1.port=XXX
authentication_policy.authentication_1.security_type=
simple
authentication_policy.authentication_1.principle=
cn=Manager,dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_1.credentials=
secret
## comment out or leave as blank on this property if
the server is not going to use SSL for the security
protocol.
#authentication_<number>.security_protocol=ssl
## search parameters for user password
authentication_policy.authentication_1.password_attribute
=userPassword
 authentication_policy.authentication_1.search_root=
dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_1.search_filter=
(uid=<userid>)
 authentication_policy.authentication_1.with_user_bind=
false
```

where authentication_1 is your first LDAP server. To use multiple LDAP servers, copy the lines for authentication_1 and modify them for the properties for authentication_2. Continue for as many servers as you want to set up.

Note: Do not edit the authentication_policy.properties file. Make all changes in the customer_overrides.properties file. See *Using Property Files*.

---

4. If you previously set up LDAP in Sterling Integrator by editing your security.properties file, comment out LDAP settings as follows:

```
#LDAP_AUTHENTICATION_ENABLED=true
#LDAP_JNDI_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#LDAP_HOST=ldap://ldapserver1.local:9999
#LDAP_SECURITY_TYPE=simple
```

```
#LDAP_PRINCIPLE=cn=Manager,dc=amr,dc=stercomm,dc=com
#LDAP_CREDENTIALS=SterlingCustomer
#LDAP_USER_PASSWORD_ATTRIBUTE=userPassword
#LDAP_SEARCH_ROOT=dc=amr,dc=stercomm,dc=com
#LDAP_SEARCH_FILTER_PATTERN=(uid=<userid>)
#LDAP_AUTHENTICATE_WITH_USER_BIND=false
##LDAP_SECURITY_PROTOCOL=ssl
#LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/server2/com/sterlingcommerce/
server2/security/units/cacerts
#LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
#LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/server2/com/sterlingcommerce/
server2/security/units/keystore
#LDAP_SECURITY_KEYSTORE_PASSWORD=password
```

The setting in authentication_policy overrides the previous setting in security.properties.

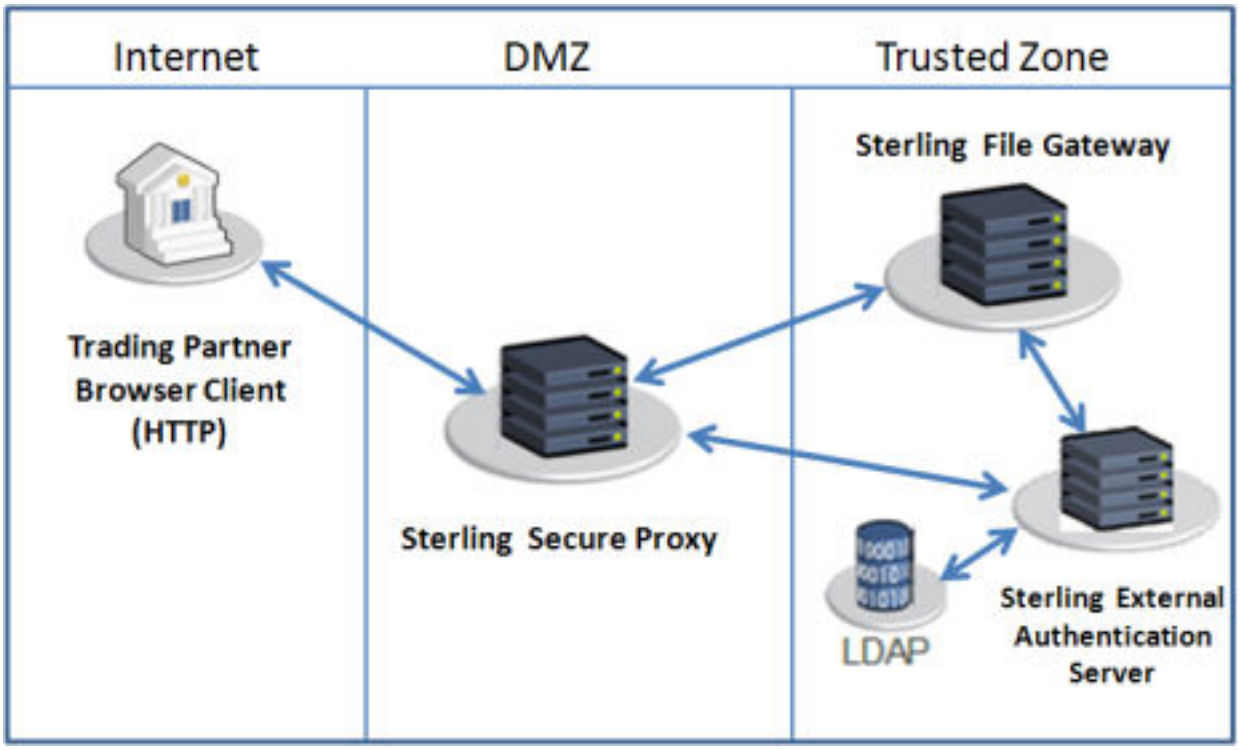
5. Restart the server for your changes to in the customer_overrides.properties file to take effect over the authentication_policy.properties file.
6. See *Using LDAP* for details about the Sterling Integrator implementation.

Configure Sterling Secure Proxy

Sterling Secure Proxycan be used as a proxy with Sterling File Gateway and other HTTP applications and supports a single sign-on connection. Single sign-on (SSO) provides access control that allows a user to log in once toSterling Secure Proxy, using the HTTP protocol, and then gain access to Sterling File Gateway without logging in again. SSO bypasses normal user authentication in Sterling File Gateway and trusts thatSterling Secure Proxy has authenticated the user.

After you set up the basic single sign-on configuration, trading partners can communicate in a secure environment that provides authentication. The trading partner first connects toSterling Secure Proxy which then connects to Sterling File Gateway on behalf of the trading partner.

Following is an illustration of the flow of data:



If you are using a load balancer to run multipleSterling Secure Proxy engines, avoid login credential errors or session timeout conditions by configuring the load balancer to use "sticky sessions" (also known as persistence, server affinity, or "sticky cookies"). Refer to your load balancer documentation for details about configuring persistence.

For more information, see the *Sterling Secure Proxy* documentation at *http://www.ibm.com/support/docview.wss?uid=swg27023891*.

Extend the Capabilities

Extend the Capabilities of Sterling File Gateway

You can customize Sterling File Gateway to support additional functionality in the following areas:

- Protocols
- Consumer identification policies
- Event codes

Add Custom Protocols

You can add support for custom protocols for listening consumers in addition to the ones preconfigured in Sterling File Gateway.

The information you provide in performing this procedure determines the text displayed in the Partner management wizard. That is, after you perform this procedure, new choices are available for protocols offered by Sterling File Gateway when creating a community and when creating a listening consumer in a community that is configured for the custom protocol.

1. Write a business process that implements the custom protocol. The business process name must be unique for each custom protocol. Do not use an underscore character (_) in the name of the business process.
2. Use the existing AFTExtensions.xml as a guide to create an AFTExtensionsCustomer.xml file to describe the protocol. Do not edit the AFTExtensions.xml file.

   The AFTExtensions.xml file is located in the following directory:`<install_dir>/container/Applications/aft/WEB-INF/classes/resources/xml`.
3. Save the AFTExtensionsCustomer.xml file to the same directory as AFTExtensions.xml.
4. Use the existing AFTExtensions.properties file as a guide to create the AFTExtensionsCustomer.properties file. Do not edit the AFTExtensions.properties file. The AFTExtensions.properties is located in the following directory:

   `<install_dir>/container/Applications/aft/WEB-INF/classes/resources`

   Note: The user interface elements to describe the protocol are specified in the htmlType parameter. Valid values are text, password, select. When "select" is chosen for htmlType, the UI presents a list whose contents

are derived from an "options" class. An example of an "options" class list is in the AFTExtensions.xml file (the text starts with "<OPTION name="SSHRemoteProfiles" class= ")

5. Save the AFTExtensionsCustomer.properties file to the same directory as AFTExtensions.properties, namely:

   `<install_dir>/container/Applications/aft/WEB-INF/classes/resources`

6. Reference the business process you created in step 1 in a new AFTExtension element in the AFTExtensionsCustomer.xml file.
7. Stop Sterling File Gateway.
8. Run <*install_dir*>/bin/setupfiles.sh.
9. Run <*install_dir*>/bin/deployer.sh.
10. Start Sterling File Gateway.

    The additional protocol will be available when adding and editing communities. After this protocol has been chosen for a community, it then becomes available when creating and editing partners in that community.

Example Custom Protocols

ProcessData for Business Processes Implementing Custom Protocols

The following elements are available in ProcessData when the business process implementing an custom protocol is executed:

Element	Description
Primary document	The primary document contains the data as it will be delivered to the consumer, so that, if the producer's document required PGP operations (such as decryption) or the consumer required PGP processing, the contents of the primary document contains the results of performing those PGP operations.
PrimaryDocumentId	Document ID for the primary document
DestinationMessageName	Name of the primary document
TransportBP	Name of the business process that will be executed for the protocol
AFTRouteId	An internal identifier needed if the AFT Route Progress Event Reporting service is called. The value of this element must not be changed by the extensibility business process.
AFTRouteWorkFlowId	An internal work flow identifier needed if the AFT Route Progress Event Reporting service is called. The value of this element must not be changed by the extensibility business process.
ProducerName	Name of the data producer
ConsumerName	Name of the data consumer

Element	Description
Parameters added to AFTExtensionsCustomer.xml	Any parameters you supply as part of your custom protocol are available in process data.

Example Adding an Connect:Enterprise UNIX Extension

For example, if you were adding Connect:Enterprise UNIX as a outbound file transfer mechanism, your business process could be the following:

```
<process name="AFTRouteViaCEU">
<sequence>
 <operation name="CEU Add Service">
  <participant name="CEUServerAdd"/>
  <output message="AddRequest">
   <assign to="." from="*"/>
   <assign to="CEUServerAdapterInstanceName"
    from="string(CEUServerAdapterInstanceName)"/>
   <assign to="CEUMailboxId" from="string(CEUMailboxId)"/>
  </output>
  <input message="inmsg">
   <assign to="CEUAddServiceResults" from="*"/>
  </input>
  </operation>
</sequence>
</process>
```

Note: ProcessData does not include the producer name or consumer name for custom protocol business processes.

AFTExtensionsCustomer.xml Adding Connect:Enterprise UNIX

The following is an example AFTExtensionsCustomer.xml adding Connect:Enterprise UNIX for outbound file transfer:

```
<AFTExtensions>
 <AFTExtension name="ceu-protocol" type="consumer-delivery-protocol"
 label="cdp.protocol.label.ceuprotocol" bp="AFTRouteViaCEU">
  <GROUP title="ceu.instance.group1.title">
  <VARDEF varname="CEUServerAdapterInstanceName" type="String" htmlType="text"
   validator="ALPHANUMERIC" size="30" maxsize="250"
   label="cdp.label.ceuprotocol.ceuserveradapterinstancename" defaultVal="BP"
  required="yes"/>
  <VARDEF varname="CEUMailboxId" type="String" htmlType="text"
   validator="ALPHANUMERIC" size="30" maxsize="250"
   label="cdp.label.ceuprotocol.ceumailboxid" required="no"/>
  </GROUP>
 </AFTExtension>
</AFTExtensions>
```

AFTExtensionsCustomer.properties Adding Connect:Enterprise UNIX

The following is an example AFTExtensionsCustomer.properties adding Connect:Enterprise UNIX for outbound file transfer:

```
#########################################################
# Connect:Enterprise UNIX
```

```
#########################################################
cdp.protocol.label.ceuprotocol = Connect:Enterprise UNIX
ceu.instance.group1.title = Connect:Enterprise UNIX
cdp.label.ceuprotocol.ceuserveradapterinstancename = CEU Server Adapter Instance
 Name
cdp.label.ceuprotocol.ceumailboxid = Connect:Enterprise UNIX Mailbox Id
```

Example Adding an HTTP Send Extension

The following is a business process that adds the HTTP protocol:

```
<process name="AFTRouteViaHTTP">
 <sequence>
  <operation name="HTTP Client Begin Session Service">
   <participant name="HTTPClientBeginSession"/>
   <output message="HTTPClientBeginSessionServiceTypeInputMessage">
    <assign to="." from="*"/>
    <assign to="HTTPClientAdapter">HTTPClientAdapter</assign>
    <assign to="RemoteHost" from="string(RemoteHost)"/>
    <assign to="RemotePasswd" from="revealObscured(RemotePasswd)"/>
    <assign to="RemotePort" from="string(RemotePort)"/>
    <assign to="RemoteUserId" from="string(RemoteUserId)"/>
    <assign to="UsingRevealedPasswd">true</assign>
   </output>
   <input message="inmsg">
    <assign to="." from="*"/>
   </input>
  </operation>
  <operation name="HTTP Client POST Service">
   <participant name="HTTPClientPost"/>
   <output message="HTTPClientPostServiceTypeInputMessage">
    <assign to="." from="*"/>
    <assign to="DocumentId" from="string(DocumentId)"/>
    <assign to="RawRequest">false</assign>
    <assign to="RawResponse">true</assign>
    <assign to="ResponseTimeout">60</assign>
    <assign to="SessionToken" from="string(SessionToken)"/>
    <assign to="ShowResponseCode">true</assign>
    <assign to="URI" from="string(URI)"/>
   </output>
   <input message="inmsg">
    <assign to="." from="*"/>
   </input>
  </operation>
  <operation name="HTTP Client End Session Service">
   <participant name="HTTPClientEndSession"/>
   <output message="HTTPClientEndSessionServiceTypeInputMessage">
    <assign to="." from="*"/>
   </output>
   <input message="inmsg">
    <assign to="." from="*"/>
   </input>
  </operation>
```

```
 </sequence>
</process>
```

Notice the process above uses the revealObscured(RemotePasswd) Xpath function. This is needed because every parameter defined in AFTExtensionsCustomer.xml of htmlType=”Password” is stored either encrypted (if the parameter name has a suffix of "_ENCRYPTED") or obscured (for all other parameters of htmlType=”Password”). In this specific case, the password is passed into the BP as an obscured value but the HTTP Client Adapter requires a password that is not obscured (because UsingRevealedPasswd is set to "true").

When extending protocols and using passwords consider how the service or adapter you plan to use accepts passwords.

AFTExtensionsCustomer.xml for HTTP Send

The following is an example AFTExtensionsCustomer.xml file to add HTTP Send support to AFT:

```
<AFTExtension name="http-protocol" type="consumer-delivery-protocol"
  label="cdp.protocol.label.httpprotocol" bp="AFTRouteViaHTTP">
  <GROUP title="http.instance.group1.title">
  <VARDEF varname="RemoteHost" type="String" htmlType="text"
   validator="ALPHANUMERIC" size="20" maxsize="20"
   label="cdp.label.httpprotocol.httpip" required="yes"/>
  <VARDEF varname="RemotePort" type="String" htmlType="text"
   validator="ALPHANUMERIC" size="20" maxsize="20"
   label="cdp.label.httpprotocol.httpport" required="no"/>
  <VARDEF varname="RemoteUserId" type="String" htmlType="text"
   validator="ALPHANUMERIC" size="20" maxsize="20"
   label="cdp.label.httpprotocol.httpuser" required="no"/>
  <VARDEF varname="RemotePasswd" type="String" htmlType="password"
   validator="ALPHANUMERIC" size="20" maxsize="20"
   label="cdp.label.httpprotocol.httppassword" required="no"/>
  <VARDEF varname="URI" type="String" htmlType="text" validator="ALPHANUMERIC"
   size="20" maxsize="20" label="cdp.label.httpprotocol.uri" required="no"/>
 </GROUP>
</AFTExtension>
```

The mandatory parameter for this example is Remote Host. Optional parameters include Remote Port, Remote User Id, Remote Password, and URI.

AFTExtensionsCustomer.properties for HTTP Send

The following is an AFTExtensionsCustomer.properties file to add HTTP Send support to AFT:

```
#########################################################
HTTP Send
#########################################################
cdp.protocol.label.httpprotocol = HTTP Send
http.instance.group1.title = HTTP Send
cdp.label.httpprotocol.httpip = HTTP IP Address
cdp.label.httpprotocol.httpport = HTTP Port
cdp.label.httpprotocol.httpuser = HTTP User
cdp.label.httpprotocol.httppassword = HTTP Password
cdp.label.httpprotocol.uri = URI
```

The user interface created by this example AFTExtensionsCustomer.properties file adds the attribute for cdp.protocol.label.httpprotocol in the Protocol list.

In the next page of the Create Partner wizard, the following elements and attributes are added:

• cdp.protocol.label.httpprotocol is at the top of the white screen
• http.instance.group1.title is title in parameter box
• cdp.label.httpprotocol.httpip parameter label
• cdp.label.httpprotocol.httpport parameter label
• cdp.label.httpprotocol.uri parameter label

In the next page of the Create Partner wizard, the following elements and attributes are added:

• cdp.protocol.label.httpprotocol is at the top of the white screen
• http.instance.group2.title is the title in parameter box
• cdp.label.httpprotocol.httpuser parameter label
• cdp.label.httpprotocol.httppassword parameter label

Encrypted Passwords

If you include an "_ENCRYPTED" suffix on a parameter it causes the user-entered values to be encrypted when saved (use only for fields of htmlType=”Password”). Do not use the revealObscured() function with passwords that are encrypted. Rather, use the encrypted password only if the particular service to be invoked can accept an encrypted password and decrypt it internally.

If a value is declared to be of type "password" and does not have an "_ENCRYPTED" suffix, the value is saved into the database obscured and delivered to ProcessData obscured. Call the revealPassword (Xpath) XPath function to reveal the password, immediately before using the password.

Example Adding an FTPS Extension

For example, if you were adding FTPS as a outbound file transfer mechanism, AFTExtensionsCustomer.xml could be the following:

```
:<!--Custom FTP/S Protocol for internal and external connections -->
<AFTExtension name="custom-ftps-protocol" type="consumer-delivery-protocol"
label="custom.ftps.protocol.label" bp="CustomFileGatewayDeliverFTPS">
<GROUP title="custom.ftps.instance.group1.title">
<VARDEF varname="FTPLocation" type="String" htmlType="select"
validator="ALPHANUMERIC" size="30" maxsize="250"
label="custom.ftps.protocol.label.ftplocation" options="CUSTOMInternalExternal"
required="yes" defaultVal="External"/>
<VARDEF varname="HostName" type="String" htmlType="text"
validator="ALPHANUMERIC" size="30" maxsize="250"
label="custom.ftps.protocol.label.hostname" required="yes"/>
<VARDEF varname="Port" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftps.protocol.label.port" required="yes"/>
<VARDEF varname="ConnectionType" type="String" htmlType="select"
validator="ALPHANUMERIC" size="30" maxsize="250"
label="custom.ftps.protocol.label.connectiontype" options="CUSTOMFTPConnType"
required="yes"/>
```

<VARDEF varname="Username" type="String" htmlType="text" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.user" required="yes"/> <VARDEF varname="ObscuredRemotePasswd" type="String" htmlType="password" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.remotepasswd" required="yes"/> <VARDEF varname="CACertificateId" type="String" htmlType="select" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.cacertificateid" options="CACertListerbyID" required="no"/> <VARDEF varname="SystemCertificateId" type="String" htmlType="select" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.systemcertificateid" options="SystemCertListerbyID" required="no"/> <VARDEF varname="SSL" type="String" htmlType="select" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.ssl" options="CUSTOMSSLMode" required="yes" defaultVal="SSL_EXPLICIT"/> <VARDEF varname="CipherStrength" type="String" htmlType="select" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.cipherstrength" options="CUSTOMCipherStrength" required="yes" defaultVal="STRONG"/> <VARDEF varname="ClearControlChannel" type="String" htmlType="select" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.clearcontrolchannel" options="CUSTOMClearControlChannel" required="yes" defaultVal="NO"/> <VARDEF varname="BaseDirectory" type="String" htmlType="text" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.directory" required="no"/> <VARDEF varname="Retries" type="String" htmlType="text" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.retries" required="Yes" defaultVal="3"/> <VARDEF varname="RetryInterval" type="String" htmlType="text" validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.retryinterval" required="Yes" defaultVal="1"/>

Add Consumer Identification Policies

The consumer identification policy is the method Sterling File Gateway uses to identify the consumer to receive the file transfer. The consumer identification policy is defined in the routing channel template. To implement a specific policy:

1. Write a business process implementing the consumer identification policy. For example, your business process may contain a map to derive the consumer name. Note the element name in ProcessData that will contain the consumer name.
2. When you create a routing channel template, select **Dynamic** for **Template Type**.
3. Under **What will determine the consumer?**, select Business Process.
4. Specify the business process name.
5. Specify the element name in ProcessData that contains the consumer name.

Add Custom Event Codes

You can add custom events to Sterling File Gateway that are associated with any custom protocols and business processes you create. You will need a code, a name, and a description for each event you want to create, as well as permission and subscription settings.

To add custom event codes:

1. Open or create a file named `/<install_dir>/properties/customer_overrides.properties`.
2. Add entries in the customer_overrides.properties file with the appropriate details about the custom event codes you are creating.

Your new event will be a series of properties describing attributes of the event. See the FGEventCodes.properties file for examples. Do not edit the FGEventCodes.properties file. Start each line of the custom event code desccription with:

```
filegateway_eventcodes.CUST
```

The following is a basic example:

```
filegateway_eventcodes.CUST_0265.name=
filegateway_eventcodes.CUST_0265.attributes=
filegateway_eventcodes.CUST_0265.text=
filegateway_eventcodes.CUST_0265.description=
filegateway_eventcodes.CUST_0265.permissions=
filegateway_eventcodes.CUST_0265.EventNotificationEmailSubject=
filegateway_eventcodes.CUST_0265.EventNotificationEmailContentType=
```

- Event Code: The event code in the example above is CUST_0265. It consists of keyword underscore 4-digit code. It is used to identify all the attributes for a particular event code. Required.
  - Keyword - any text, optimally 4 characters long, but cannot be FG_ nor AFT_ . In the example, the keyword is CUST.
  - 4-digit Code - consists of two 2-digit codes - a category identifier and a unique identifier. No two events can have the same 4-digit code.
    - Category Identifier - The first 2-digit code is a category identifier. You can use a system-defined category or create your own 2-digit code to categorize your codes in a way that is convenient for you. In the example, the category identifier is 02. The following are the system-defined category codes:

Code	Category
00	Producer File Transfer
02	Routing Business Process
04	File Gateway General
05	Route Plan Determination
06	File Transformation
07	Consumer File Transfer

    - Unique Identifier - The second 2-digit code is the unique identifier for the event within the category. 00 to 49 are successful events and 50 to 99 are error events. Error events display in red in Sterling File Gateway. You cannot exceed 99 event codes in a category. In the example, the unique identifier is 65.

- <EventCode>.name - This is the name of your event. It will be shown in the subscription UI (**Profile** > **Notifications**) if subscriptions are enabled, and in the log. Required.
- <EventCode>.attributes - A comma-delimited list of attributes for this event. While any attribute can be passed into the event, only these attributes will be stored in the database, will be searchable through the UI, and are usable in the event text defined below. They are generally indexed with the first one in the list having an index of 0. The attribute names must be names that can be passed as an xml element (no special characters, no spaces). This property is required but the list can be empty.

- <EventCode>.text - This property contains the text that will show up in the UI when this event is viewed. It can contain text and is generally limited by the Java Format rules (for example, in order to have a single quote, you must put two of them right next to each other.) You can also use attributes above by using the notation {#} which will substitute in the UI the value of the attribute at the index of the #. You do not have to use attributes, the user in the UI can click on the event and see all the attributes and they will still be searchable. So you can send in and store more attributes than you might want to show in the UI. Required.
- <EventCode>.description - This description is shown in the subscription UI (**Profile** > **Notifications**). Required.
- <EventCode>.permissions - This is a comma-delimited list of permissions for this event. There are three possible values to use: producer, consumer, subscription. This property is required but it can be empty. Empty means that only the Operator can see the event, and no one can subscribe for notifications to the event.
  - producer - This event can be seen by the producer for this route, and the producer receives notifications if subscribed.
  - consumer - This event can be seen by the consumer for this route, and the consumer receives notifications if subscribed.
  - subscription - This event can be subscribed to. After the subscription is selected for an event, the producer or consumer recieves notification of the event if the event has the corresponding producer or consumer permission AND the subscription permission. For an Operator to receive notification of an event, the event must have the subscription permission.
- <EventCode>.EventNotificationEmailSubject - This is the subject line for the email notification when the event occurs. The default value is File Gateway Routing Event E-mail Notification [Event Code = {0}], where 0 is the four-digit identifier for the event code.

<EventCode>.EventNotificationEmailContentType - This specifies the content type for the email notification when the event occurs. Valid values are text/plain and html. The default is text/plain.

Note: See the /<install_dir>/properties/FGEventCodes.properties file as an example for how to structure your event properties. Do not edit the FGEventCodes.properties file. See *Using Property Files*.

---

3. Save the customer_overrides.properties file and restart Sterling File Gateway for the new file to take effect.
4. Edit your business process that generates the new event codes to call the FileGatewayRouteEventService, with the proper parameters, including the new custom event codes.
5. Add the FileGatewayRouteEventService, with the proper parameters, including the new custom event code. The following example will fire a hypothetical event:

```
<operation>
   <participant name=" FileGatewayRouteEventService "/>
   <output message="Output">
     <assign to="EventCode">CUST_0265</assign>
     <assign to="ExceptionLevel">Normal</assign>
     <assign to="EventAttributes/Directory"
      from="directory/text()" append="true"/>
     <assign to="EventAttributes/Comment" >
      BP changed directories</assign>
     <assign to="." from="*"></assign>
   </output>
   <input message="Input">
     <assign to="." from="*"></assign>
```

```
    </input>
  </operation>
```

To send attributes to the FileGatewayRouteEventService, use the following guidelines. These guidelines only apply to the EventAttributes, not to other parameters of the service:

- The attributes will be sent to the service as a series of assigns. They need to be a series of assigns in order to support the advanced event attribute naming of Sterling File Gateway.
- The first assign must have an attribute append=”true”. This will append the EventAttributes the first time. The remaining assigns cannot have the append attribute.
  - Hardcoded Values. If you want to send a hardcoded attribute value to the service (for example, IsError=true, when you know it will be true every time) then use the following assign statement template:

    ```
    <assign to=”EventAttributes/IsError”
      from=”string(‘true’)” />
    ```

  - Process Data. If you want to send an attribute that is copied from another attribute in the service (for example, the results of another service, stored in the ProcessData at MyService/ResultCode) then use the following assign statement template:

    ```
    <assign to=”EventAttributes/MyServiceResultCode”
      from=”MyService/ResultCode/text()” />
    ```

You can combine those two methods to send both types of attributes into the service, adding the append to the first one:

```
<assign to=”EventAttributes/IsError”
  from=”string(‘true’)” append=”true” />
<assign to=”EventAttributes/MyServiceResultCode”
  from=”MyService/ResultCode/text()” />
```

Example Section in customer_overrides.properties File

Note: Although the example below shows the items displaying on multiple lines, do not do so in your implementation.

```
filegateway_eventcodes.CUST_0265.name=Custom Event - File Error
filegateway_eventcodes.CUST_0265.attributes=ConsumerName,MyServiceResultCode,IDNumber
filegateway_eventcodes.CUST_0265.text=File Error generated during
processing:Result code: {1} reported for File ID {2}
  received for Consumer {0}
filegateway_eventcodes.CUST_0265.description=Event from Custom BP
generated when error occurs
filegateway_eventcodes.CUST_0265.permissions=producer,consumer,subscription
```

Create Custom E-Mail Notifications

This procedure requires knowledge of XSLTs. IBM cannot provide support for modifying XSLTs.

To modify the text or subject for email notification of events:

1. From Sterling File Gateway, select **Tools** > **B2B Console**.
2. Select **Deployment** > **XSLT**.
3. In the Search box, type FG.
4. To edit email notifications received by administrative users, select FgRouteEventEmailNotification. To edit email notifications received by partner users, select FgRouteEventPartnerEmailNotification. Click on **Source Manager** next to the one you want to edit.

   Note: To change the email notifications for both administrative and partner users, you must edit both XSLTs.

5. Select **Check Out**. Click **OK** to lock the file for editing. An example of the original file contents is:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:output method="text"/>
<xsl:template match="/">
The following File Gateway routing event occurred:
Route Event Details:
================================================================================
Event Code:     <xsl:value-of select="/FgRouteEvent/EventCode"/>
Event Message:  <xsl:value-of select="/FgRouteEvent/EventMessage"/>
Producer:       <xsl:value-of select="/FgRouteEvent/Producer"/>
Consumer:       <xsl:value-of select="/FgRouteEvent/Consumer"/>
Filename:       <xsl:value-of select="/FgRouteEvent/Filename"/>
Timestamp:      <xsl:value-of select="/FgRouteEvent/Time"/>
================================================================================
Use the link below to sign into your myFileGateway Suite instance:
<xsl:value-of select="/FgRouteEvent/TargetURL"/>
</xsl:template>
</xsl:stylesheet>
```

6. Revise the file with the changes you need.

   See *About Event Codes* for descriptions of the codes.

7. Save the file to your local disk without changing the name.
8. Check the file back in, releasing the edit lock. Browse to the location where you saved it to your local disk. This new version will persist when you apply future upgrades.
9. To change the subject for an email notification, create or edit the customer_overrides.properties file. This applies to all event codes for your system. The subject is in the following property:

```
filegateway_eventcodes.EventNotificationEmailSubject=File Gateway Routing Event
 E-mail Notification
[Event Code = {0}]
```

   In customer_overrides.properties, add the following:

```
filegateway_eventcodes.EventNotificationEmailSubject=CUSTOM SUBJECT HERE {0}
```

   Where the {0} parameter will be substituted with the event code.

10. To change the text for an event code, create or edit the customer_overrides.properties file. The event message is in the following property:

```
filegateway_eventcodes.text=event message
```

For example, to change the text for event code FG_0506, Route Candidate Does Not Match, make the following entry in the customer_overrides.properties file:

```
filegateway_eventcodes.FG_0506.text=CUSTOM TEXT HERE
```

Substitute your message for CUSTOM TEXT HERE.

Note: Do not edit the FgEventCodes.properties file. Make all changes in the customer_overrides.properties file.

---

11. Stop and restart your system for your changes to take effect.

EBICS Integration

About EBICS Integration with Sterling File Gateway

Sterling File Gateway is required in order to route files to or from one EBICS Partners/Subscribers. After you install Sterling Integrator with the EBICS module, you must separately install Sterling File Gateway, and perform an additional procedure to set up integration.

Sterling File Gateway is an application for transferring files between partners using different protocols, file naming conventions, and file formats. Sterling File Gateway supports movement of large and high-volume file transfers, with visibility of file movement in a process-oriented and highly-scalable framework that alleviates file transfer challenges, such as protocol and file brokering, automation, and data security.

When handling EBICS transactions, Sterling File Gateway uses templates to describe how each transaction is interpreted to determine how and where it should be delivered and provides visibility into the details of the transfers for auditing and troubleshooting.

Files move between the EBICS server and Sterling File Gateway using shared partners and mailboxes. The shared mailboxes are created when EBICS partners are created. Sterling File Gateway then uses the mailboxes for transferring files to or from EBICS partners.

For inbound scenarios, a partner uses an EBICS client to perform an EBICS order file upload (FUL) to the Sterling Integrator EBICS Server, which unpackages the payload and deposits into a shared mailbox (generally of the structure /User/Partner/Inbox). Sterling File Gateway is configured to pick up the file from that mailbox, perform any needed processing, and ultimately deliver the file to a consumer mailbox.

In the outbound scenario, a file (or files) is available in an EBICS partner shared mailbox (generally of the structure /User/Partner/Outbox). The partner uses an EBICS client to perform an EBICS order file download (FDL) from the Sterling Integrator EBICS Server, which packages the payload and makes available to the EBICS client.

To ensure appropriate Sterling File Gateway operation for EBICS inbound and outbound transfer scenarios, routing channel templates and routing channels require specific configurations. Routing channel templates used in EBICS scenarios must include the configuration of provisioning facts and routing channels using those templates much include the specification of values for provisioning facts.

Operators can search for EBICS-specific activity in the Sterling File Gateway application and view an EBICS-centric information display. Alternatively, operators can search for general activity and view a file-centric information display that includes routes and deliveries that resulted from EBICS activity.

Role of EBICS System Administrators in Sterling File Gateway

EBICS System Administrators perform these functions:

- Install and maintain system software
- Handle functions accessed in Sterling Integrator
- Create and manage initial administrative user accounts
- Configure services and adapters
- Manage extensibility features
- Move resources and configurations between systems
- Set up EBICS integration with Sterling File Gateway and Sterling Integrator

Set Up an HTTP Server Adapter for EBICS

An HTTP Server adapter instance is used to receive the incoming EBICS requests and will initiate a business process to start processing the EBICS transactions.

By default, an HTTP Server adapter instance (EBICS Http Server Adapter) is auto-configured for handling EBICS requests. The HTTP Server adapter instance has a URI mapped to the business process.

The URI /ebicsrequest is the default URI specified in the EBICS HTTP Server Adapter. To configure a new URI:

1. From Sterling File Gateway, select Tools > B2B Console.
2. From the Admin console, select Deployment > Services > Configuration.
3. Next to Create New Service, click Go!
4. From the tree directory, select HTTP Server Adapter and click Save.
5. Click Next. Type a name and description for your EBICS HTTP Server Adapter instance.
6. Click Next. Enter a port number and Total Business Process queue depth threshold. Enter 0 for an unlimited queue depth threshold.
7. Click add next to New URI. Type the desired URI.
8. Select Business Process under Launch a BP Or WAR.
9. Set Send Raw Messages to No.

Note: The newly configured URI and the HTTP Server port number must match the host URL of the bank's profile.

Set Up EBICS Integration with Sterling File Gateway

Before you can use Sterling File Gateway to route files to or from EBICS Partners/Subscribers, you must set up EBICS integration with Sterling File Gateway.

To set up EBICS integration with Sterling File Gateway:

1. From Sterling File Gateway, select **Tools** > **B2B Console**.

2. From the Sterling Integrator Admin menu, select **Deployment** > **Services** > **Configuration** to enable the scheduler that will be used by the EBICS Server service for transaction housekeeping.
3. Select **EBICS** > **Subscription Manager**.
4. Select to create the following EBICS resources:
   - Bank
   - Partner
   - User
   - Offer
   - Contract
   - Permissions
5. Repeat Step 4 for as many partners as you want to create.
6. Close the Sterling Integrator window, but do not log out, to return to Sterling File Gateway.
7. From Sterling File Gateway, select **Participants** > **Groups**.
8. Select **Add Partners** and associate EBICS Partners/Subscribers with the Sterling File Gateway All Partners group.

   Note: You may see an error message that the EBICS partner does not have an associated User Account. This does not affect the association with the group.

9. Select **Routes** > **Templates** to set up a routing channel template to use for routing files to or from EBICS Partners/Subscribers. You must define a routing channel template using the UserID as a provisioning fact and then reference the UserID provisioning fact in the mailbox path for the producer, consumer, or both, depending on how the template will be used.

   Note: By adding the provisioning fact in the template, you ensure that mailbox path structures match what was previously setup during EBICS Partner/Subscriber creation. If a mailbox path structure other than /User/Partner/Inbox or /User/Partner/Outbox was specified, the template should match that structure.

10. Select **Routes** > **Channels** to set up routing channels to use for routing files between EBICS Partners/Subscribers.
11. Test the setup by accessing an EBICS client, log in as the EBICS Partner/Subscriber, and send an EBICS order.
12. Select **Routes** > **Activity**.
13. Select the EBICS Partner/Subscriber from the Producer menu.
14. Click **Find**.
15. Look for the transfer initiated in Step 11 and select the row to view details.
16. Select the message ID hyperlink to view the route details and link to dataflows and communication sessions in the B2B Console.