

Sterling File Gateway



System Administrator Help

Version 2.1

Sterling File Gateway



System Administrator Help

Version 2.1

Note

Before using this information and the product it supports, read the information in "Notices" on page 89.

This edition applies to Version 2 Release 1 of IBM Sterling File Gateway and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2008, 2012.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Install and Set Up. 1

Create User Accounts	1
User Interface Access	3
Use Preconfigured User Groups to Assign Permissions.	4
Migrate from Advanced File Transfer to Sterling File Gateway.	6
Migrate Using Export and Import	7
About Export and Import	7
Migrating a Community with Import and Export	7
Migrate Sterling Integrator Managed Resources.	8
Migrate Custom Protocols	8
Migrate Sterling File Gateway Community	10
Migrate Sterling File Gateway Configurations	14
Use Audit Records to Trace Administrative Actions	15
Set Up HTTPS for myFileGateway.	15
Rebrand Sterling File Gateway	17
Change Purge Settings.	20
filegateway.properties	21
filegateway_ui.properties	24
filegateway_protocol.properties.	26
About Event Codes.	26
filegateway_eventcodes.properties	29
Migrate Events After Applying Sterling File Gateway 2.1 Build 5100	30
Sterling File Gateway: Specific Recommendations Checklist	31
Configure a Load Balancer	34

Chapter 2. Get Started 35

Prepare Communications Adapters for Use with Sterling File Gateway	35
Sterling File Gateway System Business Processes	35
Set Up and View Logs.	36
Prepare to Use the Connect:Direct Protocol	37

Prepare to Use PGP	37
Prepare to Use SSH/SFTP	38
Exchange Information with Partners	39

Chapter 3. Authentication Outside Sterling File Gateway 41

About Authenticating Users Outside Sterling File Gateway	41
Implementing Single Sign-On in Sterling File Gateway	41
Implementing Lightweight Directory Access Protocol (LDAP) in Sterling File Gateway	42
Configure Sterling Secure Proxy	44

Chapter 4. Extend the Capabilities 45

Extend the Capabilities of Sterling File Gateway	45
Add Custom Protocols	45
Example Custom Protocols	46
Add Consumer Identification Policies	51
Add Custom Event Codes	52
Create Custom E-Mail Notifications	55
Implement AS2	56

Chapter 5. Custom File Layer Types 61

About Custom File Layer Types	61
Add Custom File Layer Types	78
Edit Custom File Layer Types	84
Add a Parameter to a Custom File Layer Type.	85
Delete a Parameter from a Custom File Layer Type	85
Delete a Custom File Layer Type	86

Notices 89

Index 93

Chapter 1. Install and Set Up

Create User Accounts

Create user accounts in the B2B Console.

About this task

When you install IBM® Sterling File Gateway, several default accounts are automatically created to get you started. You can use the default accounts to perform the tutorial described in the Overview.

One of the first actions you must take is to create your own accounts with unique IDs and passwords, because the default ones can be known by all Sterling File Gateway customers. Log in to Sterling File Gateway with the following credentials:

- User ID = fg_sysadmin
- Password = password

To create a user account:

Procedure

1. From Sterling File Gateway, select **Tools > B2B Console**.
2. From within IBM Sterling B2B 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 B2B 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 B2B 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 B2B 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 B2B 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 view details and links to details in B2B Console. Can mark routes as reviewed or not reviewed. Can replay and redeliver.	Can search and view events, but cannot view linked details. Can mark routes as reviewed or not reviewed. Cannot replay or redeliver.	Can search and view events, but cannot view linked details. Can mark routes as reviewed or not reviewed. Cannot replay or redeliver.	(Default page.) Can search and view details and links to details in B2B Console. Can mark routes as reviewed or not reviewed. Can replay and redeliver.	No access.
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.

Page	System Admin	Integration Architect	Route Provisioner	Operator	Partner
myFileGateway > Activity > Upload Files > Download Files > Reports > Profile	No access.	No access.	No access.	No access.	(Default page.) Complete access to search, generate reports, upload files, 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 B2B Integrator. Users inherit all permissions associated with the groups.

Permissions Inherited from Groups

These groups are preinstalled with Sterling B2B 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

Group	Permissions Inherited from the Group
File Gateway Partner Users	myFilegateway Login myFilegateway Logout myFilegateway User Name myFilegateway File Activity myFilegateway File Upload myFilegateway File Download 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 > Go!**
4. Type a **Group ID > Group Name > 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**.
- Click **Finish** and **Return**.
 - 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.

About this task

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:

Procedure

- Start Sterling B2B Integrator. Sterling B2B Integrator must be up and running when the following script is run.
- Run the following script: `<install_dir >/tp_import/aft2fg.sh` (for UNIX) or `aft2fg.cmd` (for Windows)

Note: Do not interrupt the script or allow Sterling B2B Integrator to stop during the script. If the script does not complete successfully, you can run it again. If the problem persists, contact Customer Support.

- 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 B2B 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.
- 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.
- The imported partners will automatically be associated with the "All Partners" partner group. A different default group can be set in `customer_overrides.properties` by editing the property:
`filegateway_ui.fgOnboardingDefaultUserGroupId=CustomUserGroup`

where CustomUserGroup is the name of the group to assign to newly migrated users. 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.

6. Disable the AFTPurgeArchiveMailboxes business process in Sterling B2B Integrator.
7. If you have created custom protocols in AFT, the custom business process that implements the protocol may need to be modified. If the business process name contained an underscore, parameters passed from AFT to custom protocol business processes were incorrectly prefixed with part of the business process name. In Sterling File Gateway, these prefixes are removed, which is the correct behavior. Edit your business process where the custom parameters are used and correctly reference them according to the table below.

Business Process Name	Parameter Definition	AFT Parameter	SFG Parameter	Changes Required?
My_CustProtBP	HostName	CustProtBP_ HostName	HostName	Yes. Change the custom protocol business process to use "HostName" instead.
CustomProtocolBP	HostName	HostName	HostName	No change required because the custom protocol business process name does not have an underscore.

See *Add Custom Protocols*.

Migrate Using Export and Import

About Export and Import

The Import/Export feature enables you to save time and increase the accuracy of duplicating supported resources on different Sterling B2B 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 B2B 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.

Migrating a Community with Import and Export

Sterling Integrator and Sterling File Gateway both let you import and export resources from one system to another so you do not have to recreate the resources. While Sterling Integrator lets you import and export single resources, for Sterling File Gateway you must import or export an entire community, not just a single resource. Some resources are not community specific and must be migrated before the community. There are specific guidelines and requirement for migrations as well as a recommended migration order. The migration is a several step process that requires multiple imports and multiple resource files.

The recommended migration order is:

1. Sterling Integrator Managed Resources – Sterling Integrator Managed Resources can be migrated at anytime (before, after, or with the Sterling File Gateway Community). However, depending on the resources being imported, some may need to be imported after the Sterling File Gateway Community is imported

(such as an AS2 Partner). Relationships and dependencies must be considered when determining when and if a Sterling Integrator Managed resource should be imported before or after the import of the Sterling File Gateway Community.

2. Custom Protocols – Custom Protocols must be migrated prior to the Sterling File Gateway Community migration.
3. Sterling File Gateway Community – The Sterling File Gateway Community must be migrated before Partner Groups (within Sterling File Gateway Configuration) and some Sterling Integrator Managed Resources such as Sterling Integrator managed partners. The Sterling File Gateway Community must be migrated after the migration of any required Custom Protocols.
4. Sterling File Gateway Configurations – Partner Groups, within Sterling File Gateway Configurations, must be migrated after the Sterling File Gateway Community has been migrated.

Migrate Sterling Integrator Managed Resources

Sterling Integrator customized resources used by the Sterling File Gateway Community must exist on the target system before the Community is migrated. These customized resources can be migrated to the target system or created new on the target system.

Sterling Integrator managed resources are any resources that are not created within Sterling File Gateway; instead these resources are created and managed within Sterling Integrator. These might include, but are not limited to: AS2 partners, SSH profiles, SSH Authorized User Keys, certificates, Pre- and Post- process business processes, customized server adapters, etc.

You can migrate the Sterling Integrator managed resources with an independent Resource Tag (non-Sterling File Gateway Community Resource Tag) or you can migrate the resources ad-hoc. Exporting these components is not subject to the same constraints as the resources within a Sterling File Gateway Community. Special consideration should be made if any of these Sterling Integrator managed resources are added to the Sterling File Gateway Community Resource Tag because it may affect the import flexibility when overwriting or adding new resources. For example, if a Sterling Integrator managed resource is imported and requires the **Update existing objects...** flag set to **YES**, then all objects within the Sterling File Gateway Community will be imported and updated.

Migrate Custom Protocols

Custom Protocols are custom configurations within the system, so the migration steps and migrated resources vary between system versions and patches. Custom Protocols are not Community specific and you should migrate them before the Sterling File Gateway Community. The Custom Protocols should not be added to the Community Resource Tag. Migrating the Custom Protocols is a multi-step process. Some of the files are migrated with the user interface and some are migrated outside the user interface. After all of the files are migrated, the system must be stopped, set up, and restarted.

Process

To migrate Custom Protocols:

1. Use the Resource Manager Resource File to migrate Custom Protocols to the target system.
2. Copy the AFTEntensionsCustomer files from the source system to the target system.

3. Stop, set up, and restart the system.

Guidelines and Requirements

Guidelines and requirements for Custom Protocol migration include:

- Custom Protocols are system specific not Community specific; they are available to all Communities on the system.
- Custom Protocol resources and files (or entries within the files) that you want to migrate should be migrated and copied to the target system before migrating the Sterling File Gateway Community.
- Custom Protocol resources should not be added to the Community Resource Tag.
- The resources that define a Custom Protocol can vary from system to system. You should migrate all customized resources that are used by the Custom Protocol. This includes any and all custom business processes and Services used by the Custom Protocol.

Use the Resource Manager Resource File to Migrate Custom Protocols

Custom Protocols used by, or available to, the Sterling File Gateway Community must be migrated to the target system before the Community is migrated. All of the custom resources that are required for the Custom Protocol to work must be exported from the source system via the Resource File from the Sterling File Gateway Resource Manager (for example, custom business processes or custom Services). These custom resources can be added to a non-Sterling File Gateway Community Resource Tag or exported ad-hoc. These resources should not be added to a Sterling File Gateway Community Resource Tag. These custom resource components are not subject to the same constraints as the resources within a Sterling File Gateway Community.

Copy the AFTExtensionsCustomer Files from the Source to the Target

After the resources used by the Custom Protocol have been migrated to the target system through the Resource Manager, both files, located within the Sterling Integrator installation directory, must be copied and moved from the file path specified below on the source system to the same file path on the target system:

AFTExtensionsCustomer.xml
The AFTExtensionsCustomer.xml is located in the following directory within the Sterling Integrator installation directory: <installation directory>/container/Applications/aft/WEB-INF/classes/resources/xml
AFTExtensionsCustomer.properties
The AFTExtensionsCustomer.properties is located in the following directory within the Sterling Integrator installation directory: <installation directory>/container/Applications/aft/WEB-INF/classes/resources/

If these files contain any Custom Protocol configurations that you do not intend to migrate, you must remove the unwanted configurations from the files before you migrate them. If the target system already contains either or both of the AFTExtensionsCustomer files, then you must add the entries from the source system files to the target system files.

Note: Only add completely new Customer Protocol entries to these files. If you add modified (different) versions of previously existing Custom Protocol entries or update previously existing Custom Protocol entries, it may lead to unexpected behavior.

Stop, Set Up, and Restart the System

After you have migrated the custom protocols and copied the AFTExtensionsCustomer files:

1. Stop the system.
2. Run setupfiles.
3. Run deployer.
4. Restart the system.

Migrate Sterling File Gateway Community

After you migrate custom protocols, you can migrate the Sterling File Gateway Community. There are guidelines and settings for the specific resources types, including communities, resource tags, and Sterling Integrator Resources.

Guidelines

The guidelines for migrating a Sterling File Gateway community include:

System	Guidelines and Requirements
Community Management	<ul style="list-style-type: none"> • You can only export or import a single community per Resource Tag at a time. • You must export the entire community as a whole from the source system based on the Resource Tag and you must import the entire community as a whole to the destination system. You must export all resources within the Resource Tag and import all resources included within the resource file. • You cannot specify individual partners to import to the target system. You must import the entire community to which the partner belongs. • You can only use a single source system in the migration path. The Sterling File Gateway Community on the target system cannot be updated with communities from multiple Sterling File Gateway source systems. • You must create all new resources within the Sterling File Gateway community on the source system and then migrate them to the target system.

Resource Tag	<p>The Resource Tag (Deployment > Resource Manager > Resource Tags) is managed by Sterling File Gateway when Community and Partner additions or updates are made.</p> <ul style="list-style-type: none"> • Never delete the Resource Tag itself. Recreating a Sterling File Gateway Community Resource Tag requires contacting customer support. • Never remove resources from a Resource Tag associated with a Sterling File Gateway Community. If you must remove a resource, delete the resource from the Community using the Sterling File Gateway user interface. This automatically removes the resource from the Resource Tag. During a migration where you removed a resource on the source system, neither the Sterling File Gateway Community nor the Resource Tag on the target system will be updated with the removal. After the migration, you must manually remove the resource from the Sterling File Gateway Community on the target system and this will automatically remove the resource from the Resource Tag. • You must manually add resources that are not managed by Sterling File Gateway (non-Sterling File Gateway partners, mailboxes, user accounts, etc....) to the Resource Tag. <p>If the Resource Tag already exists on the target system (for example, because of a previous migration), you must rename the Resource Tag before you do the migration. If you do not rename the existing Resource Tag, after the migration there will be multiple Resource Tags on the target system, each representing a portion of a Sterling File Gateway Community.</p>
Sterling Integrator Resources	<p>All Sterling Integrator customized resources used by, or available to, the Sterling File Gateway Community must exist on the target system before the Community is migrated. You can either migrate these customized resources to the target system or create the resources new on the target system.</p> <p>If you migrate these Sterling Integrator resources, you can either migrate them by adding them to a non- Sterling File Gateway Community Resource Tag or by migrating them ad-hoc.</p>

Resource Tag Management

Do not make changes to the Resource Tag. There are four Resource Types required for successful migration and all four must be selected.

- Trading Partner Data
- Accounts
- Mailboxes
- Communities

You can add other Resource Types to the Resource Tag. Be sure to include any and all related resources and components for the Resource Types you add.

The required Resource Types have required settings for migration:

Resource	Selections
Trading Partner Data Resources	<p>There are two Trading Partner Data resources that are required for migration. You must select both:</p> <p>Identities By default, Identities are added to the Resource Tag for all Trading Partners within the Community. All Identities that are added to the Resource Tag by default are required for a Community migration, so you must make sure all Identities remain selected (are present in the "Must Be Associated" field). You can add other Identities as needed. Be sure to add any and all related resources and components for the added Identity to the Resource Tag.</p> <p>Packagings By default, Packagings are added to the Resource Tag for all Trading Partners within the Community. All Packagings that are added to the Resource Tag by default are required for a Community migration, so you must make sure all Packagings remain selected (are present in the "Must Be Associated" field). You can add other Packagings as needed. Be sure to add any and all related resources and components for the added Packaging to the Resource Tag.</p> <p>You can add other Partner Resources as needed. Be sure to include any and all related resources and components for the added Partner Resources.</p>
Accounts	<p>Only the User option is required for migrating a Community managed by Sterling File Gateway. All Users that are added to the Resource Tag by default are required for a successful Community migration. You must be sure all Users remain selected (are present in the "Must Be Associated" field). You can add other users to the Resource Tag. Be sure to add any and all related resources and components to the Resource Tag for the added Users.</p> <p>Make sure "Users" is the only Account resource selected.</p> <p>Note: It is recommended that Permissions and Groups not be added to the Resource Tag for migration. They are not required and if they are migrated between systems with different versions or patches it might lead to unexpected behavior.</p>

Resource	Selections
Mailbox	<p>There are two Mailbox resources that are required for migration. You must select both:</p> <p>Mailbox Virtual Roots By default, Mailbox Virtual Roots are added to the Resource Tag for all Partners in the Community. All Mailbox Virtual Roots that are added to the Resource Tag by default are required for a Community migration, so you must make sure all Mailbox Virtual Roots remain selected (are present in the “Must Be Associated” field). You can add other Mailbox Virtual Roots to the Resource Tag.</p> <p>Mailbox Metadata By default, Mailbox Metadata are added to the Resource Tag for all Trading Partners within the Community. All Mailbox Metadata that are added to the Resource Tag by default are required for a Community migration, so you must make sure all Mailbox Metadata remain selected (are present in the “Must Be Associated” field). You can add other Mailbox Metadata to the Resource Tag. Be sure to add any and all related resources and components to the Resource Tag for the added Mailbox Metadata.</p> <p>Mailbox Routing Rules can be added as needed. Be sure to add any and all related resources and components for the Mailbox Routing Rules to the Resource Tag. For example, when adding a custom Mailbox Routing Rule, make sure you include the Business Process referenced by the Mailbox Routing Rule.</p> <p>The File Gateway Routing Rule should not be added to the Resource Tag. This routing rule may be updated between versions or patches. If it is migrated between systems with different versions or with different patches, it might lead to unexpected behavior.</p>
Communities	<p>By default, only the Community that the Resource Tag represents will appear as an option. The Community is required for a migration of a Community, so it must remain selected. If it is not present, stop the migration and contact customer support.</p>

Resource Tag Export

The export must be performed by exporting with a Resource Tag. Always examine the Export Report after generating the Resource File and verify that no errors were generated before you continue with the migration. If errors were generated in the Export Report, contact customer support to open a case and provide the export report and the Resource File generated.

Resource Tag Import

All resources within the Resource Tag must be imported. All resources within the resource file are required for the import to be successful, even if you are doing a migration to insert new resources into the target system's Community and not changing any existing resources. The Import All Resources option automatically selects all resources in the resource file for importing. It is recommended that you always use the Import All Resources option. If you do not use this option, you will be prompted to manually select all of the resources to import for each resource type.

If the target system already contains a Resource Tag with the same name as the one being imported, you must rename the Resource Tag on the target system before starting the import. Do not delete the Resource Tag on the target system prior to importing.

During the import you will be asked "Some objects being imported may exist in the system. Do you wish to update them?". This option can be set to either Yes or No. Be careful when setting this to "Yes" because the resource file being imported represents many resources within a Sterling File Gateway Community where all of the resources must participate in the import process. Also, there may be planned differences in configuration for some resources between the source and target systems. For example, the Partner User passwords may differ between the source and target systems.

Always examine the Import Report and verify that no errors were generated. If errors were generated, contact customer support to open a case and provide the import report and the Resource File used.

Migrate Sterling File Gateway Configurations

After you migrate Sterling File Gateway the Custom Protocols and Community, you can migrate the Sterling File Gateway Configurations. The configuration resources are not Community specific and carry with them additional constraints that affect the migration process. It is recommended that these resources be migrated separately from the Community.

Guidelines and Requirements

Sterling File Gateway Configurations are not added to a Resource Tag by default. It is recommended that the File Gateway Configurations not be added to the Resource Tag and that they follow an independent (parallel) migration process. Sterling File Gateway Configurations include:

Partner Groups	
	<p>You should migrate the Partner Groups before the other SFG Configurations.</p> <p>You must import Partner Groups separately from the Community when you are using the migration process to add (insert) new configurations into the Sterling File Gateway Community. Failure to import Partner Groups will lead to a partner being disassociated from the Partner Group(s) that the partner is included within, and the new Partner will not show up as a Partner within Sterling File Gateway.</p> <p>The migration of the Partner Groups should be performed in a separate migration (export and import process), either by creating a new Resource Tag that contains only Partner Groups, or an ad hoc export and import (with no Resource Tag configuration) can be performed.</p> <p>During a migration where a Partner Group with the same name already exists on the target system, the "Some objects being imported may exist in the system. Do you wish to update them?" option must be set to Yes. You must set this to Yes or the selected Partner Groups will not be updated on the target system.</p>

Consumer Customer File Layers, Producer Customer File Layers, Routing Channels, Routing Channel Templates	
	<p>After migrating the Community and the Partner Groups, you can migrate the remaining Sterling File Gateway Configurations' resources to the target system.</p> <p>If any or all of these resources exist on the target system with the same name, you must delete them from the target system before you perform the import. It is recommended that these resources are deleted before the migration of the Sterling File Gateway Community. The "Some objects being imported may exist in the system. Do you wish to update them?" option does not apply to these resources.</p>

Use Audit Records to Trace Administrative Actions

About this task

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:

Procedure

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

About this task

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 B2B 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:

Procedure

1. Set up a perimeter server in the DMZ.
2. Configure a new Perimeter Server in Sterling B2B 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 B2B 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 > 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`

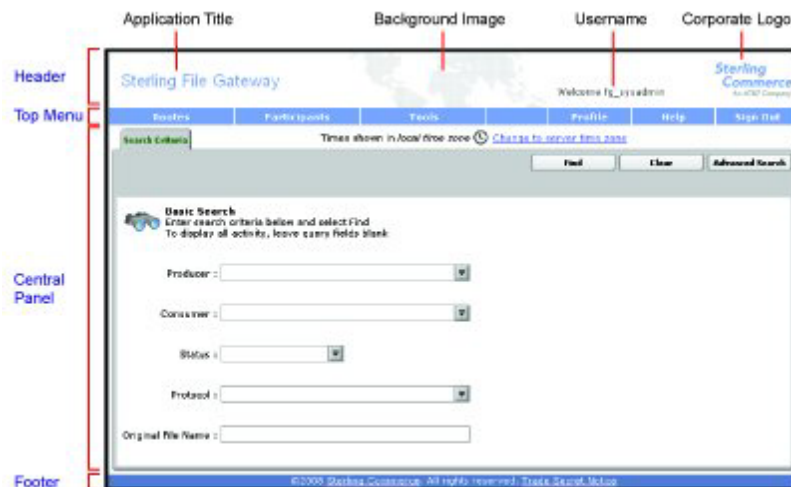
where *<host>* is the IP address or host name of the computer where the remote perimeter server is running and *<httpListenPort>* is the port previously specified. A dialog opens, requesting the user name and password to use with *myFileGateway*. If instead the browser encounters an error, verify that *<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.

Rebrand Sterling File Gateway

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*.

About this task

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 5101. 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:

Procedure

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.

Results

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

About this task

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).
- lifespan_session - length of time, in hours, before communication session records are purged. Default is 336 hours (14 days).

Values for these settings are in the established 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 B2B 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
- FG_EVENTATTR

- FG_EVENT

To change settings for purge:

Procedure

1. Open or create the following file: <install_dir>/properties/customer_overrides.properties
2. Add the following properties: dmvisibility.lifespan_dataflow=Value
dmvisibility.lifespan_adminaudit=Value
dmvisibility.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 in *Sterling B2B Integrator 5.1 online library*.

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* in the Sterling B2B Integrator 5.1 online library.

Property	Description
ignoreFilenameex	<p>Setting a regex pattern for this will cause any arrived file that matches your regex pattern to be ignored by Sterling File Gateway.</p> <p>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.</p> <p>Specify one or more file name patterns to ignore in the following format:</p> <ul style="list-style-type: none"> • filegateway.ignoreFilename1=<regex expression> • filegateway.ignoreFilename2=<regex expression> • filegateway.ignoreFilename3=<regex expression> • filegateway.ignoreFilenameex=<regex expression> <p>For example: filegateway.ignoreFilename1=.+[.]tmp\$</p> <p>would have the effect of ignoring all files with an extension of .tmp. Note: The regex pattern must match the file name in its entirety. Partial matches are not recognized.</p>
ftpClientAdapterName	<p>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:</p> <p>ftpClientAdapterName=FTPClientAdapter</p>
bpCompletionProbes.1 bpCompletionSleepMsec.1 bpCompletionProbes.2 bpCompletionSleepMsec.2	<p>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.</p> <p>First probe 120 times with 100 Milliseconds between, for a total of 12 seconds. Default is:</p> <p>bpCompletionProbes.1=120 and bpCompletionSleepMsec.1=100</p> <p>Then probe 600 times with 2000 Milliseconds between, for a total of 1200 seconds (20 minutes). Default is:</p> <p>bpCompletionProbes.2=600 and bpCompletionSleepMsec.2=2000</p>
pgpCmdline2svcname	<p>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:</p> <p>pgpCmdline2svcname=PGPCmdlineService</p>
fgRoutePGPCmdLineSocketTimeout	<p>Timeout value, in milliseconds, for PGP package and unpackage operations invoked by Sterling File Gateway. Default value is 240000 milliseconds (4 minutes)</p>

Property	Description
fgRouteConcurrentSessionLimit	<p>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.</p> <p>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)</p>
required_si_build_ver	<p>The build number (version) of Sterling B2B Integrator that Sterling File Gateway requires. This is checked at system start up. If the current version of Sterling B2B 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.</p>
fgmaxBroadcastListSize	<p>Maximum allowed size of the consumer list used for broadcast. If the returned list of consumers exceeds this size, the file is not routed. By default, the maximum size of a broadcast list is set to 100.</p>
grantIntermediateMailboxPermissions	<p>Controls permissions granted to intermediate mailboxes (those between a partner user's virtual root and the leaf mailbox). These mailboxes are created during routing channel creation or dynamic routing. Setting this property to true grants View & Execute rights to the intermediate mailboxes to eligible partner users. View rights are required to list mailbox contents. Execute rights are required to 'log in' to a mailbox. Setting both rights allows users of the FTP and SFTP protocol adapters to traverse through any intermediate mailboxes to reach the leaf. The default is false.</p> <p>For example: grantIntermediateMailboxPermissions=false</p>
extensionBPStatusIndicatorElement= <i>IgnoreThisFault</i>	<p>Use in conjunction with custom business processes that extend the capabilities of Sterling File Gateway, to override its default behavior when such a business process fails. Normally, a custom business process that encounters a fault causes processing of the associated file to fail. If extensionBPStatusIndicatorElement is set to <i>IgnoreThisFault</i> and the custom business process has created an element named <i>IgnoreThisFault</i> with value "true", Sterling File Gateway will disregard the fault and attempt to continue processing the arrived file or route.</p> <p>The value <i>IgnoreThisFault</i> is suggested for the element name value, but the value can be any string that is a legal element name in XML. By default, this property is not included in filegateway.properties..</p> <p>Use the following assignment in the custom business process to set the value of the Process Data element: <assign name="Assign" to="IgnoreThisFault">true</assign></p> <p>See <i>Handling Errors in Custom Business Processes</i> for how to implement.</p>

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. See *Using Property Files* in the Sterling B2B Integrator 5.1 online library.

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.
myFghelp.uri	Specifies the URL for the help used by <i>myFileGateway</i> . 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 <i>myFileGateway</i> . 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.

Property	Description
myFgStorageType	<p>Storage type to use for new documents sent through myFileGateway. Possible values are:</p> <ul style="list-style-type: none"> • default - use the system default • db - store documents in database • file - store documents in file system <p>The default is default.</p> <p>To change this value, use the customer_overrides.properties file. For example to set it to database: filegateway_ui.myFgStorageType=db</p>
fgMaxActivityRecords	<p>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:</p> <p>fgMaxActivityRecords=1000</p>
fgWindowTitle	<p>The title of the window that displays in the top browser bar for Sterling File Gateway. Required. Default is Welcome to Sterling File Gateway.</p>
myfgWindowTitle	<p>The title of the window that displays in the top browser bar for <i>myFileGateway</i>. Default is Welcome to Sterling File Gateway.</p>
fgSkinName	<p>The file that contains the branding information for Sterling File Gateway. Required. Default is FileGateway.</p>
myfgSkinName	<p>The file that contains the branding information for <i>myFileGateway</i>. Required. Default is FileGateway.</p>
fgOnboardingDefaultSessionTimeout	<p>The default session timeout in minutes for a Partner User created using the Sterling File Gateway onboarding.</p> <p>The default is:</p> <p>fgOnboardingDefaultSessionTimeoutInMinutes=15</p>
fgOnboardingDefaultUserGroupId	<p>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.</p>
FGConsecFailedAttempts	<p>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.</p>
FGLockInterval	<p>Length of time, in minutes, that the lock is applied after the number of failed login attempts is exceeded. Default is 30.</p>
userIdMinLength	<p>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)</p> <p>The value of # of characters must be greater than zero. To implement single sign-on, this value must match the value set in Sterling B2B Integrator.</p>

filegateway_protocol.properties

The filegateway_protocol.properties file contains properties which control the protocols available when specifying the search criteria for Sterling File Gateway activity searches.

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

Note: Do not edit the filegateway_protocol.properties file. Make all changes in the customer_overrides.properties file. For example, to change the setting for Sterling Connect:Direct® Inbound, enter the following line into customer_overrides.properties:

```
protocol.FG_CDIN=
```

See *Using Property Files* in the Sterling B2B Integrator 5.2 online library.

Property	Description
FG_CDIN	Enables the Sterling Connect:Direct Inbound protocol
FG_CDOUT	Enables the Sterling Connect:Direct Outbound protocol
FG_CD	Enables the Sterling Connect:Direct Inbound and Outbound protocol
FG_FTPIN	Enables the FTP Inbound protocol
FG_FTPOUT	Enables the FTP Outbound protocol
FG_FTP	Enables the FTP Inbound and Outbound protocol
FG_SFTPIN	Enables the SFTP Inbound protocol
FG_SFTPOUT	Enables the SFTP Outbound protocol
FG_SFTP	Enables the SFTP Inbound and Outbound protocol

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 filegateway_eventcodes.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.

Event Code	Name	Description	Default Subscription Settings
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.
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

Event Code	Name	Description	Default Subscription Settings
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
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.

Event Code	Name	Description	Default Subscription Settings
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.
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 provided 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: <ul style="list-style-type: none"> • subscription - available for subscription to notifications • producer - producers can see in events list and receive notifications • consumer - consumers can see in 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 SFGEventCodes.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*.

Migrate Events After Applying Sterling File Gateway 2.1 Build 5100

About this task

Sterling File Gateway 2.1 Build 5100 introduces event framework enhancements to support additional search fields and route details. For users upgrading to Build 5100, results on the Advanced Search page for arrived files processed prior to the upgrade will be affected. Searches using any or all of the following fields will not have the expected results:

- Template Name (Route section)
- Facts (Route section)
- Delivered Filename (Delivery section)
- Mailbox Path (Arrived File and Delivery sections)

An optional script is available to migrate the events from the old database tables to the new tables. After running the script, the Advanced Search parameters will work correctly for pre-upgrade and post-upgrade arrived files.

The script can be run while Sterling File Gateway is running, but it may result in performance degradation. To avoid degradation, schedule the script to run when the system is not running time-critical messages.

To convert pre-upgrade event information:

Procedure

1. In the <install_dir>/<tp_imports> directory, locate the script:
migrate_fg_events.sh
2. Use the parameter -q to inquire how many rows are eligible for migration. Use the parameter -h to display help information.
3. For a database with fewer than 100,000 events, run the script in SQL mode. The rows are updated at the end of the script. SQL mode is the default mode and migrates events using SQL joins in one large transaction. It is the fastest mode of migration. If you quit the migration activity mid-way, no events are migrated.
4. For larger databases, or if the SQL mode returns an error, run in batch mode. The batch size can be specified. The default is 500 rows per batch. The script converts the most recently written rows first. This method is slower, but you can stop and restart the script in batch mode.

Note: Activity records are purged, by default, after two weeks. Your lifespan setting may be set to a different length. See *Change Purge Settings*. Activity that has been purged is not available to be converted by the script.

Sterling File Gateway: Specific Recommendations Checklist

Sterling File Gateway is installed on an instance of Sterling B2B Integrator, and shares many of the resources with the latter, including:

- Communication Adapters
- Business Processes
- Security Services
- Perimeter Services
- Encryption
- Decryption
- Account Management

You should, therefore, tune your Sterling B2B Integrator installation first, and then perform the Sterling File Gateway-specific tuning and troubleshooting tasks. Be aware that the changes you make to Sterling File Gateway can also affect the performance of Sterling B2B Integrator.

Note: Do not edit the properties files. Make all the changes in the customer_overrides.properties file. For example, to change the **pgpCmdLine2svcname** property, enter the following line in the customer_overrides.properties file:

```
filegateway.pgpCmdLine2svcname=CUSTOM
```

In this line, replace **CUSTOM** with the name of your Command Line 2 adapter. For more information about the customer_overrides.properties file, See *Using Property Files* in the Sterling B2B Integrator 5.1 online library.

The following table describes some of the key parameters that must be configured to optimize Sterling File Gateway performance.

In the following table, the Development and Production column indicates whether the recommendations are Recommended (R), Critical (C), or Not Applicable (NA) in the development and production environments.

Recommendation	Development and Production	Comments
<p>Increase the value of Sterling File Gateway.</p> <p>Property: fgRouteConcurrentSessionLimit</p>	R for both	<p>Number of Sterling File Gateway services that can be run concurrently. The services are split into two groups, and each group has this value as the limit. Therefore, the total number of services that can run concurrently is equal to the value for this property multiplied by two. Set this to a value that is higher than the sum of business process threads in queues 4 and 6 (where Sterling File Gateway services run).</p> <p>Default value: 8 (Maximum: 64)</p>
<p>If you are processing very large files, increase the probe values to avoid timeout conditions.</p> <p>Property:</p> <ul style="list-style-type: none"> • filegateway.bpCompletionProbes.2 • filegateway.bpCompletionSleepMsec.2 	R for both	<p>Timeouts and sleep intervals that control the period for which Sterling File Gateway waits for each of the sub-business process it invokes. The timeouts and sleep intervals control the timeouts when a business process is executed synchronously during routing. The types of business processes that run during routing are consumer identification and PGP processing. Setting the values for these properties also enables one set of relatively quick probes, followed by a second set of slower probes. The first set will be reactive, but consumes more processor capacity. The second set will be activated for longer-running processes and will consume less processor capacity.</p> <p>First, probe 120 times, with 100 milliseconds between each probe, for a total of 12 seconds.</p> <p>Default value:</p> <ul style="list-style-type: none"> • bpCompletionProbes.1=120 • bpCompletionSleepMsec.1=100 <p>Then, probe 600 times with 2000 milliseconds between each probe, for a total of 1200 seconds (20 minutes).</p> <p>Default value:</p> <ul style="list-style-type: none"> • bpCompletionProbes.2=600 • bpCompletionSleepMsec.2=2000
<p>If you have a high volume of PGP traffic, you can improve your performance by specifying a group for the file gateway.</p> <p>Property: pgpCmdline2svcname</p>	R for both	<p>The name of the Command Line 2 adapter to be used for PGP packaging and unpackaging. You can override this property in the customer_overrides.properties file if a custom Command Line 2 adapter is used for PGP operations. You can also specify an adapter group name to balance the outbound PGP sessions load across multiple adapter instances.</p> <p>Default value:</p> <p>pgpCmdline2svcname=PGPCmdlineService</p>

Recommendation	Development and Production	Comments
<p>If you have very large files that will be processed by PGP, increase the value of the file gateway.</p> <p>Property: fgRoutePGPCmdLineSocketTimeout</p>	R for both	<p>Timeout value, in milliseconds, for PGP package and unpackage operations invoked by Sterling File Gateway.</p> <p>Default value: 240000 milliseconds (4 minutes)</p>
<p>If you have high volumes of FTP traffic, you can improve your performance by specifying a group.</p> <p>Property: filegateway.ftpClientAdapterName</p>	R for both	<p>The FTP Client Adapter instance or service group that the FileGatewayDeliverFTP business process will use. You can override this property in the customer_overrides.properties file to use a custom FTP Client Adapter instance to contact trading partners. You can also specify an adapter group name to balance the outbound FTP sessions load across multiple adapter instances.</p> <p>Default value: ftpClientAdapterName=FTPClientAdapter</p>
<p>Decrease the value of evaluation frequency.</p> <p>Property:</p> <ul style="list-style-type: none"> • MailboxEvaluateAllAutomaticRules <p>or</p> <ul style="list-style-type: none"> • MailboxEvaluateAllAutomaticRulesSubMin 	R for both	<p>You can enable either MailboxEvaluateAllAutomaticRules or MailboxEvaluateAllAutomaticRulesSubMin.</p> <p>MailboxEvaluateAllAutomaticRulesSubMin verifies the presence of routable messages once every 10 seconds, and can be edited for other intervals of less than one minute by modifying the MailboxEvaluateAllAutomaticRulesSubMin business process.</p>
<p>Suppress Duplicate Messages</p> <p>Property: mailbox.disallowDuplicateMessages=true</p>	R for both	Prevents duplicate messages from using system resources.
<p>Increase the number of steps a business process must complete prior to returning to the queue.</p> <p>Property: noapp.AE_ExecuteCycle.#</p>	R for both	<p>Number of steps involved in the completion of a business process before the business process returns to the queue. Higher values will accelerate individual business process execution, while lower values will provide smoother multitasking capabilities. Interactive use favors a lower number of steps, while batch processing favors a higher number of steps. The value of noapp.AE_ExecuteCycle.# can be different for each queue. # indicates the queue number.</p> <p>When a business process has one service to begin a protocol session and another service to use the protocol session, a very low AE_ExecuteCycle may lead many business processes to be in the queue, with only the first service running. This may result in many protocol sessions accumulating in an open state, and session limits being met sooner than is necessary.</p>

Recommendation	Development and Production	Comments
<p>Increase the time period that a business process can use a thread, before releasing it to be used for another business process.</p> <p>Property: noapp.AE_ExecuteCycleTime.#</p>	R for both	<p>Maximum time period, in milliseconds, for which a business process can use a thread before releasing it for use by another business process. This value will override the value set for AE_ExecuteCycle. Tuning the value for this property ensures that a series of unusually slow steps will not tie up a thread completely. This value can be different for each queue. .# indicates the queue number. A value that is too low may result in the accumulation of more sessions than are recommended.</p>
<p>Increase the number of concurrent threads.</p> <p>Property: noapp.MaxThreads</p>	R for both	<p>Total number of concurrent threads that Sterling File Gateway is allowed to use. This value is the total number of threads available to a workflow engine to execute business process steps. Other, nonworkflow engine threads do not come under the purview of this limit. For example, the threads set in fgRouteConcurrentSessionLimit do not come under the purview of this limit.</p>
<p>Increase the number of concurrent threads in HTTP sever adapters.</p> <p>Property: http.numOfmaxThread</p>	R for both	<p>Total number of concurrent threads for all HTTP server adapters in your Sterling Integrator installation. 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.</p>
<p>Set storage type.</p> <p>Property: filegateway_ui.storageType=file</p>	R for both	<p>File System is more efficient.</p> <p>Default value: database</p>

Configure a Load Balancer

Sterling File Gateway requires users to maintain persistent connections to operate correctly. This means that every time a user makes a request within a single session, it must be to the same server installation of Sterling File Gateway.

If you are using a load balancer to run multiple Sterling 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.

Chapter 2. Get Started

Prepare Communications Adapters for Use with Sterling File Gateway

Sterling File Gateway uses the communications adapters in Sterling B2B 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, Sterling Connect:Direct, HTTP, HTTPS, and WebDAV. Before using Sterling File Gateway to route files, configure the communications adapters in Sterling B2B Integrator.

About this task

To configure communications adapters:

Procedure

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	References
FTP, FTPS	FTP Server adapter	FTP Server Adapter
FTP, FTPS	FTP Client adapter and services	FTP Client Adapter
SSH/SFTP, SSH/SCP	SFTP Server adapter	SFTP Server Adapter
SSH/SFTP	SFTP Client adapter and services	SFTP Client Adapter
Connect:Direct	Sterling Connect:Direct Server adapter	Connect:Direct Server Adapter
PGP	Command Line Adapter 2	Command Line Adapter 2 PGP Package Service PGPUnpackage Service
HTTP, HTTPS, WebDAV (Requires extensibility. See <i>Add Custom Protocols.</i>)	HTTP Server adapter	HTTP Server Adapter
HTTP, HTTPS, WebDAV (Requires extensibility. See <i>Add Custom Protocols.</i>)	HTTP Client adapter and services	HTTP Client Adapter

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 the system business processes. Sterling File Gateway business processes run in queues 3, 4, and 6. Do not change the queue settings of the system business processes because they are configured to optimize queue usage under heavy loads. Custom business processes (used for consumer identification or layer processing) should be configured to execute on any queue except 3 or 4.

In Sterling B2B 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 B2B 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	Queue
FileGatewayDeliverFTP	Delivers files to consumers using the FTP protocol.	6
FileGatewayMailboxRoute	Gathers all mailbox messages available for routing.	4
FileGatewayMailboxRouteArrivedFile	Routes individual messages identified by FileGatewayMailboxRoute as available for routing.	3
FileGatewayRoutePGPPackageDocument	Routes PGP packaged documents.	6
FileGatewayRoutePGPUncpackageDocument	Routes PGP unpackaged documents.	6
FileGatewaySendMessage	Sends messages from File Gateway.	6

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.

About this task

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:

Procedure

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

About this task

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

Procedure

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 Sterling Connect:Direct Server adapter.
5. Select the netmap you created in the Sterling Connect:Direct Server adapter configuration. For consumers, the Sterling 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 Sterling Connect:Direct-specific parameters.

Prepare to Use PGP

About this task

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:

Procedure

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 B2B 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 B2B Integrator. Name the profile AFTPGProfile. 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 B2B Integrator.

Prepare to Use SSH/SFTP

About this task

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

Procedure

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

About this task

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:

Procedure

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 B2B 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.

Chapter 3. 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 B2B 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 B2B 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).

About this task

To enable SSO:

Procedure

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 B2B 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 vendor software integration, you must provide a custom plug-in that enables Sterling File Gateway to interface with the vendor 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 B2B Integrator using an HTTP Header. Refer to the third-party software documentation for how to do this.

Results

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.

About this task

To configure Sterling File Gateway for LDAP:

Procedure

1. Create external users in Sterling B2B Integrator.
2. For each external user created in Sterling B2B 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 B2B 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.

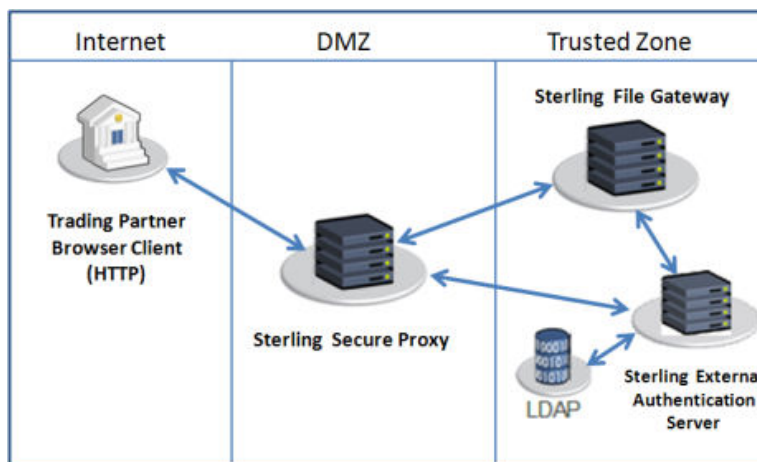
5. Restart the server for your changes to in the customer_overrides.properties file to take effect over the authentication_policy.properties file.
6. See *Using LDAP* for details about the Sterling B2B Integrator implementation.

Configure Sterling Secure Proxy

Sterling Secure Proxy can 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 to Sterling 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 that Sterling 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 to Sterling 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 multiple Sterling 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.

See *Configure a Single Sign-On Configuration between Sterling File Gateway and Sterling Secure Proxy* in the Sterling Secure Proxy online library.

Chapter 4. Extend the Capabilities

Extend the Capabilities of Sterling File Gateway

About this task

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

- Protocols
- Consumer identification policies
- Event codes
- File Layer Types

Add Custom Protocols

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

About this task

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.

Procedure

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.

Restriction: The configured business process queue is disregarded because the business process is invoked inline.

2. Use the existing `AFTEExtensions.xml` as a guide to create an `AFTEExtensionsCustomer.xml` file to describe the protocol. Do not edit the `AFTEExtensions.xml` file. The `AFTEExtensions.xml` file is located in the following directory: `<install_dir >/container/Applications/aft/WEB-INF/classes/resources/xml`.
3. Save the `AFTEExtensionsCustomer.xml` file to the same directory as `AFTEExtensions.xml`.
4. Use the existing `AFTEExtensions.properties` file as a guide to create the `AFTEExtensionsCustomer.properties` file. Do not edit the `AFTEExtensions.properties` file. The `AFTEExtensions.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`. `Select` means a drop-down list populated with possible consumer delivery protocols (if `AFTEExtension type = Protocol`) and consumer identification policies (if `AFTEExtension type = Policy`).

5. Copy the AFTExtensionsCustomer.properties file to: <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

A set of example business processes, a properties file, and an xml file are provided in your installation of Sterling File Gateway in the following directory:

<install>/samples/filegateway/protocol_extensions/

The README file provides additional information about the files. You can use these files as a model for creating the files to add these or other custom protocols.

This directory contains the following files:

- AFTExtensionsCustomer.properties
- AFTExtensionsCustomer.xml
- AFTRouteViaCEU.bpml
- AFTRouteViaHTTP.bpml
- CustomFileGatewayDeliverFTPS.bpml
- README.txt

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. If you are importing the custom protocol into Sterling File Gateway, do not use the Partner Transport record in Sterling B2B Integrator to store parameters used by Sterling File Gateway.

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

To set the route status to "failed" add the following to your business process onfault condition:

```
<assign to="FG/TransportError">true</assign>
```

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>
</AFTEExtension>
</AFTEExtensions>

```

AFTEExtensionsCustomer.properties Adding Connect:Enterprise UNIX

The following is an example AFTEExtensionsCustomer.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 AFTEExtensionsCustomer.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.

AFTEExtensionsCustomer.xml for HTTP Send

The following is an example AFTEExtensionsCustomer.xml file to add HTTP Send support to Sterling File Gateway:

```
<AFTEExtension 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>
</AFTEExtension>
```

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

AFTEExtensionsCustomer.properties for HTTP Send

The following is an AFTEExtensionsCustomer.properties file to add HTTP Send support to Sterling File Gateway:

```
#####
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 AFTEExtensionsCustomer.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-ftp-protocol" type="consumer-delivery-protocol" label="custom.ftp.protocol.label"
bp="CustomFileGatewayDeliverFTPS">
  <GROUP title="custom.ftp.instance.group1.title">
    <VARDEF varname="FTPLocation" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.ftplocation"
options="CUSTOMInternalExternal" required="yes" defaultVal="External"/>
    <VARDEF varname="HostName" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.hostname" required="yes"/>
    <VARDEF varname="Port" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.port" required="yes"/>
    <VARDEF varname="ConnectionType" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.connectiontype"
options="CUSTOMFTPConnType" required="yes"/>
    <VARDEF varname="Username" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.user" required="yes"/>
    <VARDEF varname="ObscuredRemotePasswd" type="String" htmlType="password" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.remotepasswd" required="yes"/>
    <VARDEF varname="CACertificateId" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.cacertificateid" options="CACertLysterbyID" required="no"/>
    <VARDEF varname="SystemCertificateId" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.systemcertificateid" options="SystemCertLysterbyID" required="no"/>
    <VARDEF varname="SSL" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.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.ftp.protocol.label.cipherstrength"
options="CUSTOMCipherStrength" required="yes" defaultVal="STRONG"/>
    <VARDEF varname="ClearControlChannel" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.clearcontrolchannel"
options="CUSTOMClearControlChannel" required="yes" defaultVal="NO"/>
    <VARDEF varname="BaseDirectory" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.directory" required="no"/>
    <VARDEF varname="Retries" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.retries" required="Yes" defaultVal="3"/>
    <VARDEF varname="RetryInterval" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftp.protocol.label.retryinterval" required="Yes" defaultVal="1"/>
  </GROUP>
</AFTExtension>
<OPTION name="CACertLysterbyID" class="com.sterlingcommerce.woodstock.ui.CACertLyster"/>
<OPTION name="SystemCertLysterbyID" class="com.sterlingcommerce.woodstock.ui.SystemCertLyster"/>
<OPTION name="CUSTOMInternalExternal">
  <ELE value="Internal" displayname="custom.internal"/>
  <ELE value="External" displayname="custom.external"/>
</OPTION>
<OPTION name="CUSTOMFTPConnType">
  <ELE value="ACTIVE" displayname="custom.active"/>
  <ELE value="PASSIVE" displayname="custom.passive"/>
</OPTION>
<OPTION name="CUSTOMSSLMode">
```



```

<ELE value="SSL_EXPLICIT" displayname="custom.ssl_explicit"/>
<ELE value="SSL_IMPLICIT" displayname="custom.ssl_implicit"/>
</OPTION>
<OPTION name="CUSTOMCiperStrength">
<ELE value="ALL" displayname="custom.ciperhAll"/>
<ELE value="STRONG" displayname="custom.ciperhStrong"/>
<ELE value="WEAK" displayname="custom.ciperhWeak"/>
</OPTION>
<OPTION name="CUSTOMClearControlChannel">
<ELE value="YES" displayname="custom.yes"/>
<ELE value="NO" displayname="custom.no"/>
</OPTION>

```

The following is an AFTExtensionsCustomer.properties file to add FTPS support to Sterling File Gateway:

```

#####
# CUSTOM custom FTPS listening consumer
#####
custom.ftp.protocol.label=CUSTOM FTP/SSL
custom.ftp.instance.group1.title=FTP/SSL Parameters
custom.ftp.protocol.label.ftplocation=Internal or External FTP Server:
custom.ftp.protocol.label.hostname=FTP Server Host Name(or IP address):
custom.ftp.protocol.label.port=FTP Listen Port:
custom.ftp.protocol.label.connectiontype=Connection Type:
custom.ftp.protocol.label.user=User Name:
custom.ftp.protocol.label.remotepasswd=Password:
custom.ftp.protocol.label.directory=Base Directory:
custom.ftp.protocol.label.retries=Number of retries:
custom.ftp.protocol.label.retryinterval=Interval between retries (in minutes):
custom.ftp.protocol.label.cacertificateid=Partner's Self-Signed Certificate Id:
custom.ftp.protocol.label.systemcertificateid=System Certificate Id Used To
Identify Client to Server
custom.ftp.protocol.label.ssl=SSL Negotiation, Explicit or Implicit
custom.ftp.protocol.label.ciperstrength=SSL Cipher Strength
custom.ftp.protocol.label.clearcontrolchannel=Enable Clear Control Channel
#####
# CUSTOM Custom labels for OPTION Elements
#####
custom.internal=Internal
custom.external=External
custom.active=Active
custom.ssl_explicit=Explicitcustom.passive=Passive
custom.ssl_explicit=Explicit
custom.ssl_implicit=Implicit
custom.ciperhAll=ALL
custom.ciperhStrong=STRONG
custom.ciperhWeak=WEAK
custom.yes=YES
custom.no=NO

```

Add Consumer Identification Policies

About this task

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:

Procedure

1. Write a business process implementing the consumer identification policy. For example, your business process may contain a map to derive the consumer name. Make a note of the element name in ProcessData that will contain the consumer name. Configure the business process to execute on any queue except 3 or 4.
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.

About this task

To add custom event codes:

Procedure

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 `filegateway_eventcodes.properties` file for examples. Do not edit the `filegateway_eventcodes.properties` file. 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=
```

- 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 and subscribed to by the producer for this route.
 - consumer - This event can be seen and subscribed to by the consumer for this route.
 - subscription - This event can be subscribed to. For a producer or consumer to subscribe to an event, the event must have the corresponding producer or consumer permission AND the subscription permission. For a Operator to subscribe to an event, the event requires only to have the subscription permission.
- `EventNotificationEmailSubject` - This is the subject line for the email notifications when events occurs. This applies to all event codes for your system. 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.
- `EventNotificationEmailContentType` - This specifies the content type for the email notification when the event occurs. This applies to all event codes for your system. 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.

About this task

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

Procedure

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.

- 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. See [Using Property Files](#).

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

Implement AS2

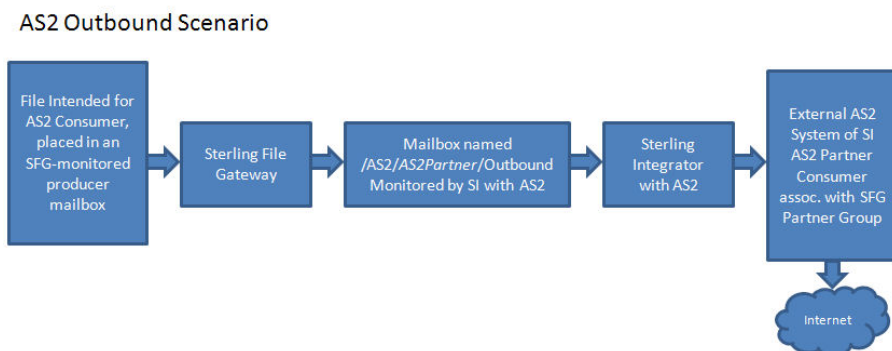
About this task

You can use Sterling File Gateway as a routing mechanism to send and receive AS2 messages through Sterling B2B Integrator. Applicability Statement 2 (AS2) EDIINT (AS2) technology is a protocol for securely exchanging data with non-repudiation of receipt over the Internet.

Sterling B2B Integrator with AS2 is a message management system enabling the exchange of a variety of documents between trading partners using secure AS2 EDIINT technology. Sterling B2B Integrator with AS2 uses the Internet as a transport mechanism, ensures privacy and security of documents exchanged, and provides a means of non-repudiation. Using AS2 with Sterling B2B Integrator and Sterling File Gateway extends your investments by sending and receiving documents and interacting with your existing processes. Basically, you put a document into a specific mailbox to send it to a specific partner and you receive documents from partners in partner-specific mailboxes.

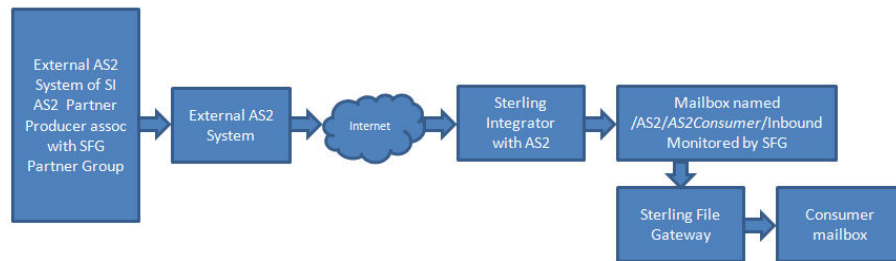
To use the features described in this topic, you must have a license for Sterling B2B Integrator with an additional license for AS2 and for Sterling File Gateway, and have them both installed.

For Sterling File Gateway to interoperate with Sterling B2B Integrator using AS2, specific mailboxes are configured as integration points. The following diagram shows the flow of outbound AS2 messages between Sterling File Gateway and other systems.



The following diagram shows the flow of inbound AS2 messages between Sterling File Gateway and other systems.

AS2 Inbound Scenario



Notice that in each of these scenarios, the mailbox path is the integration point between Sterling File Gateway and Sterling B2B Integrator. Specifying the correct mailbox paths in the routing channel templates establishes the connection between the systems.

Prerequisites

Performing this procedure requires knowledge of Sterling B2B Integrator with AS2.

You should be familiar with configuring and verifying an AS2 setup prior to configuring Sterling File Gateway with the AS2 partner.

The AS2 partner must be setup to use mailboxes instead of the file system.

An AS2 transfer from the AS2 Partner should be verified to successfully transfer from the AS2 Partner's mailbox prior to configuring Sterling File Gateway with the AS2 partner.

For more information, see *Using AS2 and the AS2 Edition* in the online library.

Use of Sterling File Gateway is not strictly limited to the selections provided in this procedure. To simplify your initial use of AS2 with Sterling File Gateway, some suggested selections are provided.

Procedure

To set up Sterling File Gateway for file transfers using AS2:

Procedure

1. From within Sterling File Gateway, select **Tools > B2B Console**.
2. In Sterling B2B Integrator, select **Trading Partners > AS2** to create an AS2 partner. For example, you may create a partner name of *AS2Partner*. You can use any valid user name that is not already in use in Sterling File Gateway. During the AS2 profile creation:
 - a. On the **Identification** page, select **Store AS2 Messages in a Mailbox**.
 - b. On the **Mailbox** page, select **Use Default Inbound/Outbound Mailboxes**. This selection will create a mailbox path of */AS2/AS2Partner/Inbound*

and

/AS2/AS2Partner/Outbound

These mailbox paths will need to be referenced in the routing channel templates.

Note: Partners created in the AS2 Edition do not belong to any Sterling File Gateway Community, and therefore cannot utilize PGP encryption, which relies on communities for key management.

3. Update the AS2 user account created during the AS2 Partner creation. In Sterling B2B Integrator, the user account in the example will be named: *AS2Partner_B2B*.
 - a. Select **Accounts** > **User Accounts**. Locate and edit the AS2 user account.
 - b. Add the *AS2Partner* user to the **File Gateway Partner Users** group.
 - c. To enable this partner to access myFileGateway, grant access to the */Inbound* and */Outbound* mailboxes listed in step 2b.
 - d. On the **User Information** screen, select the *AS2Partner* in the Identity drop-down list, and save.

Note: The AS2 partner cannot be edited from the Sterling File Gateway Community or Partner management screens and must be edited from the AS2 partner management screens in Sterling B2B Integrator.

For more information, see *Using AS2 and the AS2 Edition* in the online library.

4. Optionally, you may find it useful to create a Sterling File Gateway partner group to organize your AS2 partners. For example, create a group named *AS2 Partners*. In Sterling File Gateway, select **Participants** > **Groups** and click **Create**.
5. Add *AS2Partner* to a Sterling File Gateway group.
 - a. Select **Participants** > **Groups**. Click **Add Partners**.
 - b. Select the AS2 partner and a Sterling File Gateway Group, for example *AS2 Partners*. Click **Execute**.
6. Have the Integration Architect create a routing channel template configured to route inbound data received using AS2 or the outbound data sent to AS2.
7. Have the Route Provisioner create routing channels configured to use the AS2 routing channel templates.

Results

Partners can utilize AS2 for inbound or outbound messages.

Note: Messages received using AS2 will always have a file name of "Attachment". If you have set the following property:

```
mailbox.disallowDuplicateMessages=true
```

as recommended, messages can be overridden by subsequent messages with the same name. To avoid this, set the property to:

```
mailbox.disallowDuplicateMessages=false
```

This setting applies to all of your file transfers, not just the AS2 ones, so consider the implications before changing this property.

Note: You can track the progress of the file transfer delivery to the mailbox. In the Arrived File details, locate the event code *FG_0425*. Select the associated Dataflow

hyperlink to obtain additional details. Select the workflow ID to view details in the AS2 subsystem with details about the original document and movement to the designated mailbox.

Note: Logs for Sterling File Gateway and myFileGateway will not include information about AS2 transfers. Sterling File Gateway routes the data from one mailbox to another and does not initiate or participate in the AS2 transfer.

Chapter 5. Custom File Layer Types

About Custom File Layer Types

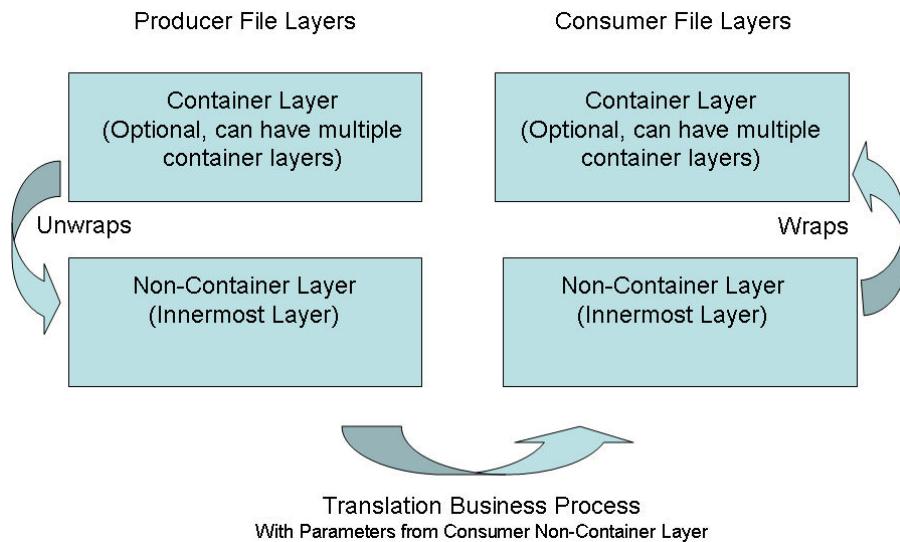
Routing channel templates use file layer types to describe producer and consumer file structures. The following file types are supported when you install:

- Container type layers - contain other container or non-container layers. For example, a PGP layer can contain a ZIP layer and a ZIP layer can contain a TEXT layer. The standard container types are:
 - ZIP
 - GZIP
 - PGP

Restriction: A zip layer can only contain multiple files if it is the outermost layer.

- Non-container type layers - or primitive, do not contain any nested layers. The standard non-container layers are:
 - Text
 - Unknown

The following graphic shows the relationship between the file layers for the producer and the consumer and the processing that Sterling File Gateway performs between each layer:



Restrictions for Custom File Layer Types

The following constraints apply to custom file layer types:

- Custom file layer types can be container or non-container types.
- A custom file layer type can be used for the producer layer, the consumer layer, or both.
- A custom container layer type must be configured with a business process that will perform the appropriate function on the container layer.

- A custom non-container layer type on the producer side may map to a custom non-container layer type on the consumer side, but a business process must be specified to perform the appropriate translation from one format to the other.
- The name provided for custom file layer types must begin with "FGC_". This indicates that table entries for the LAYER_TYPE column in the FG_P_FLR_TYPE and FG_C_FLR_TYPE tables must begin with "FGC_". The maximum length for LAYER_TYPE is 10 characters, including the "FGC_".
- You can define a maximum of 100 custom layers types, and each type can have a maximum of 10 parameters, including the required parameters.
- All parameter values for custom file layer type tables should conform to the corresponding maximum character length specified in the tables below.
- Every producer file layer type must specify the parameters in the following table for the producer file structure in the FG_P_FLR_PRM_TYPE table and FgProducerFileLayerParameterType XML element:

Ordinal Value	Parameter
0	File name pattern as regular expression
1	File name pattern group fact names, comma delimited

- Every consumer file layer type must specify the parameter in the following table for the consumer file structure in the FG_C_FLR_PRM_TYPE table and FgConsumerFileLayerParameterType XML element:

Ordinal Value	Parameter
0	File name format

- Parameters that correspond to ordinal value 0 are displayed in bold in the UI and are required. Other parameters added for custom file layer types cannot be specified to display in bold.
- You cannot can be edit or delete a file layer type if it is used in a template.

Business Processes Used for Custom File Layers

To create custom file layer types, create the business processes to perform the functions on the custom layers.

- Translation - converts a file in the producer non-container layer to a file in the consumer non-container layer
- Container layer transformation - unwraps the producer container layer to reveal the files within it
- Container layer creation - creates the consumer container layer
- Consumer identification - defines the manner in which the characteristics of the layer identify the consumer to deliver it to

Plan the mappings from your layers in the following sequence:

- Producer container
- Producer non-container
- Consumer non-container
- Consumer container

Sterling File Gateway invokes custom file layer business processes synchronously, waiting for each business process to complete before continuing with the next one. Consequently, all business processes that operate on custom file layers must:

- Complete as quickly as possible. While Sterling File Gateway waits for the business process to complete, finite resources like threads and memory are utilized. The longer the custom file layer business process waits, the longer Sterling File Gateway must wait. This use of resources reduces overall performance and throughput.
- Do not call the Sleep service or the Wait service from the business process.
- Set recovery levels to "manual". Settings of "auto recover" and "auto resume" slow down recovery after a shutdown.
- Set the business process to execute on any queue except 3 or 4.

Consumer identification business processes must also:

- Not manipulate the document, such as changing its name. While doing this may work in specific circumstances, future releases may change that behavior. What Sterling File Gateway does or does not do with the document after calling the consumer identification business process should be treated as an implementation detail subject to change.
- Not be coded to handle the case where the consumer cannot be found; if the ConsumerName element is empty or missing, Sterling File Gateway raises the appropriate event to report that the consumer could not be determined.

Container File Layer Types for Producer File Structure

To add a container file layer type for the Producer File Structure, three tables must be updated.

Table 1. FG_P_FLR_TYPE. This table specifies the new file layer type. The value provided in this table for P_FLR_TYPE_KEY will need to be repeated in the FG_P_FLR_PRM_TYPE and FG_P_FLR_TRANS tables to properly configure a custom file layer type. This table contains the following parameters:

Parameter	Example	Where in UI	Type	Max Characters
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
LAYER_TYPE	FGC_DR13D	Not visible	varchar	10
IS_CONTAINER	Y	If Y, PFS configuration requires selection of inner layer type	char	1
CONTAINS_NAME	N	Not visible	char	1
DISP_LABEL	Double Rot13 Decrypt	Not visible	varchar	255
DESCRIPTION	Double Rot13 Decrypt	File layer drop down menu	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 2. FG_P_FLR_PRM_TYPE. This table specifies the individual parameters for the new producer file layer type. Multiple entries may be made for any file layer type. At least two entries are required for the two parameters that are automatically displayed with standard producer file layer types:

- File name pattern as regular expression
- File name pattern group fact names, comma delimited. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so forth).

The FG_P_FLR_PRM_TYPE table must specify a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table.

Parameter Name	Example 1	Example 2	Where Visible in the UI	Type	Max Characters
P_FLR_PRM_TYPE_KEY	DR13D_FP_GUID	DR13D_FPF_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	DR13D_GUID	Not visible	char	24
ORDINAL	0	1	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name pattern as regular expression	File name pattern group fact names, comma delimited	PFS configuration	varchar	255
DISPLAY_TYPE	String	String	Not visible	varchar	255
DISPLAY_LABEL	File name pattern	File name pattern fact names	Not visible	varchar	255
PARAM_NAME	FILENAME_PATTERN	FILENAME_PATTERN_FACTNAMES	Not visible	varchar	255
DEFAULT_VALUE	.+	null	Not visible	varchar	255
ALLOWABLE_VALUES	null	null	Not visible	varchar	255
LOCKID	0	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	XMLMigrator	Not visible	varchar	40

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Table 3. FG_P_FLR_TRANS. This table specifies the business process that should be used to perform the work necessary to process the new producer container file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table. It takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_TRANS_KEY	SDKFJSLKFJ_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
BP_NAME	DoubleRot13Decrypt	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19

Table 3. *FG_P_FLR_TRANS* (continued). This table specifies the business process that should be used to perform the work necessary to process the new producer container file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table. It takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40
MODIFYPROGID	admin	Not visible	varchar	40

Non-Container File Layer Types for Producer File Structure

Creating a non-container file layer type is similar to creating a container file layer type, with two exceptions:

- The value for the IS_CONTAINER parameter in the FG_P_FLR_TYPE should be set to N (No).
- An entry must be made in a new table, FG_C_FLR_TRANS, instead of the FG_P_FLR_TRANS table.

To add a non-container file layer type for the Producer File Structure, three tables must be updated.

Table 4. *FG_P_FLR_TYPE*. This table specifies the new producer file layer type.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
LAYER_TYPE	FGC_BLOCK	Not visible	varchar	10
IS_CONTAINER	N	If N, PFS configuration recognizes as inner layer type	char	1
CONTAINS_NAME	N	Not visible	char	1
DISP_LABEL	Blocked Text	File layer drop down menu	varchar	255
DESCRIPTION	Blocked Text Description	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 5. FG_P_FLR_PRRM_TYPE. This table specifies the individual parameters for the new file layer type. Multiple entries may be made for any file layer type. At least two entries are required for the two parameters that are automatically displayed with standard file layer types:

- File name pattern as regular expression
- File name pattern group fact names, comma delimited. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so forth).

This table must specify a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table.

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Parameter Name	Example 1	Example 2	Where Visible in the UI	Type	Max Characters
P_FLR_PRRM_TYPE_KEY	BLOCK_FP_GUID	BLOCK_FPF_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	BLOCK_GUID	Not visible	char	24
ORDINAL	0	1	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name pattern as regular expression	File name pattern group fact names, comma delimited	PFS configuration	varchar	255
DISPLAY_TYPE	String	String	Not visible	varchar	255
DISPLAY_LABEL	File name pattern	File name pattern fact names	Not visible	varchar	255
PARAM_NAME	FILENAME_PATTERN	FILENAME_PATTERN_FACTNAMES	Not visible	varchar	255
DEFAULT_VALUE	.+	null	Not visible	varchar	255
ALLOWABLE_VALUES	null	null	Not visible	varchar	255
LOCKID	0	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	XMLMigrator	Not visible	varchar	40

Table 6. FG_C_FLR_TRANS. This table specifies the legitimate mapping between the producer and consumer inner layers. Only layers with a defined mapping can be configured in the routing channel template. It also specifies the business process that should be used to perform the work necessary to translate the producer file layer type into the corresponding consumer file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table and a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. The consumer file layer type specified is required to be a custom type.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TRANS_KEY	asdfnlsadjfs_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	24
BP_NAME	BaseMFT_Preprocessor	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19

Table 6. FG_C_FLR_TRANS (continued). This table specifies the legitimate mapping between the producer and consumer inner layers. Only layers with a defined mapping can be configured in the routing channel template. It also specifies the business process that should be used to perform the work necessary to translate the producer file layer type into the corresponding consumer file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table and a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. The consumer file layer type specified is required to be a custom type.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40
MODIFYPROGID	admin	Not visible	varchar	40

Container File Layer Types for Consumer File Structure

To add a container file layer type for the Consumer File Structure, three tables must be updated.

Table 7. FG_C_FLR_TYPE. This table specifies the new file layer type.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TYPE_KEY	DR13E_GUID	Not visible	char	24
LAYER_TYPE	FGC_DR13E	Not visible	varchar	10
IS_CONTAINER	Y	If Y, PFS configuration requires selection of inner layer type	varchar	10
DISP_LABEL	Double Rot13 Encryption	File layer drop down menu	varchar	255
DESCRIPTION	Double Rot13 Encryption Description	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 8. FG_C_FLR_PRM_TYPE. This table specifies the individual parameters for the new producer file layer type. Multiple entries may be made for any file layer type. At least one entry is required for the parameter that is automatically displayed with standard consumer file layer types, File name format. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on). This table must be provided a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table.

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_PRM_TYPE_KEY	DR13E_FF_GUID	Not visible	char	24
C_FLR_TYPE_KEY	DR13E_GUID	Not visible	char	24
ORDINAL	0	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name format	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name format	Not visible	varchar	255
PARAM_NAME	FILENAME_FORMAT	Not visible	varchar	255
DEFAULT_VALUE	\${ProducerFilename}	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 9. FG_C_FLR_TRANS. This table specifies the business process that should be used to perform the work necessary to process the new consumer file layer type. This table must be provided a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TRANS_KEY	werioweuro_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
C_FLR_TYPE_KEY	DR13E_GUID	Not visible	char	24
BP_NAME	DoubleRot13Encrypt	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40

Non-Container File Layer Types for Consumer File Structure

Creating a non-container file layer type is similar to creating a container file layer type, with two exceptions:

- The value for the IS_CONTAINER parameter in the FG_C_FLR_TYPE should be set to N (No).
- A value must be specified for the P_FLR_TYPE_KEY in the FG_C_FLR_TRANS table.

To add a non-container file layer type for the Producer File Structure, three tables must be updated.

Table 10. FG_C_FLR_TYPE. This table specifies the new consumer file layer type.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	24
LAYER_TYPE	FGC_STREAM	Not visible	varchar	10
IS_CONTAINER	N	If N, CFS configuration recognizes as inner layer type	varchar	10
DISP_LABEL	Streamed Text	File layer drop down menu	varchar	255
DESCRIPTION	Streamed Text Description	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 11. FG_C_FLR_PRM_TYPE. This table specifies the individual parameters for the new consumer file layer type. Multiple entries may be made for any file layer type. At least one entry is required for the parameter that is automatically displayed with standard consumer file layer types, File name format. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on). This table must be provided a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. This table takes the following parameters:

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_PRM_TYPE_KEY	STREAM_FF_GUID	Not visible	char	24
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	24
ORDINAL	0	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name format	PFS configuration	varchar	255

Table 11. FG_C_FLR_PRM_TYPE (continued). This table specifies the individual parameters for the new consumer file layer type. Multiple entries may be made for any file layer type. At least one entry is required for the parameter that is automatically displayed with standard consumer file layer types, File name format. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on). This table must be provided a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. This table takes the following parameters:

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name format	Not visible	varchar	255
PARAM_NAME	FILENAME_FORMAT	Not visible	varchar	255
DEFAULT_VALUE	\${ProducerFilename}	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 12. FG_C_FLR_TRANS. This table specifies the legitimate mapping between the producer and consumer inner layers. Only layers with a defined mapping can be configured in the routing channel template. It also specifies the business process that should be used to perform the work necessary to translate the producer file layer type into the corresponding consumer file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table and a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TRANS_KEY	asdfnlsadjfs_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	224
BP_NAME	BaseMFT_Preprocessor	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40
MODIFYPROGID	admin	Not visible	varchar	40

Add Custom File Layer Types

System Administrators can add custom file layer types to supplement the supplied file layer ZIP, GZIP, PGP, Text or Unknown types.

About this task

This procedure is for advanced users with a knowledge of XAPIs and APIs.

The following constraints apply to custom file layer types:

- Custom file layer types can be container or non-container types.
- A single custom file layer type can be used for the producer layer, the consumer layer, or both.
- A custom container layer type must be configured with a business process that will perform the appropriate function on the container layer.
- A custom non-container layer type on the producer side may map to a custom non-container layer type on the consumer side, but a business process must be specified to perform the appropriate translation from one format to the other.
- The name provided for custom file layer types must begin with "FGC_". This indicates that table entries for the LAYER_TYPE column in the FG_P_FLR_TYPE and FG_C_FLR_TYPE tables must begin with "FGC_". The maximum length for LAYER_TYPE is 10 characters, including the "FGC_".
- There are a maximum of 100 custom layers types, and each type can have a maximum of 10 parameters, including the required parameters.
- All parameter values for custom file layer type tables should conform to the corresponding max character length specified in the tables below.
- In the FG_P_FLR_PRM_TYPE table and FgProducerFileLayerParameterType XML element, the ordinal value "0" is reserved for the "File name pattern as regular expression" parameter and ordinal value "1" is reserved for the "File name pattern group fact names, comma delimited" parameter, both of which are required for the producer file structure in every producer file layer type.
- In the FG_C_FLR_PRM_TYPE table and FgConsumerFileLayerParameterType XML element, ordinal value "0" is reserved for the "File name format" parameter, which is required for the consumer file structure in every consumer file layer type.
- Although parameters that correspond to ordinal value "0" show up as bold in the UI and are required, the user has no control of this for any other parameters that they might add for custom file layer types.
- A file layer type can be edited or deleted only if it is not used in a template.

Before you begin, create the business processes to perform the functions, such as translation, on the custom layers. Plan the mappings from your layers in the following sequence:

- Producer container
- Producer non-container
- Consumer non-container
- Consumer container

The following procedure creates some example file layers to demonstrate the process. The specific XML will be different when you create different custom file layers. To create the example custom file layers:

Procedure

1. Create a business process named FileGatewayCustomLayerXAPI with the following BPML:

```
<process name="FileGatewayCustomLayerXAPI">
  <!--
    This business process can be used to manage File
```

```

Gateway Custom Layers.
-->
<sequence name="Begin Process">
  <operation name="XAPIServiceType">
    <participant name="XAPIService"/>
    <output message="XAPIServiceTypeInputMessage">
      <assign to="api">multiApi</assign>
      <assign to="." from="*"></assign>
    </output>
    <input message="inmsg">
      <assign to="." from="*"></assign>
    </input>
  </operation>
</sequence>
</process>

```

- Using a text editor, create a file named CreateCustomLayersSampleBPInput_EX.xml. Copy and paste the following contents into the XML file, removing any page breaks:

```

<MultiApi>
  <API Name="manageFgProducerFileLayerType">
    <!-- This API affects the first Producer File Layer Type
    and the Parameter types associated with it. See the
    FG_P_FLR_TYPE, FG_P_FLR_PRM_TYPE, and FG_P_FLR_TRANS
    table information below. -->
    <Input>
      <FgProducerFileLayerType ContainsName="N"
      Description="EX Prod Container"
      DisplayLabel="EX Prod Container " IsContainer="Y"
      LayerType="FGC_EXPCON" Lockid="0"
      ProducerFileLayerTypeKey="EXPCON_GUID">
      <FgProducerFileLayerParameterTypeList
      TotalNumberOfRecords="3">
      <FgProducerFileLayerParameterType DefaultValue="."+
      Description="File name pattern as regular expression"
      DisplayLabel="File name pattern"
      DisplayType="String" Ordinal="0"
      ParameterName="FILENAME_PATTERN"
      ProducerFileLayerParameterTypeKey="EXPCON_P1_GUID"
      ProducerFileLayerTypeKey="EXPCON_GUID" />
      <FgProducerFileLayerParameterType Description="
      "File name pattern group fact names, comma delimited"
      DisplayLabel="File name pattern fact names"
      DisplayType="String" Ordinal="1"
      ParameterName="FILENAME_PATTERN_FACTNAMES"
      ProducerFileLayerParameterTypeKey="EXPCON_P2_GUID"
      ProducerFileLayerTypeKey="EXPCON_GUID" />
      <FgProducerFileLayerParameterType
      Description="Spin value for encryption"
      DisplayLabel="Spin"
      DisplayType="String" Ordinal="2"
      ParameterName="EncryptionSpin"
      ProducerFileLayerParameterTypeKey="EXPCON_P3_GUID"
      ProducerFileLayerTypeKey="EXPCON_GUID" />
      </FgProducerFileLayerParameterTypeList>
      </FgProducerFileLayerType>
    </Input>
  </API>
  <API Name="manageFgProducerFileLayerType">
    <!-- This API affects the second Producer File Layer Type
    and the Parameter types associated with it. See the
    FG_P_FLR_TYPE, FG_P_FLR_PRM_TYPE, and FG_P_FLR_TRANS
    table information below. -->
    <Input>
      <FgProducerFileLayerType ContainsName="N"
      Description="EX Prod Non Container"
      DisplayLabel="EX Prod Non Container"

```

```

        IsContainer="N" LayerType="FGC_EXPNCN"
        ProducerFileLayerTypeKey="EXPNCN_GUID">
<FgProducerFileLayerParameterTypeList
  TotalNumberOfRecords="2">
<FgProducerFileLayerParameterType
  DefaultValue="."+
  Description="File name pattern as regular expression"
  DisplayLabel="File name pattern"
  DisplayType="String" Ordinal="0"
  ParameterName="FILENAME_PATTERN"
  ProducerFileLayerParameterTypeKey="EXPNCN_P1_GUID"
  ProducerFileLayerTypeKey="EXPNCN_GUID" />
<FgProducerFileLayerParameterType
  Description="File name pattern group fact names,
    comma delimited"
  DisplayLabel="File name pattern fact names"
  DisplayType="String" Ordinal="1"
  ParameterName="FILENAME_PATTERN_FACTNAMES"
  ProducerFileLayerParameterTypeKey="EXPNCN_P2_GUID"
  ProducerFileLayerTypeKey="EXPNCN_GUID" />
</FgProducerFileLayerParameterTypeList>
</FgProducerFileLayerType>
</Input>
</API>
<API Name="manageFgConsumerFileLayerType">
  <!-- This API affects the first Consumer File Layer Type
    (container type) and the Parameter types associated with
    it. See the FG_C_FLR_TYPE, FG_C_FLR_PRM_TYPE,
    and FG_C_FLR_TRANS
    table information below. -->
  <Input>
    <FgConsumerFileLayerType
      ConsumerFileLayerTypeKey="EXCCON_GUID"
      Description="EX Con Container"
      DisplayLabel="EX Con Container"
      IsContainer="Y" LayerType="FGC_EXCCON">
    <FgConsumerFileLayerParameterTypeList
      TotalNumberOfRecords="2">
    <FgConsumerFileLayerParameterType
      ConsumerFileLayerParameterTypeKey="EXCCON_P1_GUID"
      ConsumerFileLayerTypeKey="EXCCON_GUID"
      DefaultValue="{ProducerFilename}"
      Description="File name format"
      DisplayLabel="File name format"
      DisplayType="String" Ordinal="0"
      ParameterName="FILENAME_FORMAT" />
    <FgConsumerFileLayerParameterType
      ConsumerFileLayerParameterTypeKey="EXCCON_P2_GUID"
      ConsumerFileLayerTypeKey="EXCCON_GUID"
      DefaultValue="3" Description="Encryption Charm"
      DisplayLabel="Encryption Charm"
      DisplayType="String" Ordinal="1"
      ParameterName="EncryptionCharm" />
    </FgConsumerFileLayerParameterTypeList>
    </FgConsumerFileLayerType>
  </Input>
</API>
<API Name="manageFgConsumerFileLayerType">
  <!-- This API affects the second Consumer File Layer Type
    (non-container type) and the Parameter types associated
    with it. See the FG_C_FLR_TYPE, FG_C_FLR_PRM_TYPE, and
    FG_C_FLR_TRANS table information below.
    -->
  <Input>
    <FgConsumerFileLayerType
      ConsumerFileLayerTypeKey="EXCNCN_GUID"
      Description="EX Con Non-Container"

```

```

        DisplayLabel="EX Con Non-Container"
        IsContainer="N" LayerType="FGC_EXCNCN">
<FgConsumerFileLayerParameterTypeList
    TotalNumberOfRecords="1">
    <FgConsumerFileLayerParameterType
        ConsumerFileLayerParameterTypeKey="EXCNCN_P1_GUID"
        ConsumerFileLayerTypeKey="EXCNCN_GUID"
        DefaultValue="{ProducerFilename}"
        Description="File name format"
        DisplayLabel="File name format"
        DisplayType="String" Ordinal="0"
        ParameterName="FILENAME_FORMAT" />
    </FgConsumerFileLayerParameterTypeList>
</FgConsumerFileLayerType>
</Input>
</API>
<API Name="manageFgConsumerFileLayerTranslation">
    <Input>
        <FgConsumerFileLayerTranslation
            BusinessProcessName="CustomBP3"
            ConsumerFileLayerTranslationKey=
                "EXCTRAN1_GUID"
            ConsumerFileLayerTypeKey="EXCCON_GUID"
            ProducerFileLayerTypeKey="EXPNCN_GUID" />
        </Input>
    </API>
<API Name="manageFgConsumerFileLayerTranslation">
    <Input>
        <FgConsumerFileLayerTranslation
            BusinessProcessName="CustomBP1"
            ConsumerFileLayerTranslationKey=
                "EXCTRAN2_GUID"
            ConsumerFileLayerTypeKey="EXCCON_GUID"
            ProducerFileLayerTypeKey="" />
        </Input>
    </API>
<API Name="manageFgProducerFileLayerTranslation">
    <Input>
        <FgProducerFileLayerTranslation
            BusinessProcessName="CustomBP2"
            ProducerFileLayerTypeKey="EXPCON_GUID"
            ProducerFileLayerTranslationKey="EXPTRAN1_GUID" />
        </Input>
    </API>
</MultiApi>

```

Container File Layer Types for Producer File Structure

To add a container file layer type for the Producer File Structure, three tables must be updated.

Table 1 - FG_P_FLR_TYPE - This table specifies the new file layer type. The value provided in this table for P_FLR_TYPE_KEY will need to be repeated in the FG_P_FLR_PRM_TYPE and FG_P_FLR_TRANS tables to properly configure a custom file layer type. This table contains the following parameters:

Parameter	Example	Where in UI	Type	Max Characters
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
LAYER_TYPE	FGC_DR13D	Not visible	varchar	10
IS_CONTAINER	Y	If Y, PFS configuration requires selection of inner layer type	char	1

Parameter	Example	Where in UI	Type	Max Characters
CONTAINS_NAME	N	Not visible	char	1
DISP_LABEL	Double Rot13 Decrypt	Not visible	varchar	255
DESCRIPTION	Double Rot13 Decrypt	File layer drop down menu	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 2 - FG_P_FLR_PRM_TYPE – This table specifies the individual parameters for the new producer file layer type. Multiple entries may be made for any file layer type. At least two entries are required for the two parameters that are automatically displayed with standard producer file layer types:

- File name pattern as regular expression
- File name pattern group fact names, comma delimited. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on).

This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table. This table takes the following parameters:

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

File Layer Type Parameter #1

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_PRM_TYPE_KEY	DR13D_FP_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
ORDINAL	0	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name pattern as regular expression	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name pattern	Not visible	varchar	255
PARAM_NAME	FILENAME_PATTERN	Not visible	varchar	255
DEFAULT_VALUE	.+	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40

File Layer Type Parameter #1

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

File Layer Type Parameter #2

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_PRM_TYPE_KEY	DR13D_FPF_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
ORDINAL	1	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name pattern group fact names, comma delimited	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name pattern fact names	Not visible	varchar	255
PARAM_NAME	FILENAME_PATTERN_FACTNAMES	Not visible	varchar	255
DEFAULT_VALUE	null	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 3 - FG_P_FLR_TRANS – This table specifies the business process that should be used to perform the work necessary to process the new producer container file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table. It takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_TRANS_KEY	SDKFJSLKFJ_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
BP_NAME	DoubleRot13Decrypt	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40
MODIFYPROGID	admin	Not visible	varchar	40

Non-Container File Layer Types for Producer File Structure

Creating a non-container file layer type is similar to creating a container file layer type, with two exceptions:

- The value for the IS_CONTAINER parameter in the FG_P_FLR_TYPE should be set to 'N' (No).
- An entry must be made in a new table, FG_C_FLR_TRANS, instead of the FG_P_FLR_TRANS table.

To add a non-container file layer type for the Producer File Structure, three tables must be updated.

Table 1 - FG_P_FLR_TYPE – This table specifies the new producer file layer type, and takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
LAYER_TYPE	FGC_BLOCK	Not visible	varchar	10
IS_CONTAINER	N	If N, PFS configuration recognizes as inner layer type	char	1
CONTAINS_NAME	N	Not visible	char	1
DISP_LABEL	Blocked Text	File layer drop down menu	varchar	255
DESCRIPTION	Blocked Text Description	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 2 - FG_P_FLR_PRM_TYPE – This table specifies the individual parameters for the new file layer type. Multiple entries may be made for any file layer type. At least two entries are required for the two parameters that are automatically displayed with standard file layer types:

- File name pattern as regular expression
- File name pattern group fact names, comma delimited. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on).

This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table. This table takes the following parameters:

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

File Layer Type Parameter #1

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_PRM_TYPE_KEY	BLOCK_FP_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
ORDINAL	0	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name pattern as regular expression	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name pattern	Not visible	varchar	255
PARAM_NAME	FILENAME_PATTERN	Not visible	varchar	255
DEFAULT_VALUE	.+	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

File Layer Type Parameter #2

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
P_FLR_PRM_TYPE_KEY	BLOCK_FPF_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
ORDINAL	1	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name pattern group fact names, comma delimited	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name pattern fact names	Not visible	varchar	255
PARAM_NAME	FILENAME_PATTERN_FACTNAMES	Not visible	varchar	255
DEFAULT_VALUE	null	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19

File Layer Type Parameter #2

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 3 - FG_C_FLR_TRANS – This table specifies the legitimate mapping between the producer and consumer inner layers. Only layers with a defined mapping can be configured in the routing channel template. It also specifies the business process that should be used to perform the work necessary to translate the producer file layer type into the corresponding consumer file layer type.

This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table and a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. The consumer file layer type specified is required to be a custom type. The table takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TRANS_KEY	asdfnlsadjfs_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	24
BP_NAME	BaseMFT_Preprocessor	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40
MODIFYPROGID	admin	Not visible	varchar	40

Container File Layer Types for Consumer File Structure

To add a container file layer type for the Consumer File Structure, three tables must be updated.

Table 1 - FG_C_FLR_TYPE – This table specifies the new file layer type, and takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TYPE_KEY	DR13E_GUID	Not visible	char	24
LAYER_TYPE	FGC_DR13E	Not visible	varchar	10
IS_CONTAINER	Y	If Y, PFS configuration requires selection of inner layer type	varchar	10
DISP_LABEL	Double Rot13 Encryption	File layer drop down menu	varchar	255

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
DESCRIPTION	Double Rot13 Encryption Description	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 2 - FG_C_FLR_PRM_TYPE – This table specifies the individual parameters for the new producer file layer type. Multiple entries may be made for any file layer type. At least one entry is required for the parameter that is automatically displayed with standard consumer file layer types, File name format. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on). This table must be provided a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. This table takes the following parameters:

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_PRM_TYPE_KEY	DR13E_FF_GUID	Not visible	char	24
C_FLR_TYPE_KEY	DR13E_GUID	Not visible	char	24
ORDINAL	0	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name format	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name format	Not visible	varchar	255
PARAM_NAME	FILENAME_FORMAT	Not visible	varchar	255
DEFAULT_VALUE	\${ProducerFilename}	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 3 - FG_C_FLR_TRANS – This table specifies the business process that should be used to perform the work necessary to process the new consumer file layer type. This table must be provided a value for the C_FLR_TYPE_KEY

parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. It takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TRANS_KEY	werioweuro_GUID	Not visible	char	24
P_FLR_TYPE_KEY	DR13D_GUID	Not visible	char	24
C_FLR_TYPE_KEY	DR13E_GUID	Not visible	char	24
BP_NAME	DoubleRot13Encrypt	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	admin	Not visible	varchar	40
MODIFYUSERID	admin	Not visible	varchar	40
CREATEPROGID	admin	Not visible	varchar	40

Non-Container File Layer Types for Consumer File Structure

Creating a non-container file layer type is similar to creating a container file layer type, with two exceptions:

- The value for the IS_CONTAINER parameter in the FG_C_FLR_TYPE should be set to 'N' (No).
- A value must be specified for the P_FLR_TYPE_KEY in the FG_C_FLR_TRANS table.

To add a non-container file layer type for the Producer File Structure, three tables must be updated.

Table 1 - FG_C_FLR_TYPE – This table specifies the new consumer file layer type, and takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	24
LAYER_TYPE	FGC_STREAM	Not visible	varchar	10
IS_CONTAINER	N	If N, CFS configuration recognizes as inner layer type	varchar	10
DISP_LABEL	Streamed Text	File layer drop down menu	varchar	255
DESCRIPTION	Streamed Text Description	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 2 - FG_C_FLR_PRM_TYPE – This table specifies the individual parameters for the new consumer file layer type. Multiple entries may be made for any file layer type. At least one entry is required for the parameter that is automatically displayed with standard consumer file layer types, File name format. Each entry for a file layer type requires a new ordinal, increasing in increments of one. Parameters are displayed in the UI in the order indicated by the ordinal (0 is the first parameter in the UI, 1 is the second, and so on). This table must be provided a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. This table takes the following parameters:

Note: DEFAULT_VALUE and ALLOWABLE_VALUES are required to be in the table, but are not supported in the application.

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_PRM_TYPE_KEY	STREAM_FF_GUID	Not visible	char	24
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	24
ORDINAL	0	Controls order of appearance in UI for PFS configuration	int	9
DESCRIPTION	File name format	PFS configuration	varchar	255
DISPLAY_TYPE	String	Not visible	varchar	255
DISPLAY_LABEL	File name format	Not visible	varchar	255
PARAM_NAME	FILENAME_FORMAT	Not visible	varchar	255
DEFAULT_VALUE	\${ProducerFilename}	Not visible	varchar	255
ALLOWABLE_VALUES	null	Not visible	varchar	255
LOCKID	0	Not visible	int	5
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	SYSTEM	Not visible	varchar	40
MODIFYUSERID	SYSTEM	Not visible	varchar	40
CREATEPROGID	XMLMigrator	Not visible	varchar	40
MODIFYPROGID	XMLMigrator	Not visible	varchar	40

Table 3 - FG_C_FLR_TRANS – This table specifies the legitimate mapping between the producer and consumer inner layers. Only layers with a defined mapping can be configured in the routing channel template. It also specifies the business process that should be used to perform the work necessary to translate the producer file layer type into the corresponding consumer file layer type. This table must be provided a value for the P_FLR_TYPE_KEY parameter that matches the value for the P_FLR_TYPE_KEY parameter in the FG_P_FLR_TYPE table and a value for the C_FLR_TYPE_KEY parameter that matches the value for the C_FLR_TYPE_KEY parameter in the FG_C_FLR_TYPE table. It takes the following parameters:

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
C_FLR_TRANS_KEY	asdfnlsadjfs_GUID	Not visible	char	24
P_FLR_TYPE_KEY	BLOCK_GUID	Not visible	char	24
C_FLR_TYPE_KEY	STREAM_GUID	Not visible	char	224
BP_NAME	BaseMFT_Preprocessor	Not visible	varchar	255
LOCKID	0	Not visible	int	5

Parameter Name	Example	Where Visible in the UI	Type	Max Characters
CREATETS	2008-09-22 17:48:45	Not visible	datetime	19
MODIFYTS	2008-09-22 17:48:45	Not visible	datetime	19
CREATEUSERID	admin	Not visible	vchar	40
MODIFYUSERID	admin	Not visible	vchar	40
CREATEPROGID	admin	Not visible	vchar	40
MODIFYPROGID	admin	Not visible	vchar	40

3. Execute the FileGatewayCustomLayerXAPI business process, specifying CreateCustomLayersSampleBPInput_EX.xml you created in step 2 as the primary document.
4. Stop and restart IBM Sterling File Gateway.
5. Create an RCT using the custom layer types, using the ones you need. In the example XML, the following layers are used:
 - EX Prod Container - outer layer for producer
 - EX Prod Non Container - inner layer for producer
 - EX Con Container - outer layer for consumer
 - EX Con Non-Container - inner layer for consumer

Note: The parameters for the custom layers can include custom parameters. You can create up to eight custom parameters for each custom layer.

6. Now that you have completed the example, you can modify the XML file to create custom file layer types to meet your needs. For practice, substitute each occurrence of EX with your unique characters (represented in the steps as xx), or substituting any descriptive terms. For each one, specify the following:
 - Description - descriptive string for the layer type
 - DisplayLabel - this is what gets displayed in the drop-down box while creating layers
 - IsContainer - "Y" or "N"
 - LayerType - String
 - ProducerFileLayertypeKey - a unique value

Note: For a Layer, the value under "DisplayLabel" is displayed in the UI. For a parameter, the value under "Description" is displayed in the UI.

7. Substitute business processes that you write to translate one file type for another for the following business processes in the XML file:
 - CustomBP1 - If creating XX Con Container, substitute the business process you want to use for translation for CustomBP1.
 - CustomBP2 - If creating XX Prod Container, substitute the business process you want to use for translation for CustomBP2.
 - CustomBP3 - If creating XX Prod Non Container and XX Con Non Container, substitute the business process you want to use for translation for CustomBP3.
8. Save the XML file as CreateCustomLayersSampleBPInput_xx.xml.
9. Execute the FileGatewayCustomLayerXAPI business process, specifying CreateCustomLayersSampleBPInput_xx.xml as the primary document.
10. Stop and Restart IBM Sterling File Gateway.
11. Create an RCT using the custom layer types you need. In the example XML, the following layers are used:

- xx Prod Container - outer layer for producer
- xx Prod Non Container - inner layer for producer
- xx Con Container - outer layer for consumer
- xx Con Non-Container - inner layer for consumer

Note: The parameters for some of the custom layers include custom parameters with the changes you made to the labels.

Results

Note: You cannot move custom file layer types from one system to another. You must create any custom file layer types you require in each system separately.

Edit Custom File Layer Types

Integration Architects may identify revisions needed for the custom file layer types, and request the System Administrator make the changes.

About this task

This procedure is for advanced users with a knowledge of XAPIs and APIs. The java docs that support this functionality are located at http://lonely/api_javadocs, Package com.sterlingcommerce.fg.xapi.api.

To edit a custom file layer type:

Procedure

1. Open a text or XML editor.
2. Enter text to edit the custom file layer type by specifying the original primary key for the custom file layer type along with the new values for whatever he wants to change, as in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<MultiApi>
  <API Name="manageFgConsumerFileType">
    <Input>
      <FgConsumerFileType
        ConsumerFileTypeKey="DR13E_GUID"
        Description="NEW Double Rot13 Encryption Description"
        DisplayLabel="NEW Double Rot13 Encryption">
        <FgConsumerFileTypeParameterTypeList
          TotalNumberOfRecords="2">
          <FgConsumerFileTypeParameterType
            ConsumerFileTypeParameterTypeKey="DR13E_CH_GUID"
            Description="NEW Encryption Charm Description"
            DisplayLabel="NEW Encryption Charm"
            ParameterName="NewEncryptionCharm"/>
          <FgConsumerFileTypeParameterType
            ConsumerFileTypeParameterTypeKey="DR13E_FF_GUID"
            Description="NEW File name format"
            DisplayLabel="NEW File name format"/>
          </FgConsumerFileTypeParameterTypeList>
        </FgConsumerFileType>
      </Input>
    </API>
  </MultiApi>
```

3. Save the XML file to a local directory.
4. Select **Tools > B2B Console > Business Processes > Manager**.
5. Search for the FileGatewayCustomLayerXAPI business process.

6. Select **Execution Manager** to execute the FileGatewayCustomLayerXAPI business process, specifying the XML file from step 3 as the document.
7. The B2B Console executes the business process and updates the custom file layer type in the database.
8. Stop and Restart Sterling File Gateway to use the revised custom file layer types.

Add a Parameter to a Custom File Layer Type

Integration Architects may identify additional parameters needed for the custom file layer types, and request the System Administrator make the changes.

Before you begin

This procedure is for advanced users with a knowledge of XAPIs and APIs.

About this task

To add a parameter to a custom file layer type:

Procedure

1. Open a text or XML editor.
2. Enter text to add a parameter to the custom file layer type by specifying the original primary key for the custom file layer type along with the new parameter values for the file layer type, as in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<MultiApi>
<API Name="manageFgConsumerFileLayerType">
<Input>
<FgConsumerFileLayerType ConsumerFileLayerTypeKey="DR13E_GUID">
<FgConsumerFileLayerParameterTypeList>
<FgConsumerFileLayerParameterType
  ConsumerFileLayerParameterTypeKey="FLAVOR_GUID"
  Description="Encryption Flavor Description"
  DisplayLabel="Encryption Flavor"
  ParameterName="EncryptionFlavor" Ordinal="2"/>
</FgConsumerFileLayerParameterTypeList>
</FgConsumerFileLayerType>
</Input>
</API>
</MultiApi>
```

3. Save the XML file to a local directory.
4. Select **Tools > B2B Console > Business Processes > Manager**.
5. Search for the FileGatewayCustomLayerXAPI business process.
6. Select **Execution Manager** to execute the FileGatewayCustomLayerXAPI business process, specifying the XML file from step 3 as the document.
7. The B2B Console executes the business process and updates the custom file layer type in the database.
8. Stop and Restart Sterling File Gateway to use the revised custom file layer types.

Delete a Parameter from a Custom File Layer Type

Integration Architects may identify parameters no longer needed or valid for the custom file layer types, and request the System Administrator delete the parameter from the custom file layer.

Before you begin

This procedure is for advanced users with a knowledge of XAPIs and APIs.

About this task

To delete a parameter from a custom file layer:

Procedure

1. Open a text or XML editor.
2. Enter text to remove the parameter from the custom file layer type by specifying the original primary key along with the parameter value that should be removed from the file layer type, as in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<MultiApi>
<API Name="manageFgConsumerFileLayerType">
<Input>
<FgConsumerFileLayerType ConsumerFileLayerTypeKey="DR13E_GUID">
<FgConsumerFileLayerParameterTypeList>
<FgConsumerFileLayerParameterType
  ConsumerFileLayerParameterTypeKey="FLAVOR_GUID"
  Operation="Delete"/>
</FgConsumerFileLayerParameterTypeList>
</FgConsumerFileLayerType>
</Input>
</API>
</MultiApi>
```

3. Save the XML file to a local directory.
4. Select **Tools > B2B Console > Business Processes > Manager**.
5. Search for the FileGatewayCustomLayerXAPI business process.
6. Select **Execution Manager** to execute the FileGatewayCustomLayerXAPI business process, specifying the XML file from step 3 as the document.
7. The B2B Console executes the business process and updates the custom file layer type in the database.
8. Stop and Restart Sterling File Gateway to use the revised custom file layer types.

Delete a Custom File Layer Type

Integration Architects may identify custom file layer types that are no longer needed or valid, and request the System Administrator delete them.

Before you begin

This procedure is for advanced users with a knowledge of XAPIs and APIs.

About this task

To delete a custom file layer type:

Procedure

1. Open a text or XML editor.
2. Enter text to delete the custom file layer type by specifying the original primary key along with the "Delete" operation, as in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<MultiApi>
<API Name="manageFgConsumerFileLayerType">
<Input>
<FgConsumerFileLayerType ConsumerFileLayerTypeKey="DR13E_GUID"
Operation="Delete"/>
</Input>
</API>
</MultiApi>
```

3. Save the XML file to a local directory.
4. Select **Tools > B2B Console > Business Processes > Manager**.
5. Search for the FileGatewayCustomLayerXAPI business process.
6. Select **Execution Manager** to execute the FileGatewayCustomLayerXAPI business process, specifying the XML file from step 3 as the document.
7. The B2B Console executes the business process and deletes the custom file layer type in the database.
8. Stop and Restart Sterling File Gateway.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2013. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2013.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Index

C

checklist
 Sterling File Gateway 31

F

FGConsecFailedAttempts 24
FGLockInterval 24
fgMaxActivityRecords 24
fgMaxRoutingChannelRecords 24
fgOnboardingDefaultSessionTimeout 24
fgOnboardingDefaultUserGroupId 24
fgSkinName 24
fgWindowTitle 24
filegateway_eventcodes.properties 29
filegateway_ui.properties 24

H

help.uri 24

M

myFghelp.uri 24
myfgSkinName 24
myFgStorageType 24
myfgWindowTitle 24

N

notification.admin.url 24
notification.partner.url 24

R

reportingdirectory 24

U

userIdMinLength 24



Product Number: 5100

Printed in USA