

# **Sterling File Gateway**

---

## **System Administrator Help**

**Version 2.0**



# Contents

<b>Install and Set Up.....</b>	<b>3</b>
Create User Accounts (Build 5006 or Later).....	3
User Interface Access (Build 5006 or Later).....	4
Use Preconfigured User Groups to Assign Permissions.....	6
Migrate from Advanced File Transfer to Sterling File Gateway.....	7
About Export and Import.....	8
Migrating a Sterling File Gateway Community with Import and Export.....	8
Migrate Sterling Integrator Managed Resources.....	10
Migrate Custom Protocols.....	12
Migrate a Sterling File Gateway Community.....	14
Migrate Sterling File Gateway Configurations.....	17
Migrate Specific Sterling File Gateway Resources.....	19
Use Audit Records to Trace Administrative Actions.....	21
Set Up HTTPS for myFileGateway.....	22
Rebrand Sterling File Gateway and myFileGateway (Build 5006 or later).....	23
Change Purge Settings.....	27
filegateway.properties (Build 5006 or Later).....	28
filegateway_ui.properties (Build 5006 or Later).....	30
Sterling File Gateway: Specific Recommendations Checklist.....	32
<b>Get Started.....</b>	<b>36</b>
Prepare Communications Adapters for Use with Sterling File Gateway.....	36
Sterling File Gateway System Business Processes.....	37
Prepare to Use the Connect:Direct Protocol.....	37
Prepare to Use PGP.....	38
Prepare to Use SSH/SFTP.....	38
Exchange Information with Partners.....	39
<b>Authentication Outside Sterling File Gateway.....</b>	<b>40</b>
About Authenticating Users Outside Sterling File Gateway .....	40
Implementing Single Sign-On in Sterling File Gateway .....	40
Implementing Lightweight Directory Access Protocol (LDAP) in Sterling File Gateway .....	41
<b>Extend the Capabilities.....</b>	<b>44</b>
Extend the Capabilities of Sterling File Gateway.....	44
Add Custom Protocols.....	44
Example Custom Protocols.....	45
Add Consumer Identification Policies.....	50
Add Custom Event Codes.....	50

# Install and Set Up

---

## Create User Accounts (Build 5006 or Later)

Create user accounts in the B2B Console.

To create a user account:

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

Supply the following information about the user:

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

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

The value of # of characters must be greater than zero. To implement single sign-on, this value must match the value set in Sterling Integrator.

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

See [Managing User Accounts](#).

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

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

---

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

- fg\_sysadmin - belongs to all File Gateway groups except File Gateway Partner Users. Also belongs to Sterling Integrator Admin group.
- fg\_architect - belongs to File Gateway Integration Architects group
- fg\_provisioner - belongs to File Gateway Route Provisioners group
- fg\_operator - belongs to File Gateway Operators group

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

---

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

---

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

5. Select the permissions for the user. (Optional.) The group assignments include the standard permissions for users of each group.

6. Supply the following information for the user:

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

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

---

## User Interface Access (Build 5006 or Later)

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

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

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

Page	System Admin	Integration Architect	Route Provisioner	Operator	Partner
	view details and links to details in B2B Console. Can mark routes as reviewed or not reviewed. Can replay and redeliver.	cannot view linked details. Can mark routes as reviewed or not reviewed. Cannot replay or redeliver.	cannot view linked details. Can mark routes as reviewed or not reviewed. Cannot replay or redeliver.	details and links to details in B2B Console. Can mark routes as reviewed or not reviewed. Can replay and redeliver.	
<b>Routes &gt; Channels</b>	Can view and edit.	No access.	(Default page.) Can view and edit.	No access.	No access.
<b>Routes &gt; Templates</b>	Can view and edit.	(Default page.) Can view and edit.	No access.	No access.	No access.
<b>Participants &gt; Groups</b>	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
<b>Participants &gt; Partners</b>	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
<b>Participants &gt; Communities</b>	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
<b>Tools &gt; Reports</b>	Can view and edit.	Can view and edit.	Can view and edit.	Can view and edit.	No access.
<b>Tools &gt; Activity Snapshot</b>	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.
<b>Tools &gt; B2B Console</b>	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.
<b>Tools &gt; Logs</b>	Complete access to all logs.	No access.	No access.	Complete access to all logs.	No access.
<b>Profile &gt; Notifications</b>	Can subscribe and delete.	Can subscribe and delete.	Can subscribe and delete.	Can subscribe and delete.	No access.
<b>Profile &gt; Password</b>	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.
<b>myFileGateway &gt; Activity &gt; Upload Files</b>	No access.	No access.	No access.	No access.	(Default page.) Complete access to search, generate reports, upload files,

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

## Use Preconfigured User Groups to Assign Permissions

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

### Permissions Inherited from Groups

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

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

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

### Modify Group Permissions

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

1. Select **Tools > B2B Console**.
  2. From the Admin menu, select **Accounts > Groups**.
  3. Next to **Create a New Group**, click **Go!**
  4. Type a **Group ID** and **Group Name**. Click **Next**.
  5. On the **Assign Subgroups** page, select **BPMONITOR**. Click **Next**.
  6. On the **Assign Permissions** page, select the following:
    - **Dash AFT Theme**
    - **UI BP Manager**
    - **UI BP Monitor**
    - **UI Business Process**
    - **UI Lock Manager**
    - **UI Logs**
    - **UI Operations**
    - **UI reports**
    - **Troubleshooter**
- Click **Next**.
7. Click **Finish** and **Return**.
  8. Create or edit users, assigning them to the group you just created. These users will have access to the **Operations > Troubleshooter** menu, without access to the **Operations > System** menu and submenus.

---

## Migrate from Advanced File Transfer to Sterling File Gateway

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

To migrate partner configurations from AFT:

1. Run the following script:

<install\_dir >/tp\_import/aft2fg.sh (for UNIX) or aft2fg.cmd (for Windows)

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

The following operations are performed:

- Static and dynamic routing channels are created, based on the consumer identification policies in effect for the migrated producers.
  - AFT routing rules are replaced with a single automatic evaluation Sterling File Gateway routing rule.
  - AFT Route Business Process is disabled.
  - If a consumer identification policy of Use Map was utilized in AFT, a routing channel template is created so that the map will continue to drive the consumer identification. After conversion the name of the map used in the routing cannot be changed in Sterling File Gateway. The name of the map used is visible from the Data Session details window only.
  - PGP settings remain in effect.
  - The Advanced File Transfer tab in Sterling Integrator will be available, but limited to offer AFT Route Activity and Reporting links so that a legacy AFT user can still view old AFT data for as long as it exists in the system.
3. If the migration fails, an error message is displayed. The migration report states what changes were successfully completed. Correct the error conditions and proceed. It is safe to run the script again.
  4. The imported partners will automatically be associated with the "All Partners" partner group. You can also associate the newly migrated Partner with other Sterling File Gateway partner groups to make them work with routing channel templates that have specified these partner groups.
  5. Turn off the AFTPurgeArchiveMailboxes business process in Sterling Integrator.

---

## About Export and Import

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

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

---

## Migrating a Sterling File Gateway Community with Import and Export

You can migrate Sterling File Gateway resources from one system to another. You may have a staging system where you test new partners and other resources before you migrate them to a production system. You may also want to migrate resources from one software version to another. The Sterling File Gateway instance includes Sterling Integrator resources, Custom Protocols, and Sterling File Gateway Communities, Partners, and Configurations. The Sterling Integrator resources and Custom Protocols do not change very often, so you usually only need to migrate them once. The Communities (and all of their Partners) and Configurations can change frequently. In general, you first migrate everything in your Sterling File Gateway instance, then periodically migrate the things that change. You migrate resources using a Resource File that is an xml file



that contains resources. You can use a resource tag to create the Resource File or you can individually select the resources you want when you create the Resource File.

## Resource Files and Resource Tags

There are two types of Resource Tags:

- |                               |  |
|-------------------------------|--|
| <b>Community Resource Tag</b> | When you create a Community in Sterling File Gateway, the user interface creates a Resource Tag with that Community name in Sterling Integrator. The Community Resource Tag contains the Community and all of its Partners. This Community Resource Tag is updated and maintained by the user interface. The Resource Tag is stored in the system so you can repeatedly create Resource Files with the same set of resources in them.  |
| <b>Custom Resource Tag</b>    | A Custom Resource Tag is one that you create. You add the resources that you want to migrate to the tag and only those resources will be in the Resource File. The Custom Resource Tag is saved on the system so that you can use it repeatedly to create Resource Files with the same set of resources. However, the Custom Resource Tag is not automatically updated, you must manually modify the Custom Resource Tag to keep it current with changes you make on the system. |

## Resource Files without Resource Tags

You can create a Resource File without a Resource Tag. When creating a Resource File, the system asks you if you want to use a Resource Tag or not. If you choose to not use the Resource Tag, the system lets you create a Resource File with any resources you want, just like a Custom Resource Tag. But, the list of resources you specify for the Resource File is not stored on the system for you to use repeatedly. If you create a Resource File without a Resource Tag and want to create another Resource File with those resources in it, you must manually reselect all of the resources.

## Migrate All of the Resources in the Sterling File Gateway Instance

When you are migrating all of the resources in Sterling File Gateway for the first time, the recommended migration order is:

1. Sterling Integrator Managed Resources – You can migrate some Sterling Integrator Managed Resources at any time (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). You should consider these relationships and dependencies when you determine if you should import a Sterling Integrator Managed resource before or after you import the Sterling File Gateway Community.
2. Custom Protocols – You must migrate Custom Protocols before you migrate the Sterling File Gateway Community (and all of its Partners).
3. Sterling File Gateway Community – You must migrate the Sterling File Gateway Community (and all of its Partners) before you migrate Partner Groups (within Sterling File Gateway Configurations) and some Sterling Integrator Managed Resources such as Sterling Integrator managed partners. You must migrate the Sterling File Gateway Community (and all of its Partners) after you migrate any required Custom Protocols.
4. Sterling File Gateway Configurations – You must migrate Partner Groups, within Sterling File Gateway Configurations, after you have migrated the Sterling File Gateway Community (and all of its Partners). After you migrate the Partner Groups, you can migrate the rest of the Sterling File Gateway Configurations.

## Migrate Specific Resources from the Sterling File Gateway Instance

After you have migrated all of the resources in the Sterling File Gateway instance, you generally only have to migrate resources that have changed.

For example, if you have added Partners, you have probably added Routing Templates and Channels. You may also have created new Partner Groups. You can generally migrate these resources without having to migrate the Sterling Integrator managed resources or the Custom Protocols again.

Remember, you can not migrate specific Partners in a Community. If you add or modify Partners, you must migrate the Community that the Partners belong to. Migrating a Community will migrate all of the Community's Partners. You generally use the Community Resource Tag to migrate the Community (and all of its Partners).

## Migrate Sterling Integrator Managed Resources

Sterling Integrator customized resources used by the Sterling File Gateway Community must exist on the target system before the Sterling File Gateway Community (and all of its Partners) is migrated. You can create these resources on the target system or you can migrate these resources to the target system.

Sterling Integrator managed resources are any resources that are not created within Sterling File Gateway. 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 a Resource File that you create either with a Resource Tag that you create for repeated use or by manually creating an export file for just one use. Exporting these resources is not subject to the same constraints as the Sterling File Gateway resources.

Do NOT add the Sterling Integrator managed resources to a Sterling File Gateway Community Resource Tag.

### Related Tasks

#### Creating a Custom Resource Tag

Use this task to create a Custom Resource Tag that is used to create a Resource File to export and import resources from one system to another. Remember that a Custom Resource Tag is not automatically updated by the user interface when you change the Community's Partners. Only the Community Resource Tag is automatically updated by the user interface.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click Create New Resource Tag **Go!**.
3. Enter a name and description for the resource tag.
4. Select the resources that you want to include in the Resource File.
5. Select the resource components you want to include in the Resource File.
6. Select **Finish**.

#### Editing a Resource Tag

Use this task to change the contents of an existing Resource Tag. New Resource Files created with the edited Resource Tag will differ from previous Resource Files created with this tag.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click List Alphabetically ALL **Go!**.

3. Select **Edit** for the Resource Tag you want to edit.
4. Select the resource types that you want to include in or remove from the Resource File (for example, Communities).
5. If you are adding resources, select the individual resources you want to include in the Resource File (for example, Community 1).
6. Select **Finish**.

### **Creating a Resource File with a Resource Tag**

Use this task to create a resource file to export and import specific resources from one system to another.

This task is done on the Sterling Integrator System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Choose **XML Document** for the type of format.
4. Choose **Yes** to use a Resource Tag.
5. Select the Resource Tag you want to use.
6. Choose **Standard** export.
7. Enter and confirm a Passphrase.
8. Select **Finish**.
9. Download the export document to an accessible directory.

### **Creating a Resource File Without Using a Resource Tag**

Use this task to create a Resource File containing resources you want to export from a source system.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Select XML Document for the export file format.
4. Select **No** for **Do you wish to export resources based on a tag name?**
5. Select **Standard** for the type of export.
6. Select the resource types that you want to export (for example, Communities).
7. Select the individual resources that you want to export (for example Community 1).
8. Enter the Passphrase for the file. Confirm the Passphrase.
9. Select **Finish**

### **Importing A Resource File**

This task is done on the System Administrator's Console on the target system.

1. Select **Deployment > Resource Manager > Import/Export**.
2. Click Import Resources **Go!**.
3. Enter the File Name and Passphrase for the exported resources file and select Import All Resources.
4. If you want to, enter a Resource Tag name for the import. This is optional.
5. Select **Yes** to update the objects that already exist on the target system.
6. Select **Finish**.

## Migrate Custom Protocols

Custom Protocols are custom configurations within the system, so the migration steps and migrated resources vary between system versions and patches. You should migrate Custom Protocols before you migrate the Sterling File Gateway Community (and all its Partners) that uses the Custom Protocols. You should NOT add Custom Protocols to the Sterling File Gateway 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, redeployed, and restarted.

### Process

To migrate Custom Protocols:

1. Use the Sterling Integrator Resource Manager to create a Resource File to migrate Custom Protocols to the target system. You can create a Resource Tag for just the Custom Protocols or create an export file. The Resource File that you create must include all of the resources that the Custom Protocols use.
2. Export the Custom Protocols from the source system.
3. Import the Custom Protocols to the target system.
4. Copy the AFTExtensionsCustomer files from the source system to the target system.
5. Stop, redeploy, and restart the system.

### Copy the AFTExtensionsCustomer Files from the Source to the Target

After you have migrated the resources used by the Custom Protocols to the target system, using 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:

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

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, Redeploy, 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.

## Related Tasks

### Creating a Custom Resource Tag

Use this task to create a Custom Resource Tag that is used to create a Resource File to export and import resources from one system to another. Remember that a Custom Resource Tag is not automatically updated by the user interface when you change the Community's Partners. Only the Community Resource Tag is automatically updated by the user interface.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click Create New Resource Tag **Go!**.
3. Enter a name and description for the resource tag.
4. Select the resources that you want to include in the Resource File.
5. Select the resource components you want to include in the Resource File.
6. Select **Finish**.

### Editing a Resource Tag

Use this task to change the contents of an existing Resource Tag. New Resource Files created with the edited Resource Tag will differ from previous Resource Files created with this tag.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click List Alphabetically ALL **Go!**.
3. Select **Edit** for the Resource Tag you want to edit.
4. Select the resource types that you want to include in or remove from the Resource File (for example, Communities).
5. If you are adding resources, select the individual resources you want to include in the Resource File (for example, Community 1).
6. Select **Finish**.

### Creating a Resource File with a Resource Tag

Use this task to create a resource file to export and import specific resources from one system to another.

This task is done on the Sterling Integrator System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Choose **XML Document** for the type of format.
4. Choose **Yes** to use a Resource Tag.
5. Select the Resource Tag you want to use.
6. Choose **Standard** export.
7. Enter and confirm a Passphrase.
8. Select **Finish**.
9. Download the export document to an accessible directory.

## Creating a Resource File Without Using a Resource Tag

Use this task to create a Resource File containing resources you want to export from a source system.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Select XML Document for the export file format.
4. Select **No** for **Do you wish to export resources based on a tag name?**
5. Select **Standard** for the type of export.
6. Select the resource types that you want to export (for example, Communities).
7. Select the individual resources that you want to export (for example Community 1).
8. Enter the Passphrase for the file. Confirm the Passphrase.
9. Select **Finish**

## Importing A Resource File

This task is done on the System Administrator's Console on the target system.

1. Select **Deployment > Resource Manager > Import/Export**.
2. Click Import Resources **Go!**.
3. Enter the File Name and Passphrase for the exported resources file and select Import All Resources.
4. If you want to, enter a Resource Tag name for the import. This is optional.
5. Select **Yes** to update the objects that already exist on the target system.
6. Select **Finish**.

## Migrate a Sterling File Gateway Community

After you migrate custom protocols, you can migrate the Sterling File Gateway Community (and all of its Partners). 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"><li>• You can only export or import a single community per Resource Tag at a time.</li><li>• 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.</li><li>• You can not specify individual partners to import to the target system. You must import the entire community to which the partner belongs.</li><li>• 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.</li></ul>

Community Resource Tag	<p>The Community Resource Tag (Deployment &gt; Resource Manager &gt; Resource Tags) is managed by the Sterling File Gateway user interface when Community and Partner additions or updates are made.</p> <ul style="list-style-type: none"> <li>• Never delete the Resource Tag itself. Recreating a Sterling File Gateway Community Resource Tag requires contacting customer support.</li> <li>• Never remove resources from a Community Resource Tag. 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 Community Resource Tag on the target system.</li> <li>• You should NOT manually add resources that are not managed by Sterling File Gateway (non-Sterling File Gateway partners, mailboxes, user accounts, etc....) to the Community Resource Tag.</li> </ul> <p>If the Community 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. 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 Export

The Community export must be performed by exporting with a Community 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 Community 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 Community 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 Community 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.

## Related Tasks

### Creating a Custom Resource Tag

Use this task to create a Custom Resource Tag that is used to create a Resource File to export and import resources from one system to another. Remember that a Custom Resource Tag is not automatically updated by the user interface when you change the Community's Partners. Only the Community Resource Tag is automatically updated by the user interface.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click Create New Resource Tag **Go!**.
3. Enter a name and description for the resource tag.
4. Select the resources that you want to include in the Resource File.
5. Select the resource components you want to include in the Resource File.
6. Select **Finish**.

### Editing a Resource Tag

Use this task to change the contents of an existing Resource Tag. New Resource Files created with the edited Resource Tag will differ from previous Resource Files created with this tag.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click List Alphabetically ALL **Go!**.
3. Select **Edit** for the Resource Tag you want to edit.
4. Select the resource types that you want to include in or remove from the Resource File (for example, Communities).
5. If you are adding resources, select the individual resources you want to include in the Resource File (for example, Community 1).
6. Select **Finish**.

### Creating a Resource File with a Resource Tag

Use this task to create a resource file to export and import specific resources from one system to another.

This task is done on the Sterling Integrator System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Choose **XML Document** for the type of format.
4. Choose **Yes** to use a Resource Tag.
5. Select the Resource Tag you want to use.
6. Choose **Standard** export.



7. Enter and confirm a Passphrase.
8. Select **Finish**.
9. Download the export document to an accessible directory.

### Creating a Resource File Without Using a Resource Tag

Use this task to create a Resource File containing resources you want to export from a source system.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Select XML Document for the export file format.
4. Select **No** for **Do you wish to export resources based on a tag name?**
5. Select **Standard** for the type of export.
6. Select the resource types that you want to export (for example, Communities).
7. Select the individual resources that you want to export (for example Community 1).
8. Enter the Passphrase for the file. Confirm the Passphrase.
9. Select **Finish**

### Importing A Resource File

This task is done on the System Administrator's Console on the target system.

1. Select **Deployment > Resource Manager > Import/Export**.
2. Click Import Resources **Go!**.
3. Enter the File Name and Passphrase for the exported resources file and select Import All Resources.
4. If you want to, enter a Resource Tag name for the import. This is optional.
5. Select **Yes** to update the objects that already exist on the target system.
6. Select **Finish**.

## Migrate Sterling File Gateway Configurations

After you migrate the Custom Protocols and Sterling File Gateway Community (and all its Partners) using the Community Resource Tag, 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 the Community Resource Tag by default. You should NOT add the File Gateway Configurations to the Community Resource Tag. Configurations include:

Partner Groups	
	<p>You should migrate the Partner Groups before the other Sterling File Gateway Configurations.</p> <p>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 either by creating a new Resource Tag that contains only Partner Groups or by manually creating the Resource File without a Resource Tag.</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>
<p><b>Consumer Customer File Layers, Producer Customer File Layers, Routing Channels, Routing Channel Templates</b></p>	
	<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>

## Related Tasks

### Creating a Custom Resource Tag

Use this task to create a Custom Resource Tag that is used to create a Resource File to export and import resources from one system to another. Remember that a Custom Resource Tag is not automatically updated by the user interface when you change the Community's Partners. Only the Community Resource Tag is automatically updated by the user interface.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click **Create New Resource Tag Go!**.
3. Enter a name and description for the resource tag.
4. Select the resources that you want to include in the Resource File.
5. Select the resource components you want to include in the Resource File.
6. Select **Finish**.

### Editing a Resource Tag

Use this task to change the contents of an existing Resource Tag. New Resource Files created with the edited Resource Tag will differ from previous Resource Files created with this tag.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click **List Alphabetically ALL Go!**.
3. Select **Edit** for the Resource Tag you want to edit.
4. Select the resource types that you want to include in or remove from the Resource File (for example, Communities).
5. If you are adding resources, select the individual resources you want to include in the Resource File (for example, Community 1).
6. Select **Finish**.

## Creating a Resource File with a Resource Tag

Use this task to create a resource file to export and import specific resources from one system to another.

This task is done on the Sterling Integrator System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Choose **XML Document** for the type of format.
4. Choose **Yes** to use a Resource Tag.
5. Select the Resource Tag you want to use.
6. Choose **Standard** export.
7. Enter and confirm a Passphrase.
8. Select **Finish**.
9. Download the export document to an accessible directory.

## Creating a Resource File Without Using a Resource Tag

Use this task to create a Resource File containing resources you want to export from a source system.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Select XML Document for the export file format.
4. Select **No** for **Do you wish to export resources based on a tag name?**
5. Select **Standard** for the type of export.
6. Select the resource types that you want to export (for example, Communities).
7. Select the individual resources that you want to export (for example Community 1).
8. Enter the Passphrase for the file. Confirm the Passphrase.
9. Select **Finish**

## Importing A Resource File

This task is done on the System Administrator's Console on the target system.

1. Select **Deployment > Resource Manager > Import/Export**.
2. Click Import Resources **Go!**.
3. Enter the File Name and Passphrase for the exported resources file and select Import All Resources.
4. If you want to, enter a Resource Tag name for the import. This is optional.
5. Select **Yes** to update the objects that already exist on the target system.
6. Select **Finish**.

## Migrate Specific Sterling File Gateway Resources

After you have initially migrated your Sterling File Gateway resources to a production system, you only need to migrate resources that have changed. The resources that change most often are Partners. As Partners are added and removed, there are changes to Partner Groups as well as Routing Channel. You use the System Administrator's user interface on Sterling Integrator to select the specific resources that you want to export

from one system to another. Remember that to migrate Partners you must migrate the Community that the Partners belong to. Migrating a Community migrates all of the Partners in that Community, including Partners that may already exist on the target system.

You should migrate the resources in order:

1. Sterling File Gateway Community (and all of its Partners) with the Community Resource Tag.
2. Sterling File Gateway Partner Group Configuration, with either a Custom Resource Tag or without a Resource Tag.
3. Sterling File Gateway Configurations, such as Routing Channels with either a Customer Resource Tag or without a Resource Tag.

## Related Tasks

### Creating a Custom Resource Tag

Use this task to create a Custom Resource Tag that is used to create a Resource File to export and import resources from one system to another. Remember that a Custom Resource Tag is not automatically updated by the user interface when you change the Community's Partners. Only the Community Resource Tag is automatically updated by the user interface.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click **Create New Resource Tag Go!**.
3. Enter a name and description for the resource tag.
4. Select the resources that you want to include in the Resource File.
5. Select the resource components you want to include in the Resource File.
6. Select **Finish**.

### Editing a Resource Tag

Use this task to change the contents of an existing Resource Tag. New Resource Files created with the edited Resource Tag will differ from previous Resource Files created with this tag.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Resource Tags**.
2. Click **List Alphabetically ALL Go!**.
3. Select **Edit** for the Resource Tag you want to edit.
4. Select the resource types that you want to include in or remove from the Resource File (for example, Communities).
5. If you are adding resources, select the individual resources you want to include in the Resource File (for example, Community 1).
6. Select **Finish**.

### Creating a Resource File with a Resource Tag

Use this task to create a resource file to export and import specific resources from one system to another.

This task is done on the Sterling Integrator System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click **Export Resources Go!**.

3. Choose **XML Document** for the type of format.
4. Choose **Yes** to use a Resource Tag.
5. Select the Resource Tag you want to use.
6. Choose **Standard** export.
7. Enter and confirm a Passphrase.
8. Select **Finish**.
9. Download the export document to an accessible directory.

### Creating a Resource File Without Using a Resource Tag

Use this task to create a Resource File containing resources you want to export from a source system.

This task is done on the System Administrator's Console.

1. On the source system, select **Deployment > Resource Manager > Import/Export**.
2. Click Export Resources **Go!**.
3. Select XML Document for the export file format.
4. Select **No** for **Do you wish to export resources based on a tag name?**
5. Select **Standard** for the type of export.
6. Select the resource types that you want to export (for example, Communities).
7. Select the individual resources that you want to export (for example Community 1).
8. Enter the Passphrase for the file. Confirm the Passphrase.
9. Select **Finish**

### Importing A Resource File

This task is done on the System Administrator's Console on the target system.

1. Select **Deployment > Resource Manager > Import/Export**.
2. Click Import Resources **Go!**.
3. Enter the File Name and Passphrase for the exported resources file and select Import All Resources.
4. If you want to, enter a Resource Tag name for the import. This is optional.
5. Select **Yes** to update the objects that already exist on the target system.
6. Select **Finish**.

---

## Use Audit Records to Trace Administrative Actions

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

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

```
select * from YFS_AUDIT
```

3. Click **Execute** to view all audit records.

4. Or, select the tables and columns you are interested in, for example:

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

---

## Set Up HTTPS for myFileGateway

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

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

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

To configure *myFileGateway* to run in the DMZ:

1. Set up a perimeter server in the DMZ.
2. Configure a new Perimeter Server in Sterling Integrator.  
The port specified in the Perimeter Server configuration must *not* be the HTTP listen port (to which trading partners are expected to connect), which is specified in a subsequent stage.
3. Ensure that the remote perimeter server is running.
4. Create a new instance of the HTTP Server Adapter configuration.
  - a) Log into Sterling File Gateway as a system administrator.
  - b) Select **Tools > B2B Console**.
  - c) From the Sterling Integrator Admin menu, select **Deployment > Services > Configuration**.
  - d) Under **Create**, next to **New Service**, click **Go!**
  - e) For **Service Type**, open the List View, select **HTTP Server Adapter** and click **Save**, then **Next**.
  - f) Give the adapter a new unique name and description. If you are using a clustered environment, from the **Environment** list, select the node where the remote perimeter server is to be assigned. Click **Next**.
  - g) For the **HTTP Listen Port**, specify the port that the Partner is expected to connect to. This port must not be used by a different application on the computer that the remote perimeter server is installed on. No two HTTP Server adapter configurations can listen on the same port on the same remote perimeter server computer. The default port for Sterling File Gateway is 33, so select a different port number.
  - h) From the **Perimeter Server Name** list, select the name of the Perimeter Server (previously configured) that corresponds to the specific remote perimeter server to be used. The name is in the format *node & name*, where name is what you specified.
  - i) For **Total Business Process queue depth threshold**, enter a number of business processes to allow in queue. The value of this setting has no effect if Sterling File Gateway is the only application hosted on this HTTP Server adapter, because Sterling File Gateway does not initiate business processes.
  - j) For **Document Storage and User Authentication Required**, you can accept the default or change to match your system.
  - k) For **Use SSL**, select **Must** to implement stronger security. Click **Next**. See [Implementing SSL](#) for more information about settings for the SSL Settings page. Click **Next**.

- l) On the Services Configuration page, click **add**, type the URI /myfilegateway.
  - m) Select **War File**. Click **Next**.
  - n) **Enter the War File Path**. The *myFileGateway* War file is located at *<install dir>\SI\container\Applications\myfilegateway.war*. (For UNIX, *<install dir>/container/Applications/myfilegateway.war*.)
  - o) Click **Save**.
  - p) In the **Confirm** page, verify that all parameters are as specified.
  - q) Ensure the **Enable Service for Business Process** check box enabled.
  - r) Click **Finish**.
5. If you have access to the computer on which the remote perimeter server is running, log in to that computer and run the following command:

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

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

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

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

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

---

**Note:** If you have many concurrent users, you may find some degradation of performance. All HTTP server adapters in your Sterling Integrator installation share the setting for maximum number of threads. To increase the maximum number of threads running at the same time, edit *customer\_overrides.properties* to modify the following property:

```
http.numOfmaxThread = X
```

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

<http://www.sterlingcommerce.com/Documentation/SI50/PropFilesPage.htm> in the Sterling Integrator library for more information about changing property values.

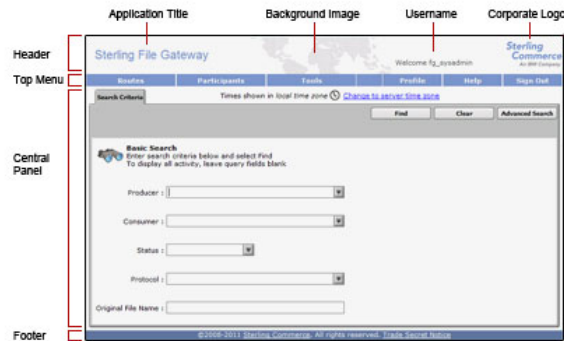
---

## Rebrand Sterling File Gateway and *myFileGateway* (Build 5006 or later)

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

skin, and restart your system. You can use the same or different skins for Sterling File Gateway and *myFileGateway*.

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



The corresponding file names are:

- Header:
  - [skin]/brandingcontent/header.txt
  - [skin]/brandingcontent/myFgHeader.txt
  - [skin]/load\_skin.js
  - [skin]/images/FGimages/brandingimages/...
- Top Menu: [skin]/skin\_styles.css
- Central Panel:
  - [skin]/skin\_styles.css
  - [skin]/load\_skin.js
  - [skin]/images/...
- Footer: [skin]/brandingcontent/footer.txt

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

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

To rebrand Sterling File Gateway:

1. Locate files in the following directories for the default skins:  
<install\_dir>/container/Applications/filegateway/isomorphic/skins/FileGateway



and

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

2. Copy and rename the “FileGateway” directory in path:

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

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

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

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

4. To change the Application Title:

- a) Open the following file:

```
[skin]/brandingcontent/header.txt
```

- b) Change line 15 to refer to your company name (padding-left: 15px" nowrap="nowrap">My Company</td> )

- c) Open [skin]/brandingcontent/myFgHeader.txt

- d) Change line 15 to refer to your company name (or another name) (padding-left: 15px" nowrap="nowrap">My Company</td> )

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

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

in customer\_overrides.properties as

```
filegateway_ui.fgWindowTitle=xxx
```

and

```
filegateway_ui.myfgWindowTitle=xxx
```

6. To change the Background Image:

- a) Create a new Background Image GIF image, 66 pixels high by 800 pixels wide and named “MastheadBkgd\_Map.gif”

- b) Place this GIF in the following directory:[skin]/images/FGimages/brandingimages/

- c) Open the following file: [skin]/brandingcontent/header.txt

- d) Change line 3 to refer to your skin’s directory where the background image (from step 5) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ MastheadBkgd\_Map.gif)

- e) Open [skin]/brandingcontent/myFgHeader.txt

- f) Change line 3 to refer to your skin’s directory where the background image (from step 5a) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ MastheadBkgd\_Map.gif)

7. To change the Corporate Logo:

- a) Create a new Corporate Logo GIF image, which should be 66 pixels high by 93 pixels wide and named “hdr\_logo.gif”

- b) Place this GIF in the following directory:[skin]/images/FGimages/brandingimages/
  - c) Open the following file: [skin]/brandingcontent/header.txt
  - d) Change line 18 to refer to your skin's directory where the corporate logo image (from step 6a) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ hdr\_logo.gif)
  - e) Open [skin]/brandingcontent/myFgHeader.txt
  - f) Change line 18 to refer to your skin's directory where the corporate logo image (from step 6a) is located (isomorphic/skins/[skin]/images/FGimages/brandingimages/ hdr\_logo.gif)
8. To change the position of the user name:
- a) Open the following file:[skin]/load\_skin.js
  - b) Change the two variables on Lines 14 and 15 to position the name label where you desire:
    - headerUserNameTop (expressed in absolute pixels from the top)
    - headerUserNameLeft (expressed as a percentage of page width, from the left side)
9. To change the headerALT, which is displayed while the header is loading:
- a) Open the following file:[skin]/load\_skin.js
  - b) Change the variable on Line 13 (headerALT) to your company name (e.g. "My Company").
10. To change the footer:
- a) Open the following file: [skin]/brandingcontent/footer.txt
  - b) Modify the first line to refer to your company name as well as the link to your corporate Web site, if desired: ...href='http://www.MyCompany.com' target='\_blank'>My Company...
11. To reference the new [skin], create or open customer\_overrides.properties in a text editor. Add the following line:
- ```
filegateway_ui.fgSkinName=[skin]
```
- where [skin] is your new skin name for Sterling File Gateway and
- ```
filegateway_ui.myfgSkinName=[skin]
```
- where [skin] is your new skin name for myFileGateway. The values for [skin] can be different for Sterling File Gateway and myFileGateway.
12. To change the header only for myFileGateway:
- Modify only the two files, header.txt and myFgHeader.txt in the new directory  
at(<install\_dir>/container/Applications/myfilegateway/isomorphic/skins/[skin]/brandingcontent
13. Run the following scripts:
- <install\_dir>/bin/hardstop.sh
  - <install\_dir >/bin/deployer.sh
  - <install\_dir >/bin/run.sh
14. Refresh your browser cache.

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

---

## Change Purge Settings

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

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

---

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

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

---

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

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

The tables in Sterling File Gateway that are purged are:

- `FG_ARRIVEDFILE`
- `FG_ROUTE`
- `FG_DELIVERY`
- `FG_EVENT_ATTR`
- `FG_ROUTE_EVENT`

To change settings for purge:

1. Open or create the following file:  
`<install_dir>/properties/customer_overrides.properties`
2. Add the following properties:  
`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](#).

## filegateway.properties (Build 5006 or Later)

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

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

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

```
filegateway.pgpCmdline2svcname=CUSTOM
```

substituting CUSTOM with the name of your Command Line 2 adapter. See [Using Property Files](#).

Property	Description
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"><li>• filegateway.ignoreFilename1=&lt;regex expression&gt;</li><li>• filegateway.ignoreFilename2=&lt;regex expression&gt;</li><li>• filegateway.ignoreFilename3=&lt;regex expression&gt;</li><li>• filegateway.ignoreFilenameex=&lt;regex expression&gt;</li></ul> <p>For example:</p> <pre>filegateway.ignoreFilename1=.[.]tmp\$</pre> <p>would have the effect of ignoring all files with an extension of .tmp.</p> <p><b>Note:</b> 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> <pre>ftpClientAdapterName=FTPClientAdapter</pre>
bpCompletionProbes.1 bpCompletionSleepMsec.1	<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</p>

Property	Description
bpCompletionProbes.2 bpCompletionSleepMsec.2	<p>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> <pre>bpCompletionProbes.1=120 and bpCompletionSleepMsec.1=100</pre> <p>Then probe 600 times with 2000 Milliseconds between, for a total of 1200 seconds (20 minutes). Default is:</p> <pre>bpCompletionProbes.2=600 and bpCompletionSleepMsec.2=2000</pre>
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> <pre>pgpCmdline2svcname=PGPCmdlineService</pre>
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>
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:</p> <pre>filegateway.fgRouteConcurrentSessionLimit=(# of limit)</pre>
required_si_build_ver	<p>The build number (version) of Sterling Integrator that Sterling File Gateway requires. This is checked at system start up. If the current version of Sterling Integrator does not equal the required_si_build_ver, a warning is issued and the system is shut down. Required. Do not change or override this property.</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>

Property	Description
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 <code>customer_overrides.properties</code>:</p> <pre>userIdMinLength.ui=(# of characters)</pre> <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 Integrator.</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>

## filegateway\_ui.properties (Build 5006 or Later)

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](#).

Property	Description
reportingdirectory	<p>Location of the reports templates.</p> <p>Default - <code>reportingdirectory=&amp;INSTALL_DIR/reporting</code></p> <p>Required. Do not modify or override.</p>
help.uri	<p>Specifies the URL for the Help used by Sterling File Gateway. Required. The default is:</p> <pre>http://help.sterlingcommerce.com/SFG20/index.jsp</pre> <p>This site is hosted by Sterling Commerce.</p>
myFghelp.uri	<p>Specifies the URL for the help used by <i>myFileGateway</i>. Required. The default is:</p> <pre>http://help.sterlingcommerce.com/mySFG20/index.jsp</pre> <p>This site is hosted by Sterling Commerce.</p>
notification.partner.url	<p>Login URL for partner users to access <i>myFileGateway</i>.</p> <p>Required. The default is:</p> <pre>notification.partner.url=http://&amp;HOST_ADDR;:&amp;PORT1;/myfilegateway</pre>

Property	Description
	<p><b>Note:</b> 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.</p>
notification.admin.url	<p>Login URL for administrative users to access Sterling File Gateway. Required. The default is:</p> <pre>notification.admin.url=http://&amp;HOST_ADDR;:&amp;PORT1/filegateway</pre> <p><b>Note:</b> The specified URL will be included in email messages generated to administrative users.</p>
fgMaxRoutingChannelRecords	<p>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.</p>
myFgStorageType	<p>Storage type to use for new documents sent through myFileGateway. Possible values are:</p> <ul style="list-style-type: none"> <li>• default - use the system default</li> <li>• db - store documents in database</li> <li>• file - store documents in file system</li> </ul> <p>The default is default.</p> <p>To change this value, use the customer_overrides.properties file. For example to set it to database:</p> <pre>filegateway_ui.myFgStorageType=db</pre>
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> <pre>fgMaxActivityRecords=1000</pre>
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> <pre>fgOnboardingDefaultSessionTimeoutInMinutes=15</pre>
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,</p>

Property	Description
	or the partner's identity is associated with a File Gateway partner group. Required. Default is File Gateway Partners Users Group.
FGConsecFailedAttempts	Number of consecutive failed login attempts that are allowed before a user is locked out of the application. Default is 0, which means users are never locked out.
FGLockInterval	Length of time, in minutes, that the lock is applied after the number of failed login attempts, FGConsecFailedAttempts, is exceeded. Default is 30.

---

## Sterling File Gateway: Specific Recommendations Checklist

Sterling File Gateway is installed on an instance of Sterling 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 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 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, refer to the *Sterling Integrator Property Files* documentation, which can be accessed from:

<http://www.sterlingcommerce.com/Documentation/SI50/PropFilesPage.htm>

---

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

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

Recommendation	Dev	Prod	Comments
Increase the value of Sterling File Gateway services that run concurrently. Property: <code>fgRouteConcurrentSessionLimit</code>	R	R	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



Recommendation	Dev	Prod	Comments
			<p>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"> <li>filegateway.bpCompletionProbes.2</li> <li>filegateway.bpCompletionSleepMsec.2</li> </ul>	R	R	<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"> <li>bpCompletionProbes.1=120</li> <li>bpCompletionSleepMsec.1=100</li> </ul> <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"> <li>bpCompletionProbes.2=600</li> <li>bpCompletionSleepMsec.2=2000</li> </ul>
<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: ppgCmdline2svcname</p>	R	R	<p>The name of the Command Line 2 adapter to be used for PGP packaging and unpackaging. You can override this property in the <code>customer_overrides.properties</code> 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: ppgCmdline2svcname=PGPCmdlineService</p>
<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	R	<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	R	<p>The FTP Client Adapter instance or service group that the FileGatewayDeliverFTP business process will use. You can override this property in the <code>customer_overrides.properties</code> file to use a custom FTP Client Adapter instance to contact trading partners. You can also specify an adapter group name to</p>

Recommendation	Dev	Prod	Comments
			balance the outbound FTP sessions load across multiple adapter instances. Default value: ftpClientAdapterName=FTPClientAdapter
Decrease the value of evaluation frequency. Property: • MailboxEvaluateAllAutomaticRules or • MailboxEvaluateAllAutomaticRulesSubMin	R	R	You can enable either MailboxEvaluateAllAutomaticRules or MailboxEvaluateAllAutomaticRulesSubMin.  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.
Suppress Duplicate Messages Property: mailbox.disallowDuplicateMessages=true	R	R	Prevents duplicate messages from using system resources.
Increase the number of steps a business process must complete prior to returning to the queue. Property: noapp.AE_ExecuteCycle.#	R	R	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.  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.
Increase the time period that a business process can use a thread, before releasing it to be used for another business process. Property: noapp.AE_ExecuteCycleTime.#	R	R	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.
Increase the number of concurrent threads. Property: noapp.MaxThreads	R	R	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.
Increase the number of concurrent threads in HTTP server adapters. Property: http.numOfmaxThread	R	R	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

Recommendation	Dev	Prod	Comments
			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.
Set storage type. Property: filegateway_ui.storage_type=file	R	R	File System is more efficient, and enables storage of much larger files.  Default value: database
Set persistence setting for business processes that perform protocol translation to System Default.	R	R	Business processes that must have persistence settings set to System Default: <ul style="list-style-type: none"> <li>• FileGatewayRoutePGPPackageDocument</li> <li>• FileGatewayRoutePGPUnpackageDocument</li> <li>• User defined business processes used for translation of custom file layers</li> </ul>

# Get Started

---

## Prepare Communications Adapters for Use with Sterling File Gateway

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

To configure communications adapters:

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

The following adapters can be used with Sterling File Gateway:

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

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

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

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

System Business Process	Function	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
FileGatewayRoutePGPUnpackageDocument	Routes PGP unpackaged documents.	6
FileGatewaySendMessage	Sends messages from File Gateway.	6

---

## Prepare to Use the Connect:Direct Protocol

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

1. Create a node by selecting **B2B Console > Deployment > Adapter Utilities > C:D Netmaps > C:D Nodes**.
2. Create a netmap by selecting **B2B Console > Deployment > Adapter Utilities > C:D Netmaps > C:D Netmaps**.
3. Create a cross-reference between the node and netmap by selecting **B2B Console > Deployment > Adapter Utilities > C:D Netmaps > C:D Netmap X-REF**.
4. Set up the Connect:Direct Server adapter.
5. Select the netmap you created in the Connect:Direct Server adapter configuration. For consumers, the Connect:Direct node that the Partner hosts is the SNODE.

6. Proceed with creating partners. When you onboard a listening consumer, specify the netmap information for the Connect:Direct specific parameters.

---

## Prepare to Use PGP

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

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

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

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

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

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

1. Install one of the supported PGP vendor's products.
2. Start a `<install_dir>/client/cmdline2/CLA2Client.jar` process on the machine that the PGP vendor's product runs on.
3. Edit the `PGPCmdlineService` (which is a configuration of the Command Line 2 adapter) in Sterling Integrator, or create a new configuration of the Command Line 2 adapter. Set the following parameters:
  - Remote Name - IP address or machine name for the machine where the PGP server is running
  - Remote Port - the port number on the PGP server machine that the `CLA2Client.jar` is listening on
  - Working directory (optional)
4. If you create a new configuration of the Command Line 2 adapter, edit the `customer_overrides.properties` file to override the default setting for the `pgpCmdline2svcname` parameter in the `filegateway.properties` file to point to the new configuration.
5. Create a PGP profile in Sterling Integrator. Name the profile `AFTPGPProfile`. The Sterling File Gateway Router can only work with a profile that has this name and cannot use any other PGP profiles defined in Sterling Integrator.

---

## Prepare to Use SSH/SFTP

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

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

---

## Exchange Information with Partners

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

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

---

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

---

# Authentication Outside Sterling File Gateway

---

## About Authenticating Users Outside Sterling File Gateway

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

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

---

## Implementing Single Sign-On in Sterling File Gateway

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

To enable SSO:

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

---

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

---

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

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



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

See [Using Single Sign-On](#).

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

```
authentication_policy.SSO_AUTHENTICATION_ENABLED=true
```

---

**Note:** Do not edit the `authentication_policy.properties` file. Make all changes in the `customer_overrides.properties` file. See [Using Property Files](#).

---

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

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

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

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

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

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

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

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

---

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

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

To configure Sterling File Gateway for LDAP:

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

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

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

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

---

**Note:** Do not edit the `authentication_policy.properties` file. Make all changes in the `customer_overrides.properties` file. See [Using Property Files](#).

---

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

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

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

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

5. Restart the server for your changes to in the `customer_overrides.properties` file to take effect over the `authentication_policy.properties` file.
6. See [Using LDAP](#) for details about the Sterling Integrator implementation.

# Extend the Capabilities

---

## Extend the Capabilities of Sterling File Gateway

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

- Protocols
- Consumer identification policies
- Event codes

---

## Add Custom Protocols

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

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

1. Write a business process that implements the custom protocol. The business process name must be unique for each custom protocol. Do not use an underscore character ( `_` ) in the name of the business process.

---

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

---

2. Use the existing `AFTExtensions.xml` as a guide to create an `AFTExtensionsCustomer.xml` file to describe the protocol. Do not edit the `AFTExtensions.xml` file.

The `AFTExtensions.xml` file is located in the following directory: `<install_dir>/container/Applications/aft/WEB-INF/classes/resources/xml`.

3. Save the `AFTExtensionsCustomer.xml` file to the same directory as `AFTExtensions.xml`.
4. Use the existing `AFTExtensions.properties` file as a guide to create the `AFTExtensionsCustomer.properties` file. Do not edit the `AFTExtensions.properties` file. The `AFTExtensions.properties` is located in the following directory:

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

---

**Note:** The user interface elements to describe the protocol are specified in the `htmlType` parameter. Valid values are `text`, `password`, `select`. When "select" is chosen for `htmlType`, the UI presents a list whose contents are derived from an "options" class. An example of an "options" class list is in the `AFTEExtensions.xml` file (the text starts with "`<OPTION name="SSHRemoteProfiles" class="`")

---

5. Save the `AFTEExtensionsCustomer.properties` file to the same directory as `AFTEExtensions.properties`, namely:

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

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

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

---

## Example Custom Protocols

### ProcessData for Business Processes Implementing Custom Protocols

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

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

Element	Description
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.

### Example Adding an Connect:Enterprise UNIX Extension

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

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

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

### AFTExtensionsCustomer.xml Adding Connect:Enterprise UNIX

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

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

### AFTExtensionsCustomer.properties Adding Connect:Enterprise UNIX

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

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

```

<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 AFT:

```

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

```



The user interface created by this example 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, AFTEExtensionsCustomer.xml could be the following:

```
:<!--Custom FTP/S Protocol for internal and external connections -->
<AFTEExtension 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.ftps.protocol.label.connectiontype" options="CUSTOMFTPCConnType"
required="yes"/>
<VARDEF varname="Username" type="String" htmlType="text" validator="ALPHANUMERIC" size="30"
maxsize="250" label="custom.ftps.protocol.label.user" required="yes"/> <VARDEF
varname="ObscuredRemotePasswd" type="String" htmlType="password" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftps.protocol.label.remotepasswd" required="yes"/> <VARDEF
varname="CACertificateId" type="String" htmlType="select" validator="ALPHANUMERIC" size="30"
maxsize="250" label="custom.ftps.protocol.label.cacertificateid" options="CACertListerbyID" required="no"/>
<VARDEF varname="SystemCertificateId" type="String" htmlType="select" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftps.protocol.label.systemcertificateid"
options="SystemCertListerbyID" required="no"/> <VARDEF varname="SSL" type="String" htmlType="select"
validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.ssl"
options="CUSTOMSSLMode" required="yes" defaultVal="SSL_EXPLICIT"/> <VARDEF
varname="CipherStrength" type="String" htmlType="select" validator="ALPHANUMERIC" size="30"
maxsize="250" label="custom.ftps.protocol.label.cipherstrength" options="CUSTOMCipherStrength"
required="yes" defaultVal="STRONG"/> <VARDEF varname="ClearControlChannel" type="String"
htmlType="select" validator="ALPHANUMERIC" size="30" maxsize="250"
label="custom.ftps.protocol.label.clearcontrolchannel" options="CUSTOMClearControlChannel" required="yes"
defaultVal="NO"/> <VARDEF varname="BaseDirectory" type="String" htmlType="text"
validator="ALPHANUMERIC" size="30" maxsize="250" label="custom.ftps.protocol.label.directory"
required="no"/> <VARDEF varname="Retries" type="String" htmlType="text" validator="ALPHANUMERIC"
size="30" maxsize="250" label="custom.ftps.protocol.label.retries" required="Yes" defaultVal="3"/> <VARDEF
varname="RetryInterval" type="String" htmlType="text" validator="ALPHANUMERIC" size="30"
maxsize="250" label="custom.ftps.protocol.label.retryinterval" required="Yes" defaultVal="1"/>

```

---

## Add Consumer Identification Policies

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

1. Write a business process implementing the consumer identification policy. For example, your business process may contain a map to derive the consumer name. 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.

To add custom event codes:

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

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

```
filegateway_eventcodes.CUST
```

The following is a basic example:

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

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

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

- **Unique Identifier** - The second 2-digit code is the unique identifier for the event within the category. 00 to 49 are successful events and 50 to 99 are error events. Error events display in red in Sterling File Gateway. You cannot exceed 99 event codes in a category. In the example, the unique identifier is `65`.
- `<EventCode>.name` - This is the name of your event. It will be shown in the subscription UI (**Profile > Notifications**) if subscriptions are enabled, and in the log. Required.

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

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

---

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

---

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

```
<operation>
  <participant name=" FileGatewayRouteEventService "/>
  <output message="Output">
    <assign to="EventCode">CUST_0265</assign>
    <assign to="ExceptionLevel">Normal</assign>
    <assign to="EventAttributes/Directory"
      from="directory/text()" append="true"/>
  </output message>
</operation>
```

```

    <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

```

# Index

## C

checklist

    Sterling File Gateway 32