Gentran Integration Suite™

Advanced File Transfer

Version 4.2

Sterling Commerce
An IBM Company

Contents

Advanced File Transfer Overview

Advanced File Transfer (AFT) provides reliable, secure, scalable B2B content distribution and Web services across business boundaries, communication modes, and document formats.

AFT is a centralized, dynamic file-exchange platform for secure transfer of files within and between organizations. It provides end-to-end visibility of file movement in an event-driven, process-oriented, highly-scalable SOA framework. These capabilities enable you to accelerate new product introduction, improve customer service, rapidly enable AFT partners, and improve operational efficiencies.

Gentran Integration Suite AFT is built on an extensible Java-based architecture that supports comprehensive Internet protocols, document-oriented as well as stream-oriented processing, advanced application integration, and tight integration with Gentran Integration Suite Mailbox, Sterling Control Center, Connect:Direct and Connect:Enterprise UNIX server products. AFT supplies a reliable and secure operational data exchange environment, implementing a policy-based automation and file transfer routing infrastructure.

The primary features of Gentran Integration Suite AFT are:

- Routing – file transfer based on policies and profiles
- Visibility – communication adapters record events for monitoring and reporting
- Notifications – subscriptions for notification of AFT events to AFT partners by email
- Onboarding – streamlines the establishment of AFT partner relationships
- Predefined business processes – reduces the number of custom business processes
- Extensible – custom features can be added to support additional situations

Licensing for AFT

A separate license is required to use the Advanced File Transfer Management menu and the AFT functionality. You must activate your license for AFT prior to using the Advanced File Transfer Management menu.

AFT Terminology

Within Gentran Integration Suite, the new Advanced File Transfer menu sets up and monitors the routing capability, referred to as the *Router*. Routing enables a *producer* of data to direct a file to a particular *consumer* of that data, where the producer and consumer are *AFT partners* of the Router. Partners can be external, such as customers or suppliers, or internal, such as business units of the entity hosting the Router.

Administrators organize partners into *AFT communities* for ease of administration and to tailor the set of protocol choices that different AFT partners are offered. Each AFT partner belongs to one and only one AFT community. You cannot alter an AFT partner’s membership in an AFT community, except by deleting that AFT partner and recreating it in a different AFT community.

The following table contains definitions of the AFT components:

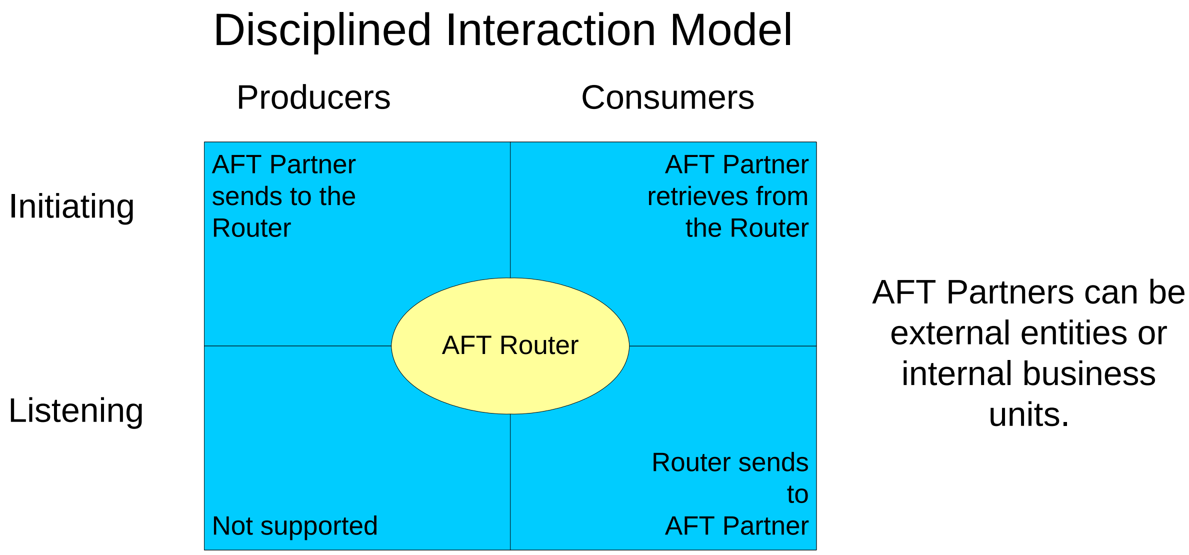
Term	Definition
AFT Community	Organization of protocols and options that are available to member AFT partners
AFT Partner	Individual profiles that belong to a community, with selected options within the structure of the community
Consumer	Recipient of data in a file transfer
Consumer identification policy	Method the producer uses to identify the consumer to receive the file transfer. An example is ‘use filename’, where the consumer is identified by the name of the transferred file.
Endpoint	Either the initiating or listening server in a file transfer
Initiator	AFT partner that takes the first action in a file transfer, *initiating* activity
Listener	AFT partner that waits for someone else to start a connection for a file transfer, *listening* for activity
Producer	Supplies the data in a file transfer
Router	Within Gentran Integration Suite, the Advanced File Transfer routing capability
Route Record	Contains the details about a route, including the endpoint, consumer, producer, start and end times, any errors that occurred, and other details.
Data flow	Aggregates in a single page all documents that are related and annotates them with correlation entries and file transfer events.
Workflow	Contains a trace of the services that were invoked in the sequence defined by the business process and the status of each.
Communication Session	Contains the authentication, authorization, file transfer, or non-file transfer records, for all communication activities that adapters participate in, whether or not data actually gets transferred.

AFT communities are distinct and separate from the EDI-centric communities created using the Community Management menu. Because AFT partners must belong to an AFT community, you must create the AFT community first. The protocol selections made during creation of the community determine the selections that display during creation of the AFT partners in that AFT community.

AFT Partner Interaction within AFT Communities

AFT partners exchange files according to the constraints of their AFT community with partners in the same community or different AFT communities. An AFT partner can *initiate* protocol connections or *listen* for connections from the Router. AFT partners are consumers or producers of data, or both. This interaction model for AFT partners within the AFT community improves scalability by constraining the allowed behaviors of the AFT partners (external partners or internal business units). These constraints also minimize the configuration necessary for onboarding each AFT partner.

This simple, but complete, interaction model is the fundamental organizing principle for Gentran Integration Suite AFT. This model enables you to quickly and easily scale your file transfer exchange communities because interaction modes are constrained. The following graphic shows the interactions enabled by the AFT Router:


Disciplined Interaction Model
Producers
Consumers
Initiating
Listening
AFT Partner sends to the Router
AFT Partner retrieves from the Router
AFT Router
Not supported
Router sends to AFT Partner
AFT Partners can be external entities or internal business units.

The roles and protocols for each type of user are:

- Initiating Producer – an AFT partner that sends data to the AFT Router, which sends the data to the consumer. The AFT partner can use any protocol that Gentran Integration Suite supports, such as FTP, FTPS, Mailbox Browser Interface (MBI), WebDAV, SSH/SFTP, SSH/SCP, Connect:Direct, or protocol that can be implemented to utilize the Mailbox Add service.
- Initiating Consumer – an AFT partner that initiates a protocol connection and retrieves files from the Inbox mailbox, sent by one or more producers. The AFT partner can use any Mailbox protocol supported by Gentran Integration Suite that enables retrieving messages from their mailbox, or a custom protocol, implemented using a business process that utilizes the Mailbox Extract service.
- Listening Consumer – an AFT partner that listens for protocol connections from the AFT Router to receive files sent by producers. The partner can use SSH/SFTP, Connect:Direct, FTP, or FTPS protocols, or a custom protocol, added using the extensibility functionality of AFT.

Consumer Identification Policies

Each producer selects a consumer identification policy which is the method the producer uses to identify the consumer to receive the file transfer. The following consumer identification policies are available when Gentran Integration Suite is installed:

- Use sub-mailbox name – each consumer the producer can send to has a corresponding sub-mailbox under the producer's mailbox. The producer is assigned a sub-mailbox for every consumer (one or more) that the producer can send to. The consumer must be created before the producer can select this policy for that consumer. The sub-mailbox that it drops the file in is the consumer that the data is sent to. An error would occur if producer BizUnit1 left a file in their root mailbox ("/BizUnit1") because the AFT Router does not know which consumer to route that data to.

For example, if partner "BizUnit1" is a producer enabled to send files to Partner22 and Partner47, the BizUnit1 mailbox directory is the following:

/BizUnit1

/BizUnit1/Partner22

/BizUnit1/Partner47

- Use filename – the filename includes the consumer's name as a prefix. The Router sends files prefixed by the consumer's name. To send the file named "xyz" to Partner37 (a consumer) this producer would drop a file named Partner37_xyz in the producer’s mailbox. The Router interprets the prefix as the name of the consumer. A producer using the filename policy is not assigned sub-mailboxes.
- Specify one consumer for always – the consumer is statically associated with the producer and not determined for each message. Data in this producer's mailbox is always routed to a specified consumer. The consumer partner must be created before the producer can select this policy for that consumer. There is no runtime determination of the consumer because this producer can only send to that particular consumer. The producer is not assigned sub-mailboxes.
- Use map to derive consumer name - contents of the transferred files are parsed using a map to determine the recipient. Use Sterling Map Editor to build your maps.

The AFT administrator can enable the Gentran Integration Suite AFT Router to offer custom choices for the consumer identification policy. See *Add Consumer Identification Policies* on page 62.

Protocols Supported in AFT

With AFT, you can exchange files with AFT partners in a wide variety of industry-standard protocols. The following protocols are supported for initiating producers and initiating consumers, when Gentran Integration Suite AFT is installed:

- FTP
- FTPS
- SSH/SFTP or SSH/SCP
- WebDAV
- Connect:Direct

The following protocols are supported in AFT for listening consumers, when Gentran Integration Suite is installed:

- SSH/SFTP
- FTP
- FTPS
- Connect:Direct

You can customize AFT to support additional protocols for listening consumers. See *Add Custom Protocols* on page 54.

Data Exchange Security

With Gentran Integration Suite AFT, you can accommodate the security requirements of many different AFT partners with the variety of security schemes supported by the AFT Router:

- PGP (signing, encryption)
- FTPS
- SSH/SFTP (or SSH/SCP for initiators)

View Ongoing Activities

On the AFT home page, a histogram provides an overview of ongoing activities involving Advanced File Transfer. The routing activity summary shows the number of file transfers over the previous 60 minutes, 24 hours, and 7 days with a status of Successful, Failed, and Reviewed. Administrators change the status of failed transfers to *Reviewed* when the problem that caused the failure is resolved or determined to not need action.

MyAFT

AFT partners can access Gentran Integration Suite AFT through an Internet browser accessing **MyAFT**. MyAFT requires a log on using a valid user account in Gentran Integration Suite, set up through the Create Partner wizard.

The MyAFT interface consists of a home page with menus that let the AFT partner search for routes, generate reports about routes, manage notifications, and view their profile information. The home page is similar to the AFT Home page in that it presents the Routing Activity Summary, displaying recent activity and status. The difference is that on MyAFT, the activity displayed is only routes the AFT partner originated as a producer or received as a consumer. In the Status field, only Successful and Failed display, because external partners cannot review and resolve issues related to failed routes.

System Requirements for MyAFT

MyAFT must be run using Internet Explorer 5.0 or later, on a server with a configuration of Gentran Integration Suite HTTP Server adapter and MBI. To ensure security of file transfers, SSL must be enabled.

The “MBI Http Server Adapter” is installed with the /myaft and /mailbox URLs. No Web application other than the Mailbox Browser Interface (which /mailbox refers to) should share an HTTP Server Adapter instance with the MyAFT application.

Manage Mailboxes

From MyAFT, AFT partners can access features that enable them to perform basic mailbox operations without having to log on separately. These features include:

- Mailbox Send (most beneficial to initiating producers)

- Route details of messages uploaded using Mailbox Send
- Mailbox Search (most beneficial to initiating consumers)
- Download of messages returned from Mailbox Search
- Change user’s password

Edit Notifications

AFT partners can subscribe to receive email notifications of any error or completion events listed in *Interpret Event Codes* on page 46. AFT partners can also edit and delete their subscriptions to notifications in MyAFT. The AFT community the partner is a member of must also enable notifications in order for the partner to receive email notification.

Field	Description
By Name	Filter the data for notifications by the name or partial name of an event. Optional.
By Type	Filter the data for notifications by the type of event. Optional.
Available Events	Event codes and descriptions for all events.
Selected Events	Use the arrows to select the events the AFT partner will receive email notification for. Optional.

MyAFT Report

The report available on MyAFT contains the route details only for routes that the AFT partner participated in. Otherwise, it is the same as the report generated at **AFT Management Menu** > **Reports** > **Generate Report**. See *Generate Report* on page 27.

Mailboxes and AFT

When an AFT partner is created, a mailbox with the same name is created for it. For example, if the partner is named "PartnerOne", the mailbox absolute path is "/PartnerOne". Do not change the absolute path of the mailbox.

The Create Partner wizard creates a Gentran Integration Suite user account for the AFT partner and makes that user's virtual root the AFT partner mailbox. Mailboxes are assigned according to the type of user as follows:

AFT Partner Type	Mailbox
Initiating consumer	List and retrieve their messages from the sub-mailbox named Inbox, under their virtual root
Listening consumer	Not assigned a mailbox

AFT Partner Type	Mailbox
Producer	One or more archive sub-mailboxes are created. Consumer sub-mailboxes are created, if the consumer identification policy for the producer is “Use sub-mailbox name”.

AFT Admin

The AFT Router depends on specific Mailbox Routing Rules, which run as the admin named aft_user. The mailbox virtual root for aft_user is “/”, which you must not change. This admin has permissions to the producer’s and the initiating consumer’s mailboxes in the directory under “/”. Do not change these permissions. This admin is required for customizing the functionality within AFT, replaying routes, and accessing the AFT logs.

Set the Mailbox Properties File

Set the following value in your mailbox.properties file:

```
disallowDuplicateMessages=true
```

This ensures that every message in a single mailbox has a unique name. It also ensures that a message and a mailbox do not have the same name. If you write a message to a mailbox and the name matches the name of a message in the mailbox, the service deletes the old message before adding the new message.

Enable Mailbox Schedule

Prior to creating AFT communities and AFT partners, you must enable either of the following schedules:

- MailboxEvaluateAllAutomaticRules (runs once per minute and can be edited for longer intervals)
- MailboxEvaluateAllAutomaticRulesSubMin (checks for the presence of routable messages once every ten seconds and can be edited for other intervals less than one minute by modifying the MailboxEvaluateAllAutomaticRulesSubMin business process)

To enable either of these schedules, from the Administration menu, select **Deployment** > **Schedules**.

AFT Extensibility

You can customize AFT to support additional functionality in the following areas:

- Protocol support – see *Add Custom Protocols* on page 54
- Consumer identification policy support – see *Add Consumer Identification Policies* on page 62
- Event codes – see *Add Custom Event Codes* on page 50

AFT Onboarding

AFT onboarding consists of the following:

- From the Admin console, set up protocol adapters as appropriate for your communities:
  - Connect:Direct Server adapter
  - FTP Server adapter
  - HTTP Server adapter
  - SFTP Server adapter
  - Command Line Adapter 2
- From the Advanced File Management menu, configure AFT.

Prepare to Use the Connect:Direct Protocol

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

1. Set up the Connect:Direct Server adapter.
2. Create an appropriate netmap entry in the Connect:Direct Server adapter. If the AFT partner is a listening consumer, the Connect:Direct node that the AFT partner hosts is the SNODE.
3. Proceed with creating the AFT community and AFT partners. When you onboard a listening consumer, specify the netmap information for the Connect:Direct specific parameters.

Prepare to Use PGP in AFT

PGP encryption is supported by the AFT Router, in combination with FTP and other protocols.

For producers, you specify in the Create Partner wizard whether files received from this producer must be PGP unpackaged. If PGP Unpackaging is required, the secret key used for decryption is specified at the AFT community level. PGP Unpackaging includes decryption if the data is encrypted and verification if the data is signed. Data from a producer with this option must not be sent as plain text.

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, but the consumer is or is not, only encrypted files can be sent. If the producer is set to No Encryption, and the consumer is set to Encryption, unencrypted files are sent and the Router encrypts them.

PGP compression can be applied for either consumers or producers.

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

1. Install one of the supported PGP vendor’s products.
2. Start a CLA2Client.jar process.

3. Modify the PGPCmdlineService in Gentran Integration Suite. Edit the PGPCmdlineService (which is a configuration of the Command Line 2 adapter).
4. You can specify the working directory in the PGPCmdlineService, but it is optional.
5. Create a PGP profile in Gentran Integration Suite. Name the profile AFTPGPProfile. The AFT Router can only work with a profile that has this name and cannot use any other PGP profiles defined in Gentran Integration Suite.

Prepare to Use SSH/SFTP

Prior to creating an AFT community with AFT 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 remote profile partner when you create the AFT listening consumer partner.
2. For SSH/SFTP or SSH/SCP producer or initiating consumer an Authorized User Key may be required. Select Trading Partner > SSH > Authorized User Key to generate a key. This key can be imported before configuration and selected when creating the AFT partner or imported during the AFT 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.

Prepare to Use Map for Consumer ID

You can use a map to determine the consumer ID from the file contents of a message. You must first do the following:

1. From the Admin menu, select **Deployment** > **Maps**.
2. Download the Map Editor and install it.
3. Create a map using Sterling Map Editor.

   In the Field Properties for a field with a name of PARTNER_ID, on the Standard Rule tab, use the following settings:

Field	Value
Please select the standard rule to use:	Update
Please select the table (or group) to update:	Process Data
Please enter the XPath to evaluate:	/ProcessData/AFTROUTECONSUMERNAME
Please select the column (or filed) to update:	XPath Result

4. Check it into Gentran Integration Suite at **Deployment** > **Maps** > **Check In Map**.

5. Name this map with a prefix of AFT (optional) to make it easier to select from the list of all available maps when you create the AFT community that will use it.
6. Create an AFT community, selecting **Use map to identify consumer** as the consumer identification policy.
7. Select the map you created for AFT.

When files are transferred within communities with this consumer identification policy, the file contents are parsed against the specified map. Files must contain the consumer name to be parsed. The file is then delivered to the consumer whose name is identified in the AFTROUTECONSUMERNAME parameter.

A working sample of this capability is available at <gis_install>/samples/aft/map_sample. This directory contains an importable file (AFTDocSample_exported.xml) that includes a basic community (one producer and one consumer). To use this sample:

1. Import the file <gis_install>/samples/aft/map_sample, using a passphrase of ‘password’.
2. Log in to MyAFT as the producer (SampleProducerUsingMap), using a password of ‘password’.
3. Upload the data file (AFTDocSamplePolicyMap.inputfile).
4. Witness the data file being routed to the consumer (SampleInitiatingConsumer1).
5. Log out of MyAFT.
6. Log in to MyAFT as the consumer (SampleInitiatingConsumer1), using a password of ‘password’.
7. Verify that the file was transferred to this mailbox.

For more information, see:

<install>/samples/aft/map_sample/README.txt.

Configure AFT

To use Advanced File Transfer:

1. Enable the Advanced File Transfer menu.
2. Add an AFT community.
3. Add AFT partners.
4. Transfer files using the protocols supported by the AFT community.

Note: All AFT community management must be performed from the Advanced File Transfer menu. Do not use the Community Management menu.

Enabling the Advanced File Transfer Menu

The Advanced File Transfer menu must be enabled. To create a new user account with AFT:

1. From the Admin menu, select **Accounts** > **User Accounts**.
2. Next to **Create a new Account**, click **Go!**

3. Complete the fields as usual, except for:
   - **Accessibility**, select **Dashboard UI**
   - **Dashboard Theme**, select **AFT**

To modify an existing user to add the AFT menu:

1. From the Gentran Integration Suite Home page, select **Manage Layout** in the upper right hand corner of the page.
2. Click **Add Pane**.
3. Type *Advanced File Transfer* for the name of the pane to add.
4. Click **Apply**.
5. Select the new hyperlink titled **Advanced File Transfer** from the Manage Layout list.
6. Select **Add Portlet**.
7. Check the box next to **Advanced File Transfer Management**.
8. Click **Apply**.
9. For **Decoration**, select **Clear Borders and Title**.
10. Click **Apply**.
11. Click **Save and Apply**.

Add Community – Profile

Field	**Description**
Community Name	A meaningful name to describe the AFT community. Required. Cannot be a name previously used in Gentran Integration Suite. Do not use spaces, tabs, or the following special characters: ! @ # % ^ * ( ) + ? , < > [ ] { } / ' \ " | ;
Secret key for PGP signing	Select from list of keys assigned to AFTPGPProfile. Required if any of the consuming partners belonging to this community require PGP signed data from the Router. See *Prepare to Use PGP in AFT* on page 13.
Secret key for PGP decryption	Select from list of keys assigned to AFTPGPProfile. Required if any of the producing partners belonging to this community send PGP encrypted data to the Router. This secret key may be the same or different from the one for PGP signing. See *Prepare to Use PGP in AFT* on page 13.

Add Community – Protocols

Field	Description
Partner Initiates Protocol Connections to Mailbox	Select to make this option available when creating AFT partners belonging to this AFT community. A unique mailbox is created for AFT partners that initiate connections. Depending on other selections, submailboxes are created for AFT partners to enable them to drop files off for routing, or pick up files routed to them.
Partner Listens for Protocol Connections	Select to enable protocols available to listening AFT partners belonging to this AFT community. When selected, the following choices are available when creating AFT partners belonging to this AFT community: ◆ FTP or FTPS ◆ Connect:Direct ◆ SSH/SFTP **Note:** If the administrator adds other protocols to the AFTExtensionsCustomer.xml file, they are also provided as choices here.
Should member partners receive notifications that they are subscribed to?	Select Yes to enable notifications for partners. Default is No. **Note:** If No is selected, AFT partners can still manage their subscriptions in MyAFT. They will not receive notifications unless Yes is selected here.

Add Community – Confirm

Field	Description
Community Information	AFT community name given to this AFT community Secret key for signing associated with the AFTPGPProfile, if present Secret key for decrypting associated with the AFTPGPProfile, if present
Protocols	Lists the protocols available as choices when AFT partners are created belonging to this AFT community
Notifications	States whether notifications are enabled or disabled for member partners.

Community Information

To view community information, a list contains AFT communities created in Gentran Integration Suite. Select an AFT community to retrieve the AFT community information.

Field	Description
Community Name	Name given to the AFT community when it was created
Secret key for PGP signing	Key associated with the AFTPGPProfile, if present

Field	Description
Secret key for PGP decryption	Key associated with the AFTPGPProfile, if present
Notifications	Checkbox is checked if notifications are enabled.

Add Partner

You must create an AFT community before you create an AFT partner. When you create an AFT partner, you select from a list of available AFT communities created in Gentran Integration Suite.

Field	Description
Community	Select from the list of all AFT communities created in Gentran Integration Suite.

Add Partner – Information

Field	Description
Partner Name	Unique and descriptive name of the AFT partner you are creating. This is the name that will be displayed in searches and reports. Can contain letters and numbers. Do not use the following characters: ! @ # % ^ * ( ) + ? , < > { } [ ] \ / ‘ “ ; Required.
Address	Address of the AFT partner. Optional.
City	City of the AFT partner. Optional.
State	State or province the AFT partner operates in. Optional.
Postal Code	Postal code for the AFT partner. Optional.
Phone	Phone contact number for the AFT partner. Required.
Country	Select from the list. Required. Default is UNITED STATES
Time Zone	Select from the list. Required. Default is (GMT-05:00) Eastern Time (US & Canada)
Email Address	E-mail address of the AFT partner. Required.

Add Partner – User Account

The AFT partner must use this user account to log in to MyAFT. This user name and password is also used to initiate connections when using a protocol that performs password authentication, such as FTP, WebDAV, or MBI. After you create the AFT partner, supply them with this information using e-mail so they have it to log into MyAFT.

Field	Description
User Name	Unique user name for the AFT partner to log in. Required. Can contain letters and numbers. Do not use the following characters: ! @ # % ^ * ( ) + ? , < > [ ] { } / ' \ " | ; It cannot be a user name that already exists in Gentran Integration Suite. This is the Gentran Integration Suite user account and is only used for log in.
Password	Password. Required. Password must be at least six characters in length.
Confirm Password	Retype the password. Required.
First Name	First name of the user representing the AFT partner. Required.
Last Name	Last name of the user representing the AFT partner. Required.

Add Partner: Partner Role

Field	Description
Partner is a Consumer of Data	Select if the partner receives data from the Router. Valid for the following partner conditions: ◆ Initiates Protocol Connections ◆ Listens for SSH/SFTP Connections ◆ Listens for FTP Connections ◆ Listens for Connect:Direct Connections ◆ Listens for FTPS Connections ◆ (Any custom protocols that have been added by the administrator) **Note:** The first partner created in a community should be a consumer or both a consumer and a producer.
Partner is a Producer of Data	Select if this AFT partner initiates protocol connections and produces data.

Add Partner – Initiate Connections Settings

Field	Description
Will *Partner* use either SSH/SFTP or SSH/SCP protocol to initiate connections?	Select Yes or No. Default is No. If Yes, you can specify if Partner will use an Authorized User Key to authenticate.

Field	Description
Will *Partner* use an Authorized User Key to authenticate?	Select Yes or No. Default is No. If Yes, you must provide the Authorized User Key.

Add Partner – Check In Authorized User Key

Field	Description
Check In Authorized User Key	Select from the list of keys that have been checked into Gentran Integration Suite, or check in a new key.
Key Name	Name for the new key that will display in the list. Required.
Public Key Filename	Browse to locate the file in your directory. Required to authenticate using an Authorized User Key.
Enabled	Check the checkbox to enable the Authorized User Key. Required to authenticate using an Authorized User Key.

Add Partner – Protocol

Select the protocol this AFT partner will use for file transfer. The choices listed here depend on the selections made when creating the AFT community that this partner will belong to and the Partner Role selected. If the AFT partner is a consumer of data and initiates connections, the protocol is Mailbox. A dedicated mailbox is created for the AFT partner.

If the AFT partner is a consumer of data and listens for connections the following protocol options are available:

- *Listen for SSH/SFTP Connections* on page 20
- *Listen for FTP Connections* on page 21
- *Listen for Connect:Direct Connections* on page 20
- *Listen for FTPS Connections* on page 22

Listen for SSH/SFTP Connections

Field	Description
SSH Remote Profile	Required.

Listen for Connect:Direct Connections

Field	Description
Local Node Name	The name of the Connect:Direct Server adapter set up to communicate with the AFT partner’s Connect:Direct node. Required.

Field	Description
Remote Node Name	The name of the Connect:Direct Server node set up to represent the AFT partner's Connect:Direct node (the netmap entry) in the Connect:Direct Server adapter. Required.
Remote User Id	The user name the partner specified for the Router to use to log in to the Connect:Direct node. Required.
Remote Password	The password the partner specified for the Router to use to log in to the Connect:Direct node. Optional.
Remote Password Confirm	Retype the password if entered above.
Remote File Name	Optional. If left blank, the name of the file delivered is the original name of the file.

Listen for FTP Connections

Field	Description
FTP Server Host Name (or IP address)	Host name or IP address for an FTP server that is listening for connections. Required.
FTP Listen Port	The port specified by the AFT partner, to which connections must be made. Required. Default is 21.
User Name	The user name that the AFT partner specified for the Router to use to log in to the FTP server. Required.
Password	Password the partner specified for the Router to use to log in to the FTP server. Required.
Confirm Password	Retype the password. Required.
Base Directory	Directory for the data to be transferred to. Required. Default is \.
Local Port Range	Range within which the local data port must be chosen, specified in the form: min-port,max-port Optional.
Control Port Range	Range within which the local control port must be chosen, specified in the form: min-port,max-port Optional.
Number of retries	Number of times the server tries to make a connection to the AFT partner's FTP server before reporting a failure. Required. Default is 3.
Interval between retries (in minutes)	Length of time the server waits between attempts to establish a connection with the AFT partner's FTP server. Required. Default is 1.
Upload file under a temporary name first?	Whether to upload using a temporary name and then rename it to the real name or to upload it under the real name. Default is No. This is useful because different FTP servers mandate different conventions for indicating the end of a successful file transfer.

Listen for FTPS Connections

Field	Description
FTPS Server Host Name (or IP address)	Host name or IP address for the FTP server that is listening for connections. Required.
FTP Listen Port	The port specified by the AFT partner, to which connections must be made. Required. Default is 21.
User Name	The user name that the AFT partner has specified for the Router to log in to the FTP server. Required.
Password	Password the partner specified for the Router to use to log in to the FTP server. Required.
Confirm Password	Retype the password. Required.
Base Directory	Directory for the data to be transferred to. Required. Default is \.
Local Port Range	Range within which the local data port must be chosen, specified in the form: min-port,max-port Optional.
Control Port Range	Range within which the local control port must be chosen, specified in the form: min-port,max-port Optional.
Number of retries	Number of times the server tries to make a connection to the AFT partner’s FTP server before reporting a failure. Required. Default is 3.
Interval between retries (in minutes)	Length of time the server waits between attempts to establish a connection with the AFT partner’s FTP server. Required. Default is 1.
Upload file under a temporary name first?	Whether to upload using a temporary name and then rename it to the real name or to upload it under the real name. Default is No. This is useful because different FTP servers mandate different conventions for indicating the end of a successful file transfer.
Encryption Strength	Set of SSL cipher suites permitted for this connection, either the set of STRONG algorithms or WEAK algorithms or ALL. Default is STRONG.
Use CCC	Whether Clear Control Channel must be enables for this connection. Default is No.
Use Implicit SSL	Whether the SSL connection is implicit or explicit. If implicit, the SSL negotiation occurs before the FTP connection is established. Default is No. **Note:** SSL client authentication is not supported. The AFT Router cannot authenticate itself using SSL client authentication when acting as the SSL client.
Select CA Certificates	One or more CA digital certificates to be used for validating the server for this connection, chosen from the list of CA certificates imported into Gentran Integration Suite. At least one is required.

Add Partner – Policy Settings

Field	Description
If Partner is a producer of data, Select Policy.	Select a policy to decide which consumer(s) get this producer's data: ◆ Use sub-mailbox name – then select from the list all consumers set up in the Router to indicate which consumers are permitted to consume this AFT partner's data. The producer must drop the file to be routed in the submailbox under their dedicated mailbox, with the name matching the name of the consumer the file is intended for. ◆ Use filename. The producer must drop the file to be routed in their dedicated mailbox with a name that has the consumer's name as a prefix, separated by an underscore from the rest of the name. For example, if consumer1 is the intended recipient of the file name xyz.txt, the filename is consumer1_xyz.txt. **Note:** This policy enables a producer to send data to any consumer identified by name. Security can be compromised if this policy is assigned to AFT partners that could send to the wrong consumers. Use this policy only with trusted AFT partners, such as internal business units. ◆ Specify one consumer for use always – then select one consumer from the list of all consumers set up in the Router, including those belonging to other AFT communities. The producer must drop the file to be routed in their dedicated mailbox. ◆ Use map to derive consumer name - transferred file is parsed using a map, which has rules for the portion of the file that identifies the recipient. The name of the recipient is extracted to ProcessData, but the file itself is not translated. Use Sterling Map Editor to build your maps. Name the map with a prefix of AFT to make it easier to locate in the list for MapName. ◆ (Any custom policies that have been added by the administrator.) The producer must drop the file to be routed in their dedicated mailbox.
MapName	Select from a list of all available maps. Required if Policy is *Use map to derive consumer name*.

PGP Settings

Field	Description
Will *Partner* send data that requires PGP processing?	Valid values are Yes and No. Default is No. This option only applies for partners that are producers of data. If Yes, data from the AFT partner must be PGP packaged. The Router unpackages the data and performs the following: ◆ If the data sent is encrypted, it is decrypted using the Router's secret PGP key. ◆ If the data sent is signed, it is verified using the AFT partner's public PGP key. Verification succeeds if that public key is present in the public key ring.

Field	Description
Does *Partner* require data to be signed by the Router?	Valid values are Yes and No. Default is No. This option only applies for AFT partners that are consumers of data. If Yes, the AFT partner expects the Router to encrypt data using the AFT partner’s public PGP key. This key is imported into the public key ring and must be identified by entering its key ID. If Yes, additional option displays: “Does *Partner* require data to be compressed by the Router?”
Does *Partner* require data to be encrypted by the Router?	Valid values are Yes and No. Default is No. This option only applies for AFT partners that are consumers of data. If Yes, provide the AFT partner’s key ID in the public key ring to be used for encryption.
Does *Partner* require data to be compressed by the Router?	Valid values are Yes and No. Default is No. This option only applies for AFT partners that are consumers of data that require data to be encrypted by the Router.
ASCII Armor	Select if the partner requires data to be ASCII armored. This option only applies for AFT partners that are consumers of data and require data to either be signed or encrypted by the Router. Default is selected.
Text Mode	Select if the partner requires data to be sent in text mode. This option only applies for AFT partners that are consumers of data and require data to either be signed or encrypted by the Router. Default is unselected.

View Partner’s Records

You can search for AFT partners in Gentran Integration Suite and view the records associated with them. Or, you can list all the AFT partners belonging to a specific AFT community, or to all the AFT communities in Gentran Integration Suite. To search for AFT partners, from the AFT Management menu, select **Partners** > **View Partners**. You can edit or delete AFT partners from this page.

Field	Description
Partner Name	Name or partial name to search for within the records matching the other search criteria.
Partner Role	Whether the AFT partner is a Producer or Consumer or both.
Community Name	Select ALL or a community name from the list.

Edit or Delete AFT Partners

To edit or delete AFT partners:

1. From the AFT Management menu, select **Partners** > **View Partners.**

2. Search for the AFT partner to edit or delete.

Field	Description
Partner Name	Name or partial name to search for within the records matching the other search criteria.
Partner Role	Whether the AFT partner is a Producer or Consumer or both.
Community Name	Select ALL or a community name from the list.

3. Select **edit** to modify the profile, user account, protocol (including partner role, connection direction, SSH settings, transport method, and signing and encryption requirements), or community membership.
4. Select delete to completely remove the AFT partner and all of its related resources.
5. A warning displays:

   Are you sure you want to delete this trading partner. Contents related to this trading partner will be lost?

   Select OK to delete the AFT partner.

Note: Do not delete AFT partners from the Administration menu, **Accounts** > **User Accounts**. This does not remove all the related resources, and only disables the account. You can edit AFT partners from the Administration menu, **Accounts** > **User Accounts** to change the Authentication Type to External.

Exchange Information with AFT Partners

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

- The specific details for how an AFT 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 Gentran Integration Suite, such as by e-mail.
- If a particular protocol requires extra parameters specific to the AFT partner, such as SFTP requiring user keys, set these up in the Gentran Integration Suite Administration menu after creating the AFT partner.

Note: SFTP Authorized User Key can be added before or during SFTP initiating consumer 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. The public part of this key may be exported and can become a Known Host Key for a Remote Profile for a remote server.

Route Records

Gentran Integration Suite creates route records for each file transfer. From the AFT Management menu, select **Views** > **Route Records**. You can search for individual records, or for records matching multiple criteria, as described by the following fields:

Field	Description
Producer	Name of the AFT partner that originated the data the Router is routing
Consumer	Name of the partner intended to receive the data the Router is routing
Status	◆ Success ◆ Failed ◆ In Progress ◆ Reviewed
Activity From	Date/Time Range when the route was initiated
File Name	Name of the file as specified by the producer
File Size From/to	Size range of the file as sent by the producer
Search by ID	List a particular route record directly by entering the route ID.

Route Details

To view the details about a route, click on the route ID in the list of routes that met your search criteria.

Field	Description
ID	Unique ID assigned by Gentran Integration Suite to each route. Each time a route is replayed, it is assigned a new ID.
Producer	Name of the AFT partner that originated the data the Router is routing
Consumer	Name of the partner intended to receive the data the Router is routing
File Name	Name of the file as specified by the producer
File Size	Size of the file as sent by the producer
Status	◆ Success ◆ Failed ◆ In Progress ◆ Reviewed

Field	Description
Replay	Click on the arrow next to Replay to replay the route.
Time Stamp	Date and time the route was initiated. Format is YYYY-MM-DD HH:MM:SS.0.
Event Code	The event code for each step of the route progress. See *Interpret Event Codes* on page 46.
Route Fact	Additional information about each step of the route progress. Within this information, each data flow, workflow, and communication session is an active hyperlink. Use these hyperlinks to access additional detail about the route execution.

Generate Report

To generate the AFT Routing Detailed Report or the AFT Routing Summary Report, from the AFT Management menu, select **Report** > **Generate Report**.

Field	Description
Producers	Select AFT partners that are producers for the routes to report on
Consumers	Select AFT partners that are consumers for the routes to report on
Group by	◆ Producer ◆ Consumer
Activity From	Date Range
Status	◆ Success ◆ In Progress ◆ Failed ◆ Reviewed
Format	◆ PDF (requires Acrobat 6.x or higher) ◆ HTML ◆ XLS **Note:** The AFT Routing Summary Report is only available in Acrobat PDF format.
Sort by	◆ Status ◆ File Name ◆ File Size
Report Type	◆ Detailed ◆ Summary

Import and Export AFT Communities and AFT Partners

If you want to use the same configurations of AFT communities and AFT partners in multiple Gentran Integration Suite installations, you can create them in one installation, export them from there, and import them into other installations. This is useful for first creating a test system and then moving the successful configurations to a production system.

You can only export one AFT community at a time and each goes into its own XML file. This is because each AFT community is associated with a unique resource tag that is applied to every partner belonging to the community (and to all resources that belong to each AFT partner). Partners cannot be exported individually. Partners are exported by exporting the community the partners belongs to, which exports all partners in the community at once.

Note: Do not use export community. That does not export the entire AFT community resource.

To export an AFT community:

1. From the Administration menu, **Deployment > Resource Manager > Import/Export**.
2. Choose **XML Document** for the type of format.
3. Select **Yes** for tag name.
4. Choose the resource tag with the name of the community name you want to export from the list.
5. Select whether to export private certificates.

The export file is created. Examine the export report to confirm that there are no errors.

When importing a community, a page is presented for each kind of resource in the export file. Choose all the objects for each kind of resource so all objects are imported. You cannot specify individual partners for import; all the partners in the exported community are imported at once. Keep the name of the resource tag the same.

Exporting an AFT community and the AFT partners that belong to it exports the AFT resources. The Gentran Integration Suite resources created from the Admin menu, such as adapters and SSH profiles must be exported separately. From the Admin menu, select **Deployment** > **Resource Manager** > **Import/Export**.

Replay a Route

An administrator can replay the route without contacting the data producer to request the route be replayed. This is useful if a route destined for a consumer failed, and the cause of failure is resolved. Messages are archived when the original message is extracted by the AFT Router. The message is moved to the archive mailbox and a prefix of the dataflow ID is added to the message name.

To replay a file transfer route:

1. From the AFT Management menu, select **Views** > **Route Records**.
2. Search for the route you want to replay.

3. Click on the ID link to obtain the Route Details.
4. Click on the arrow next to Replay in the Route Details.
5. On the Route Replay Confirm page, verify:
   - Name of Message to replay
   - Mailbox for Message to replay
6. Enter any information in the Reason for Replay text box.
7. Click Finish to replay the route.
8. The route details for the original route are updated to include the facts about the replay, with hyperlinks to the replay details.

Visibility Data Records

The visibilities properties provides settings for the Advanced File Transfer reports and tracking. Change the default settings to:

- Control the amount of visibility data available for AFT tracking and reports
- Change the interval for writing records to the database
- Change the default value AFT route fact records use for the event code
- Change the intervals for purging event records

To avoid having your customized settings overwritten during future installation of Gentran Integration Suite upgrades or patches, change property file settings using the customer override property file:

1. In the <install_dir>\properties directory, locate (or create, if necessary) the customer_overrides.properties file.
2. Open the customer_overrides.properties file in a text editor.
3. Add the properties that you want to override, using the following format:
4. PROPERTY_FILE_NAME.PROPERTY_NAME=PROPERTY_VALUE
5. PROPERTY_NAME **-** The name of the property as used in the specified property file.
6. PROPERTY_VALUE **-** The value you want to assign to the property.

7. Configure the vibilities.properties.in properties according to the following table:

Property	Description
visibility_coverage	Determines which components of Advanced File Transfer are available for reports and tracking. Valid values are: ◆ CommAll – All components of AFT visibility are enabled. This includes all of the other values, except none. ◆ CommBase – Basic level of visibility which includes communication sessions, file transfers, process file events, and AFT routing event and records. ◆ Authentication – Displays authentication events and records, such as identification and verification of identity for entry. ◆ Authorization – Displays authorization events and records, such as access to resources in Gentran Integration Suite ◆ NonFileXfer – Non-file transfer events and records, such as FTP CWD. ◆ AdminAudit – Administrative audit trail events and records, such as user creation and deletion. ◆ None – AFT visibility is disabled. Multiple values can be combined in a comma-delimited value. For example: `visibility_coverage=CommBase,Authentication,AdminAudit`
event_input_queue_capacity	Sets the capacity of the bounded queue through which all AFT events pass on their way to the database. If this queue reaches full capacity, AFT clients are blocked until space becomes available in the queue to process more events. The visibility log file prints alerts when this queue reaches full capacity, and records when operation returns below the full capacity level. Making the queue too large requires more memory. This parameter needs to be tuned with the persistent_batching_interval to achieve optimum results. Default is 2048.
persistent_batching_interval	Sets the interval, in ms, between batching AFT events to the database. Default is 2000.
default_route_fact_event_code	The default value that AFT route fact records use for the event code. Default is Cust-0000.
lifespan_session	Lifespan for AFT session records, in hours. Default is 336 (equals 2 weeks). Controls the lifespan of entries in these database tables: ◆ AFT_SESSION ◆ AFT_AUTHENTICATE ◆ AFT_AUTHORIZE ◆ AFT_XFER ◆ AFT_NON_XFER Data for these tables is purged by the Purge service once the lifespan_session has expired.

Property	Description
lifespan_dataflow	Lifespan for AFT data Flow records, in hours. Default is 336 (equals 2 weeks). Controls the lifespan of entries in these database tables: ◆ DATA_FLOW ◆ DMI_ROUTE ◆ DMI_ROUTE_FACT Data for these tables is purged by the Purge service once the lifespan_dataflow has expired.
lifespan_adminaudit	Lifespan for AFT admin audit records, in hours. Default is 336 (equals 2 weeks). Controls the lifespan of entries in these database tables: ◆ ADMIN_AUDIT Data for this table is purged by the Purge service once the lifespan_adminaudit has expired.
maxDFRecords	Maximum number of records returned by querying for data flows. Default is 500.
maxCSRecords	Maximum number of records returned by querying for communication sessions. Default is 500.

Purge AFT Visibility Data

AFT visibility data is purged from Gentran Integration Suite, not archived. The parameters lifespan_dataflow and lifespan_adminaudit (see *Visibility Data Records* on page 29) control the lifespan of entries in the tables. Once these lifespans expire, the Purge service removes data from the database every ten minutes. Data that is purged is unrecoverable. You can change the schedule for purging by editing the Purge schedule.

Predefined Business Processes

There are predefined business processes installed with Gentran Integration Suite AFT to enable the functionality of AFT. You can modify these business processes as necessary to accomplish your tasks.

Business Process Name	Description
AFTRouteAddMailboxMessage	Adds a message to a Mailbox as the result of a route.
AFTRouteEventEmailNotification	Sends email notifications when subscribed events occur.
AFTRouteExtractMailboxMessage	Extracts a message from a Mailbox as the result of a route.
AFTRouteFTPPUT	Executes an FTP PUT command using the FTP Server adapter.
AFTRouteHTTP	Uses the HTTP Server adapter.
AFTRoutePackageDocument	Uses the PGP Package service.

Business Process Name	Description
AFTRouteSendMessage	Sends a message to a Mailbox as the result of a route.
AFTRouteSFTPPUT	Executes an SFTP PUT command using the FTP Server adapter.
AFTRouteUnpackageDocument	Uses the PGP Unpackage service.
AFTRouteViaCD	Uses the Connect:Direct Server adapter.
Schedule AFTPurgeArchive	Purges archived messages from the Mailbox.

Purge Archived AFT Messages

When Gentran Integration Suite AFT is installed, the business process 'AFTPurgeArchiveMailboxes' is enabled and scheduled to run once a day. This BP queries the MBX_MESSAGE table for archived messages whose dataflows no longer exist in the DATA_FLOW table. These messages are then removed using the Mailbox Delete Service.

Test the Purge of Archive Mailboxes

To test the purging of archive mailboxes:

1. Create an AFT route with an initiating producer.
2. Edit the <install_dir>\properties\visibility.properties file to set the lifespan_dataflow to 1.

   ```
   lifespan_dataflow=0
   ```

3. Restart Gentran Integration Suite so the properties file change take effect.
4. FTP a message into the producer's Inbox and wait for the AFT Router to route the message to a consumer.
5. As aft_user, log into the producer’s archive mailbox to verify the message has been archived and has a name of '<dataflowId>_<originalName>.
6. Search Data Flows for the dataflow ID to verify the data flow exists.
7. Search for the business process 'Schedule_PurgeService'. Set it to run every 10 minutes.
8. Wait an hour for the data flow ID to expire.
9. Wait for the Purge schedule to occur.
10. Search Data Flows to verify that the data flow no longer exists.
11. Manually execute the AFTPurgeArchiveMailboxes business process.
12. Log into the archive mailbox to verify the archived message has been purged.

Troubleshoot AFT

To aid you in troubleshooting the setup of adapters used in file transfer, Gentran Integration Suite includes a visibility event listener, DmiVisEventListener. By default this listener is not enabled. To enable the event listener:

1. Edit the listenerStartup.properties file to uncomment the DmiVisEventListener.
2. Edit this property to define a list of adapter names to trace for AFT events as:

   ```
   debug_listener_adapter_filters=FTP_SERVER_ADAPTER,HttpClientAdapter,TestHTT
   PServerAdapter-toFS,EDIINTParse
   ```
3. You can use the following optional qualifiers:
   - `All` – to trace all adapters, as in:

     ```
     debug_listener_adapter_filters=All
     ```
   - `admin_events` – to trace admin audit events, as in:

     ```
     debug_listener_admin_event=True
     ```
   - `log_file_home` – defines the directory that the debug tracing logs are written to, with the trailing delimiter \ on the directory name, as in:

     ```
     debug_listener_log_file_home=\localhome\install\logs\
     ```

External Event Driven Notification

For simple email notification for external AFT partners, enable notifications when you create or edit an AFT community. Then, inform AFT partners that they can subscribe to notifications using MyAFT. AFT error and completion events are available for email notification when enabled for the AFT community. When routes are executed that incur the events the AFT partners are subscribed to, Gentran Integration Suite sends an email to the AFT partner.

Note: When you install Gentran Integration Suite, you must specify a valid SMTP mail server host. This host sends the email notifications to the partner’s email address specified in the AFT partner profile.

Internal Event Driven Notification

You can create business processes that are invoked by certain events. This is useful for administrators to be informed when certain events happen within Gentran Integration Suite. The triggering of the business process is based on a combination of the event type and the evaluation of an Xpath expression written against the contents of the event itself.

To configure the optional event listener, XpathBPLauncherEventListener:

1. Edit the listenerStartup.properties and listenerStartup.properties.in files to include the line:

   ```
   Listener.Class.xx=com.sterlingcommerce.server1.dmi.visibility.event.XpathBP
   LauncherEventListener
   ```

   Where *xx* is the next available number according to how many listeners are already enabled in the file.

2. Edit the visibility.properties and visibility.properties.in files to add the necessary information to configure the listener to launch the proper business processes based on the correct events. The pattern for registering the events with the listener is:

   ```
   bp_event_trigger.X=eventPreFilter,xPathExpression,bpname,userId
   ```

   where:

   - **X** is a numerical index into each unique event-bp combination being registered. (1, 2, 3, and so on).
   - **eventPreFilter** is the prefix for the event type of the events to be evaluated (aft.visibility.xxx). The event can be any valid Gentran Integration Suite event, not just visibility events. The eventPreFilter is comprised of scope (Aft), subsystem (Visibility), name (for example, CommAuthentication), and numTag (for example, 1). The numTag is optional.

     The values for name and numTag are provided in *Values for eventPreFilter Fields* on page 35.
   - **xPathExpression** is any valid Xpath expression that can be evaluated to a boolean result.
   - **bpname** is the name of the business process to be launched.
   - **userId** is the name of a valid Gentran Integration Suite user used by the launched business process to determine any authorizations required by the business process.

For example, to launch an e-mail business process (aft_email_notifier) with user credentials ‘admin’ every time there is a failed authentication for the user account ‘acme’:

```
bp_event_trigger.1=Aft.Visibility.CommAuthentication,//Event/isSuccessful=’
false’ and //Event/principal = ‘acme’, aft_email_notifier,admin
```

Or, an example to launch an e-mail business process (EmailNotifXferEvent) with user credentials ‘admin’ when there is a completed file transfer on the FTP server:

```
bp_event_trigger.1=Aft.Visibility.CommFileXferComplete.1,//Event/isPut='fal
se' and //Event/isSuccessful='true',EmailNotifXferEvent,admin
```

Or, an example to launch an e-mail business process (EmailNotifXferEvent) with user credentials ‘admin’ when there is a non-file transfer event such as delete or move on the FTP server:

```
bp_event_trigger.2=Aft.Visibility.CommNonTransfer.1,//Event/type='delete'
or //Event/type='move',EmailNotifNonXferEvent,admin
```

Values for eventPreFilter Fields

The following event types are specified in the name position of the eventPreFilter field:

Name	Attributes
Aft.Visibility.CommConnect	◆ sessionId – Required. ◆ sessionArchiveId – Required. ◆ wfId – Optional. ◆ wfStep – Optional. ◆ startTime – Required. ◆ endTime – Required. ◆ endpoint1 – Required. ◆ endport1 – Optional. ◆ endpoint2 – Required. ◆ endport2 – Optional. ◆ isSuccessful – Required. Valid values are true, false. ◆ errorMsg – Optional. ◆ adapterType – Required. Valid values are FtpClientAdapter, FtpServerAdapter, HttpClientAdapter, HttpServerAdapter, EDIINTMessageService, EDIINTPipelineService, MailboxBrowserInterface, Connect:DirectServerAdapter, SFTPClientAdapter, SFTPServerAdapter. ◆ adapterName – Required. ◆ psInstance – Optional. ◆ protocol – Required. Valid values are FTP, HTTP, Connect:Direct, AS2, MBI, SFTP, WEBDAV. ◆ secureMode – Required. Valid values are none, SSL, SSH, CCC. ◆ isLocallyInitiated – Required. Valid values are true, false. ◆ childSessionId – Optional. ◆ state – Optional. ◆ processNumber – Optional. ◆ principal – Optional.
Aft.Visibility.CommSessionUpdate	◆ sessionId – Required. ◆ username – Optional. ◆ userpath – Optional. ◆ secureMode – Optional. Valid values are none, SSL, SSH, CCC. ◆ state – Optional.

Name	Attributes
Aft.Visibility.CommDisconnect	◆ sessionId – Required. ◆ wfId – Optional. ◆ wfStep – Optional. ◆ startTime – Required. ◆ endTime – Required. ◆ isSuccessful – Required. Valid values are true, false. ◆ errorMsg – Optional.
Aft.Visibility.CommAuthentication	◆ authenticateId – Required. ◆ sessionId – Required. ◆ sessionArchiveId – Required. ◆ wfId – Optional. ◆ wfStep – Optional. ◆ time – Required. ◆ isSuccessful – Required. Valid values are true, false. ◆ principal – Required. ◆ credentialType – Required. Valid values are contract, sender, SHA1/MD5, none, unknown, sslClientAuth, netmapCheck, publickey, ◆ password. ◆ credentialValue – Required. ◆ isCounterParty – Required. Valid values are true, false.
Aft.Visibility.CommAuthorization	◆ authorizeId – Required. ◆ sessionId – Required. ◆ sessionArchiveId – Required. ◆ time – Required. ◆ isSuccessful – Required. Valid values are true, false. ◆ errorMsg – Optional. ◆ principal – Required. ◆ resourceType – Required. Valid values are MAILBOX, URL, BP, WARFILE, CONTRACT, AS2 SIGNING, AS2 UNSIGNED. ◆ resource – Required. ◆ actionType – Required. Valid values are add, extract, execute, access, list, submit.

Name	Attributes
Aft.Visibility.CommFileXferBegin	◆ transferId – Required. ◆ sessionId – Required. ◆ sessionArchiveId – Required. ◆ isPut – Required. Valid values are true, false. ◆ documentId – Required. ◆ documentName – Required. ◆ wfId – Optional. ◆ wfStep – Optional. ◆ time – Required. ◆ fileSize – Optional. ◆ remoteFileName – Optional. ◆ mailboxPath – Optional. ◆ messageId – Optional. ◆ messageName – Optional. ◆ errorMsg – Optional. ◆ isBinary – Required. Valid values are true, false. ◆ isSecure – Required. Valid values are true, false. ◆ isRestart – Required. Valid values are true, false. ◆ isLocallyInitiated – Required. Valid values are true, false. ◆ ignoreTracking – Required.
Aft.Visibility.CommFileXferUpdate	◆ transferId – Required. ◆ bytesTransferred – Required. ◆ time – Required.
Aft.Visibility.CommFileXferComplete	◆ transferId – Required. ◆ bytesTransferred – Required. ◆ time – Required. ◆ isSuccessful – Required. Valid values are true, false. ◆ errorMsg – Optional. ◆ isLocallyInitiated – Required. Valid values are true, false. ◆ isPut – Required. Valid values are true, false. ◆ ignoreTracking – Required.

Name	Attributes
Aft.Visibility.CommNonTransfer	◆ nonTransferId – Required. ◆ sessionId – Required. ◆ sessionArchiveId – Required. ◆ type – Required. Valid values are processFile, transactionId, CWD, move, delete. ◆ value – Required. ◆ isSuccessful – Required. Valid values are true, false. ◆ errorMsg – Optional. ◆ startTime – Required. ◆ endTime – Required. ◆ wfId – Optional. ◆ wfStep – Optional.
Aft.Visibility.AdminAudit	◆ adminAuditId – Required. ◆ time – Required. ◆ principal – Required. ◆ actionType – Required. Valid values are Create, Edit, Delete, Add, Remove. ◆ actionValue – Required. ◆ objectType – Required. Valid values are User Account, Mailbox, Trading Partner, Service / Adapter, Group, Subgroup, Permission, Virtual Root, Routing Rule, System. ◆ objectName – Required.
Aft.Visibility.RouteDiscoveryEvent	◆ dataFlowId – Required. ◆ wfid – Required. ◆ time – Required. ◆ producer – Required. ◆ consumer – Optional. ◆ documentId – Optional.
Aft.Visibility.RouteCompleteEvent	◆ dataFlowId – Required. ◆ wfid – Required. ◆ time – Required. ◆ isSuccess – Required. Valid values are true, false.

Name	Attributes
Aft.Visibility.RouteFactEvent	◆ dataFlowId – Required. ◆ wfid – Required. ◆ time – Required. ◆ value – Required. ◆ eventCode – Required.

The following event types are specified in the numTag position of the eventPreFilter field:

NumTag	Resource
1	FTPSERVER
2	FTPCLIENT
3	HTTPSERVER
4	HTTPCLIENT
5	CDSERVER
6	ADMIN_AUDIT
7	MBI
8	AS2
9	SFTPSERVER
10	SFTPCLIENT
11	WEBDAV
99	TEST
5000	ROUTE_DISCOVERY
5100	ROUTE_COMPLETE
5200	ROUTE_FACT

Special Considerations for AFT Routing in a Cluster

When using AFT routing in a clustered environment, comply with the following considerations:

- A shared file system must be used if the document storage mechanism in a cluster is file system, so that all messages from producers are stored with the content in the file system.
- The jdbc.properties must include this setting "# Default directory to store on-disk documents. document_dir=<install_dir>/<some_common_dir_that_both_nodes_can_see>”. Otherwise, one node will not see documents on disk that the other node persisted.

- All nodes of the cluster must be installed at the same path. For example, if node1 is installed at C:\GIS42 on one server, node2 must also be installed at C:\GIS42 on another server.
- If a route fails before a message transfer is complete, it is not routed, deleted, and moved to archive. It remains in the producer’s mailbox and is not rerouted because it is already marked as routed. If this occurs, edit the message in the Administration menu to make it eligible for automatic routing again.

Data Flows

To trace a document from the time it transfers into Gentran Integration Suite, as it is processed by Gentran Integration Suite, through to when it is transferred out of Gentran Integration Suite to an external system, use the Data Flows page. You can view detailed communication records associated with the document's transfers integrated with a document tracking view of the document within Gentran Integration Suite. For example, a producer uses FTP to send a message into a mailbox, Gentran Integration Suite packages the document and transports to a consumer using Connect:Direct.

To track data moving into or out of Gentran Integration Suite by streaming through an adapter (data flows), from the Administration menu, select **Business Processes** > **Advanced Search** > **Data Flows**.

Field	Description
Endpoint	The remote endpoint of the data flows to search for. Host name or IP address. Optional.
Direction	Direction of the data flows to search for. Optional. Valid values are: ◆ Inbound ◆ Outbound
Protocol	Protocol for the data flows to search for. Optional. Valid values are: ◆ AS2 ◆ HTTP ◆ FTP ◆ SFTP ◆ MBI ◆ Connect:Direct ◆ WebDAV ◆ SWIFTNet
Status	Status of the data flows to search for. Optional. Valid values are: ◆ Normal ◆ Error
Document Name	For data flows associated with a specific document, enter the document name. Optional.
Data Size	Range of size of the data transferred to search for. From/To in bytes, KB, MB, or GB. Optional.
Date Range	From – The beginning date and time for data flows to search for To – The end date and time for data flows to search for **Note:** Select the calendar icon to the right of the date to access calendar information. Optional.
Save search values using tag	Enter a string for use in repeating the search in another session. Required.

Field	Description
Results per page	Select how many results to display per page. Required. Valid values are: ◆ 10 ◆ 25 ◆ 50 ◆ 100 ◆ 200 ◆ 250 ◆ 400 ◆ 500 Default is 10.
List Directly	By Data Flow ID

Communication Session Records

Gentran Integration Suite creates communication session records for any associated authentication, authorization, file transfer, or non-file transfer records, even if a document is not transferred and no data flow record is created. For example, session data can include a user connecting to a mailbox using FTP, receiving messages, and then quitting the FTP session.

The following types of communication session records are available:

- File transfer records
  - Protocol independent data
  - Protocol specific data
  - Statistics for file transfers
- Non-file transfer records
  - FTP directory commands, not file transfer events
  - Connect:Direct SUBMIT Service invocations
  - AS2 Session and AS2 Process File events
  - Business process trigger records
- Authentication records
  - Password
  - Public key (SFTP)
  - SSL client session authentication
  - Connect:Direct Netmap authentication (if Netmap checking is enabled)
  - AS2 Contract (authenticate using a certificate in the partner profile)
- Authorization Records
  - When a user in a communication session attempts to access resources requiring permissions
  - Attempts to access particular HTTP URLs (not requiring permissions, but controlled resources)

To view communications sessions records:

1. From the Administration menu, select **Business Processes** > **Advanced Search** > **Communication Sessions**.
2. Complete the fields using the following descriptions:

Field	Description
Endpoint	The remote endpoint of the communication sessions to search for. Host name or IP address. Optional.

Field	Description
Protocol	Protocol for the communication sessions to search for. Optional. Valid values are: ◆ AS2 ◆ HTTP ◆ FTP ◆ SFTP ◆ MBI ◆ Connect:Direct ◆ WebDAV ◆ SWIFTNet
Principal	Search for communication sessions associated with a Principal participant. Optional.
Secure Mode	Search for communication sessions in a secure mode. Optional. Valid values are: ◆ SSL ◆ CCC
Locally Initialized	Search for communication sessions that were locally initialized. Optional. Valid values are: ◆ true ◆ false
Status	Search for communication sessions by status. Optional. Valid values are: ◆ Normal ◆ Error
Connection	Search for communication sessions by connection status. Optional. Valid values are: ◆ ACTIVE ◆ Closed
DateRange	From – The beginning date and time to search for communication sessions To – The end date and time to search for communication sessions **Note:** Select the calendar icon to the right of the date to access calendar information. Optional.
Save search results values by using tag	Enter a string for use in repeating the search in another session. Required.

Field	Description
Results per page	Select how many results to display per page. Required. Valid values are: ◆ 10 ◆ 25 ◆ 50 ◆ 100 ◆ 200 ◆ 250 ◆ 400 ◆ 500 Default is 10.
Search by Process ID	Enter a specific Process ID to list directly. Optional.
List Directly By Communication Session ID	Enter a specific Communication Session ID to list directly. Optional.

Interpret Event Codes

Display descriptions of event codes by rolling your mouse over the event code in the message.

For reference, event codes and their descriptions are provided here. The syntax of the AFT event code is the following:

AFT_####

where the first two # are the AFT subsystem code and the second two # are the AFT event number.

- A number less than 50 indicates a success.
- A number greater than 50 but less than 99 indicates an error.
- A number equal to 99 indicates completion.

Base Subsystem Codes

Code	Meaning
00	Generic, not specific to any particular AFT subsystem
01	Trading partner profiles
02	PGP
03	Business processes/Workflow related
04	Routing Events

Protocol Subsystem Codes

Code	Meaning
11	Mailbox
12	FTP/FTPS

Extensibility Subsystem Codes

Code	Meaning
80	Consumer ID method extensibility
81	Consumer protocol extensibility

Generic Event Codes

Event Codes	Meaning
AFT_0001	Consumer destination message name is {0}
AFT_0002	Producer message name is {0}
AFT_0050	ERROR: The consumer name cannot be determined from the producer file {0} using the pattern ConsumerName {1} Filename

Trading Partner Profile Messages

Event Codes	Meaning
AFT_0101	Message producer is {0}
AFT_0102	Message consumer is {0}
AFT_0103	Consumer profile found for {0}
AFT_0104	Consumer protocol is {0}
AFT_0105	Consumer identification policy for {0} is {1}
AFT_0150	ERROR: Consumer ID policy for producer identity {0} is missing
AFT_0151	ERROR: Consumer identity not found for {0}
AFT_0152	ERROR: The producer identity for {0} is missing the consumer identity name
AFT_0153	ERROR: Producer identity not found for {0}
AFT_0154	ERROR: Consumer profile {0} not found for consumer {1}
AFT_0155	ERROR: Transport receiving protocol for consumer {0} is missing or undefined
AFT_0156	ERROR: The destination mailbox setting for the consumer profile {0} is missing or empty
AFT_0157	ERROR: The protocol {0} specified by the consumer profile for {1} is not supported
AFT_0158	ERROR: Producer package {0} is missing
AFT_0159	ERROR: Consumer package {0} is missing

PGP Messages

Event Codes	Meaning
AFT_0200	Producer PGP Options are encryption {0}, digital signing {1}, compress {2}
AFT_0201	Consumer PGP Options are encryption {0}, digital signing {1}, compress {2}
AFT_0202	Producer document has been unpackaged

Event Codes	Meaning
AFT_0203	Consumer document has been packaged
AFT_0250	ERROR: Producer encryption method not found
AFT_0251	ERROR: Consumer encryption method not found
AFT_0252	ERROR: Community secret key is missing
AFT_0253	ERROR: Producer payload is not set
AFT_0254	ERROR: Consumer payload is not set
AFT_0255	ERROR: Failed to unpackage producer document {0}
AFT_0256	ERROR: Failed to package consumer document {0}
AFT_0257	ERROR: Consumer public key is missing

BP/Workflow Messages

Event Codes	Meaning
AFT_0350	ERROR: An error occurred during the execution of the business process {0}. Check the AFT Routing log for additional details.
AFT_0351	ERROR: Unable to load the primary document for document ID{0}. Have an administrator check the AFT Routing log for additional details.
AFT_0352	ERROR: Unable to start the business process {0}. Have an administrator check the AFT Routing log for additional details.

Event Messages

Event Codes	Meaning
AFT_0400	Email notifications for event code {0} sent to {1}

Mailbox Messages

Event Codes	Meaning
AFT_1100	Route started for mailbox message {0}
AFT_1101	Consumer destination mailbox is {0}
AFT_1102	Mailbox message {0} extracted to document {1}
AFT_1103	Producer message is stored in the mailbox {0}

Event Codes	Meaning
AFT_1110	Message archived into mailbox {0}
AFT_1111	Message archived as {0}
AFT_1150	ERROR: The consumer name cannot be determined because the message to route is not stored in a sub mailbox under the producer root mailbox
AFT_1151	ERROR: Unable to extract document for mailbox message {0}
AFT_1152	ERROR: Mailbox message {0} does not exist
AFT_1199	Routing document {0} to consumer mailbox {1} is complete

FTP Messages

Event Code	Meaning
AFT_1299	Routing document {0} via FTP using the consumer profile {1} is complete.

HTTP Messages

Event Code	Meaning
AFT_1400	Route started for HTTP message {0}

Consumer ID Method Extensibility Messages

Event Codes	Meaning
AFT_8000	The business process {0} will be used to determine the consumer name.
AFT_8050	ERROR: The consumer ID method business process name for producer {0} is missing or undefined
AFT_8051	ERROR: The consumer ID method business process {0} for producer {1} did not return the name of the consumer.

Consumer Protocol Extensibility Messages

Event Codes	Meaning
AFT_8100	Consumer protocol is defined in the extensibility XML file
AFT_8101	The business process {0} will be used to route the message to the consumer {1}
AFT_8150	ERROR: The protocol business process name for consumer {0} is missing or undefined

Event Codes	Meaning
AFT_8199	Routing document {0} via consumer protocol business process {1} is complete

Add Custom Event Codes

The event code list is extensible so that you can create additional codes to track specific events according to your needs. You can create event codes to display custom messages in the Details view of a route. This is useful when you add custom protocols and policies. To add event codes to the custom list:

1. Use the existing AFTEventCodes.properties file from <install_dir>\properties\resources as a template to create AFTEventCodesCustomer.properties and add your custom events to it. Do not edit the AFTEventCodes.properties file.

   The property file should be formatted as:

   Event_Code=The message to be displayed.

   The display message may contain parameters that can be set in the service call that triggers the event. Parameters must be in the form of {#}, where {#} is a number starting with 0. An event message with parameters would look like this:

   Event_Code=Message with two parameters. The first parameter is: {0} and the second is {1}.

   Custom codes must not be prefixed AFT_. The AFT_ prefix is reserved for the AFT Router. Use any other prefix, such as CUST_. The following is an example AFTEventCodesCustomer.properties file:

   ```
   The value of the property will be displayed as the event with {#} used as
   parameters.
   Events
   CUST_1401=Message successfully delivered via HTTP to host {0}, port {1}, URI
   {2}
   ```

2. Save AFTEventCodesCustomer.properties to:

   `<GIS_INSTALL>\properties\resources`

   To retrieve custom event codes from a previous release of Gentran Integration Suite, go to `[GISInstall]\uninstall\SP_0\PATCH_x\displaced_files\properties\resources\AFTEventCodes.properties.`

   where x is the number of the patch you have installed. Rename this file AFTEventCodesCustomer.properties and save it to `<GIS_INSTALL>\properties\resources.`

3. Stop Gentran Integration Suite and run:

   ```
   <GIS_INSTALL>\bin\setupfiles.sh
   <GIS_INSTALL>\bin\deployer.sh
   ```

4. Restart Gentran Integration Suite.

5. Configure an instance of the AFT Route Progress Event Reporting Service and add it to the business process that is reporting the event. The RouteEventMessageParameters are colon delimited.

Note: The AFTEventCodesCustomer.properties file is not managed by the Gentran Integration Suite Resource Manager. It must be backed up, archived, and restored separately.

The following is an example business process that includes the AFT Route Progress Event Reporting Service:

```
<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>
      <operation name="AFT Route Progress Event Reporting archive mailbox">
         <participant name="AFTRouteProgressEventService"/>
         <output message="AFTRouteProgressEventServiceTypeInputMessage">
            <assign to="." from="*"/>
            <assign to="AFTRouteEventId">CUST_1401</assign>
            <assign to="AFTRouteEventMessageParameters"
from="concat(string(RemoteHost),':', string(RemotePort),':',string(URI))"/>
         </output>
         <input message="inmsg">
            <assign to="." from="*"/>
         </input>
      </operation>
   </sequence>
</process>
```

Extend the Capabilities of AFT

You can customize AFT to support additional functionality in the following areas:

- Protocol support – see *Add Custom Protocols* on page 54
- Consumer identification policy support – see *Add Consumer Identification Policies* on page 62
- Event codes – see *Add Custom Event Codes* on page 50

To add custom protocols or consumer identification policies, edit the AFTExtensionCustomer.xml file.

Edit the AFTExtensionsCustomer.xml File

The following elements and attributes are in the AFTExtensionCustomer.xml file:

Element	Attributes
AFTExtensions	AFTExtension supports the attributes: ◆ name – Name of the extension. Required. ◆ type – Protocol or Policy extension. Required. ◆ label – Display name to use on the interface. Required. ◆ bp – The business process that implements this extension. Required.
GROUP	You can have multiple pages of parameters. A group represents a page. Subgroups also represent a page. They allow you to capture dependencies between pages. For example, if 'varA' is set to true, display subgroupA, else display subgroupB. GROUPs can contain VARDEFs. GROUP supports the attribute: ◆ title – the title to display on the page
SUBGROUP	SUBGROUP supports the attributes: ◆ title – the title to display on the page ◆ dependencyvar – varname that is SUBGROUP is dependent on ◆ dependencyvalue – the value of the dependencyvar that should cause this page to get displayed To specify multiple dependent vars, you can specify the attributes ◆ depnum – number of dependencies that should all match ◆ dependencyvar<0..n> – ◆ dependencyvalue<0..n> – SUBGROUPs can contain other SUBGROUPs and/or VARDEFs. On SUBGROUP, with a single dependency, the dependencyvar is optional. When not specified, it defaults to the varname of the enclosing VARDEF. With multiple dependencies, depnum, dependencyvar<0..n>, dependencyvalue<0..n> are all required.

Element	Attributes
VARDEF	Supported attributes are: ◆ varname – the name of the variable. This will be the element name in Process Data. ◆ label – the name of the label for the variable in the user interface. This corresponds to the name in AFTExtensionsCustomer.properties. ◆ htmlType – determines how the variable is displayed to users. Valid values are: text password select – drop down list populated by consumer delivery protocol (if AFTExtension type = Protocol) and consumer identification policy (if AFTExtension type = Policy) ◆ required – whether the variable must be specified. Optional. Default is false. If true, a variable must be supplied by the user. **Note:** If htmlType = password, required must = true. ◆ options – name of class that provides options ◆ defaultVal – A default value used if not specified. Optional. ◆ size – (not supported and not required) ◆ maxsize – (not supported and not required) ◆ type – (not supported and not required) ◆ validator – (not supported and not required) VARDEFs can contain SUBGROUPs.

Add Custom Protocols

You can add support for custom protocols for listening consumers in addition to the ones preconfigured in the Gentran Integration Suite AFT installation. The information you provide in performing this procedure determines the text displayed in the Create Community and Create Partner wizards. That is, after you perform this procedure, new choices are available for protocols offered by AFT communities and new parameters display in the Create Partner wizard for listening consumers selecting the new protocol.

To add protocols:

1. Write a business process that implements the protocol.
2. Use the existing AFTExtensions.xml as a template 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 and also to:

   ```
   <install_dir>\container\Applications\myaft\WEB-INF\classes\resources\xml
   ```
4. Reference the BP you created in step 1 in the newly created AFTExtension element in the AFTExtensionsCustomer.xml file.

5. Stop Gentran Integration Suite.
6. Use the existing AFTExtensions.properties file as a template to create the AFTExtensionsCustomer.properties file. Do not edit the AFTExtensions.properties file.
7. The AFTExtensions.properties is located in the following directory: `<install_dir>\container\Applications\aft\WEB-INF\classes\resources`
8. Save the AFTExtensionsCustomer.properties file to the same directory and also to: `<install_dir>\container\Applications\myaft\WEB-INF\classes\resources`
9. Run `<install_dir>\bin\setupfiles.sh.`
10. Run `<install_dir>\bin\deployer.sh.`
11. Start Gentran Integration Suite.

The additional protocol will be available when adding and editing AFT communities. The specified parameters are then available when creating and editing AFT partners.

Exporting and Importing Custom Protocols

The AFTExtensionsCustomer.xml and AFTExtensionsCustomer.properties files are not managed by the Gentran Integration Suite Resource Manager. These files must be backed up, archived, and restored separately.

To use custom protocols in another installation of Gentran Integration Suite:

1. Copy the AFTExtensionsCustomer.xml file from the following directory:

   ```
   <src_install_dir>\container\Applications\aft\WEB-INF\classes\resources\xml
   ```

   to the following two directories on the destination Gentran Integration Suite installation:

   ```
   <dest_install_dir>\container\Applications\aft\WEB-INF\classes\resources\xml
   <dest_install_dir>\container\Applications\myaft\WEB-INF\classes\resources\x
   ml
   ```

   where src_install_dir is the original Gentran Integration Suite install directory and dest_install_dir is the new Gentran Integration Suite installation.

2. Copy the AFTExtensionsCustomer.properties file from the following directory:

   ```
   <src_install_dir>\container\Applications\aft\WEB-INF\classes\resources
   ```

   to the following two directories on the destination Gentran Integration Suite installation:

   ```
   <dest_install_dir>\container\Applications\aft\WEB-INF\classes\resources
   <dest_install_dir>\container\Applications\myaft\WEB-INF\classes\resources
   ```

   where src_install_dir is the original Gentran Integration Suite install directory and dest_install_dir is the new Gentran Integration Suite installation.

3. Restart Gentran Integration Suite for the custom protocols to become available.

Examples Adding Custom Protocols

The examples below provide a business process, AFTExtensionsCustomer.xml file, and AFTExtensionsCustomer.properties file for adding Connect:Enterprise UNIX or HTTP Send. You can use these as a model for creating the files to add other custom protocols.

Note: The AFTRouteViaCEU and AFTRouteViaHTTP business processes referred to in this section are available in your Gentran Integration Suite installation at <install>/samples/aft/extensions_sample/ (with the extension .bpml.). Sample AFTExtensionsCustomer.xml and AFTExtensionsCustomer.properties files are included in the same directory. For more information, see <install>/samples/aft/extensions _sample/README.txt.

ProcessData for Business Processes Implementing Custom Protocols

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

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

Example Adding an Connect:Enterprise UNIX Extension

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

```
<process name="AFTRouteViaCEU">
<sequence>
   <operation name="CEU Add Service">
      <participant name="CEUServerAdd"/>
      <output message="AddRequest">
```

```
          <assign to="." from="*"/>
          <assign to="CEUServerAdapterInstanceName"
             from="string(CEUServerAdapterInstanceName)"/>
          <assign to="CEUMailboxId" from="string(CEUMailboxId)"/>
       </output>
       <input message="inmsg">
          <assign to="CEUAddServiceResults" from="*"/>
       </input>
       </operation>
</sequence>
</process>
```

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

AFTExtensionsCustomer.xml Adding Connect:Enterprise UNIX

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

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

AFTExtensionsCustomer.properties Adding Connect:Enterprise UNIX

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

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

Example Adding an HTTP Send Extension

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

```
<process name="AFTRouteViaHTTP">
   <sequence>
      <operation name="HTTP Client Begin Session Service">
```

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

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

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

AFTExtensionsCustomer.xml for HTTP Send

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

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

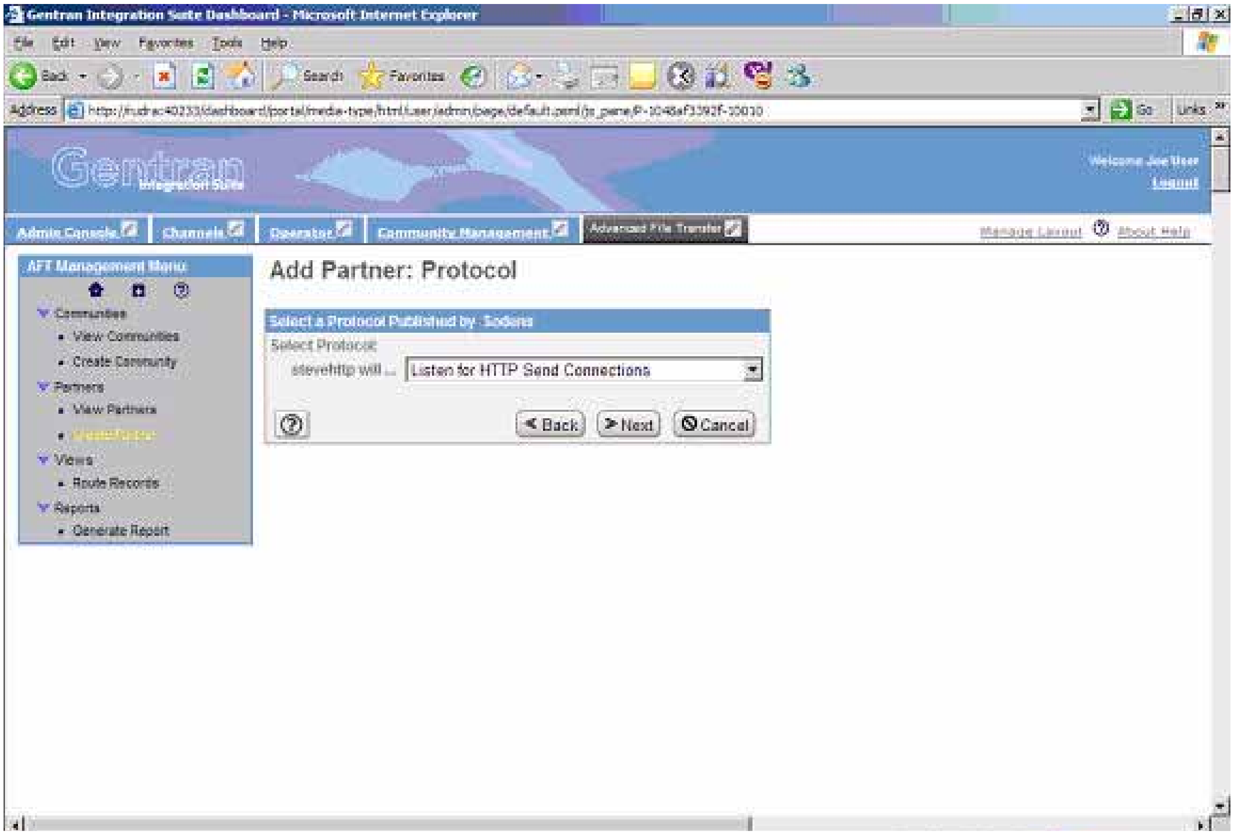
The mandatory parameter for this example is Remote Host. Optional parameters include Remote Port, Remote User Id, Remote Password, and URI.

AFTExtensionsCustomer.properties for HTTP Send

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

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

The user interface created by this example AFTExtensionsCustomer.properties file is shown in the following. The attribute for cdp.protocol.label.httpprotocol is added to the Protocol list:



Add Partner: Protocol

Select a Protocol Published by Sodens

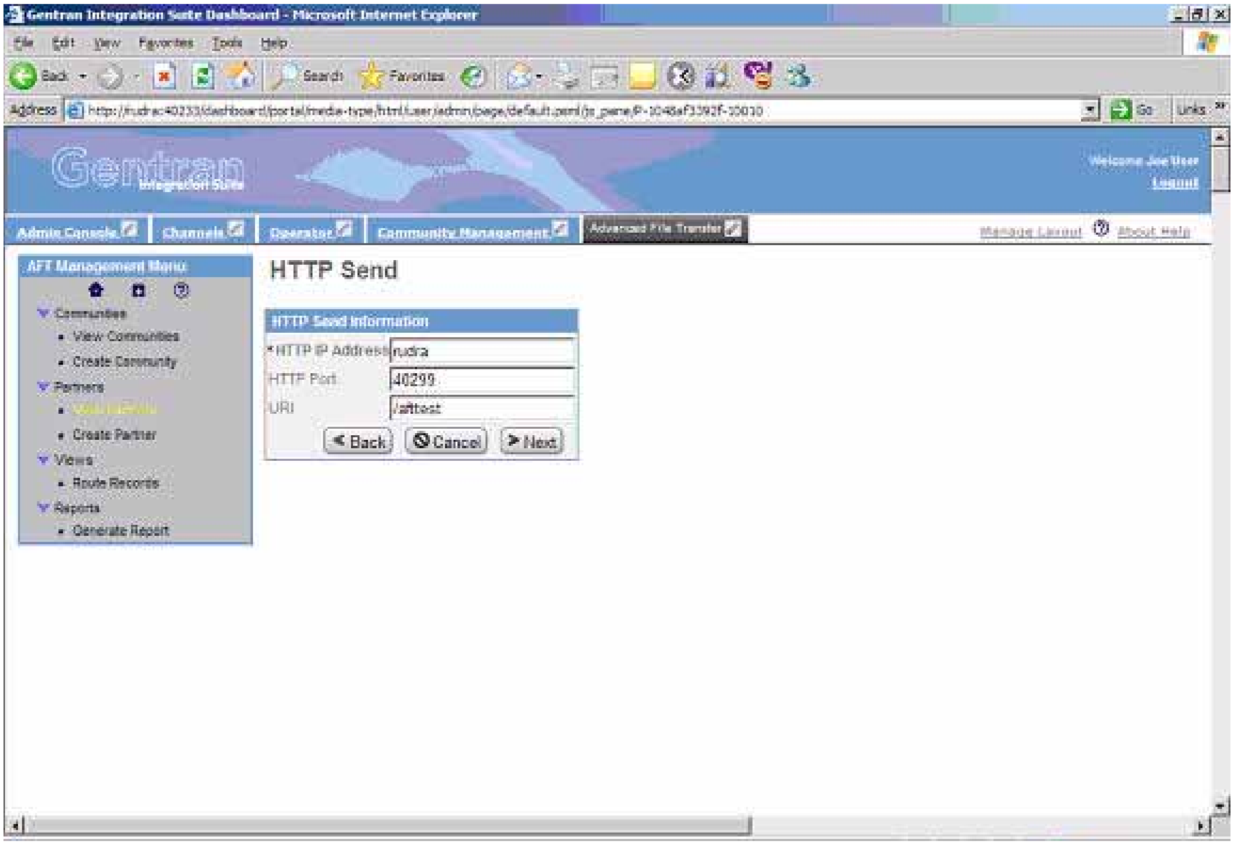
Select Protocol:

stevehttp will ... Listen for HTTP Send Connections

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



HTTP Send

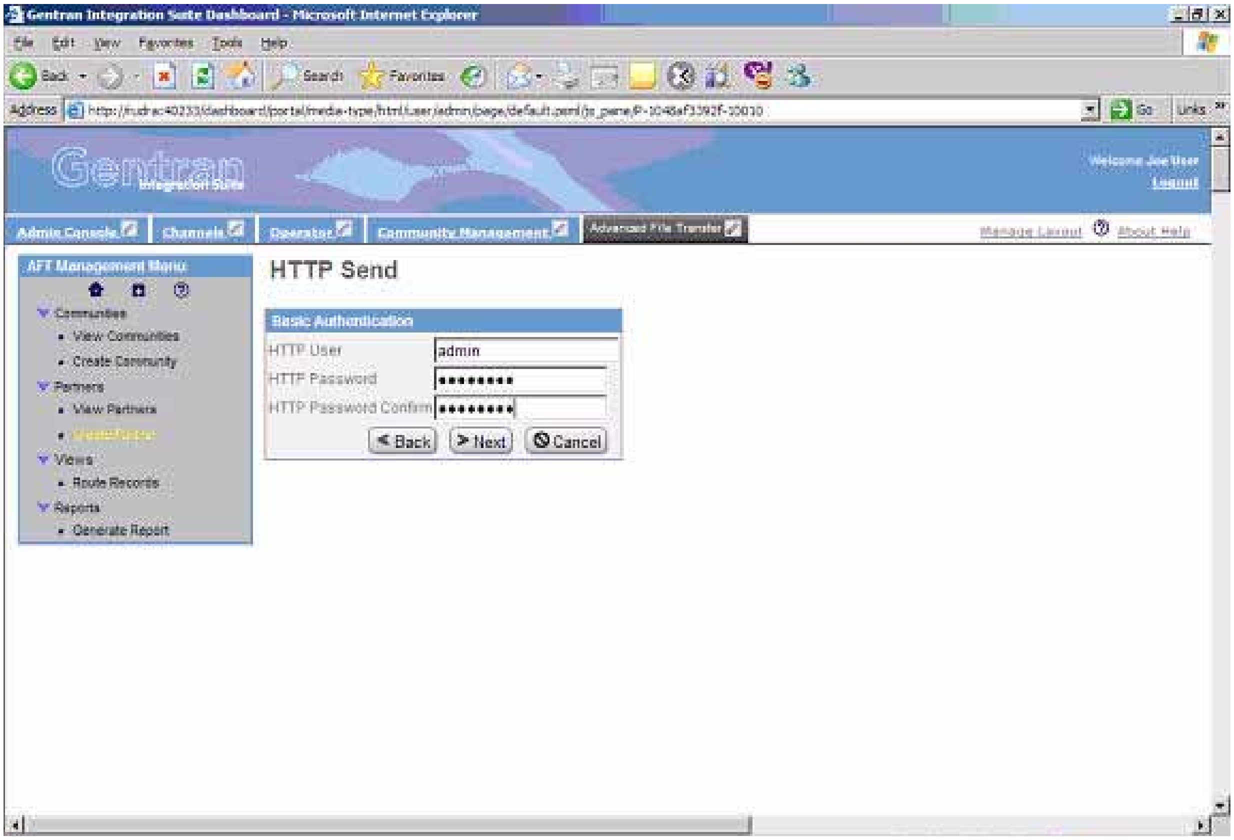
HTTP Send Information

*HTTP IP Address	rudra
HTTP Port	40299
URI	/afttest

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



HTTP Send

Basic Authentication

HTTP User	admin
HTTP Password	●●●●●●●●
HTTP Password Confirm	●●●●●●●●

< Back | > Next | Cancel

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.

Add Consumer Identification Policies

The consumer identification policy for each producer is the method the producer uses to identify the consumer to receive the file transfer. You can add consumer identification policies beyond the policies initially supported by Gentran Integration Suite. To add a consumer identification policy:

1. Write a business process implementing the consumer identification policy.

2. Edit the AFTExtensionsCustomer.xml file. See *Edit the AFTExtensionsCustomer.xml File* on page 53.

   The AFTExtensions.xml file is located in the following directory:

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

   Reference the BP you created in step 1 in the AFTExtensionsCustomer.xml file.
3. Stop Gentran Integration Suite.
4. Create the AFTExtensionsCustomer.properties file in the AFT container directory:

   `<install_dir>\container\Applications\aft\WEB-INF\classes\resources`
5. Copy the file into MyAFT container directory:
   `<install_dir>\container\Applications\myaft\WEB-INF\classes\resources`
6. Run `<install_dir>\bin\setupfiles.sh`.
7. Run `<install_dir>\bin\deployer.sh`.
8. Start Gentran Integration Suite.

The additional consumer identification policy will be available when adding and editing AFT partners that are producers.

Example Adding Consumer Identification Policies

The example below provides a business process, AFTExtensionsCustomer.xml file, and AFTExtensionsCustomer.properties file for filtering to consumer by filename. You can use these as a model for creating the files to add other consumer identification policies.

Note: The AFTRouteFilenameSubstring business process referred to in this section is available in your Gentran Integration Suite installation at <install>/samples/aft/extensions_sample/ (with the extension .bpml.) The AFTExtensionsCustomer.xml and AFTExtensionsCustomer.properties file in this directory have the xml definitions needed for AFT to recognize the AFTRouteFilenameSubstring policy.

ProcessData for Business Processes Implementing Custom Consumer Identification Policies

The following elements are available in ProcessData when the business process implementing an custom consumer identification policy 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
PrimaryDocumentName	Name of the primary document
ProducerName	Name of the producing partner

Element	Description
AFTRouteId	An internal identifier needed if the AFT Route Progress Event Reporting service is called. The value of this element must not be changed by the extensibility business process.
AFTRouteWorkFlowId	An internal work flow identifier needed if the AFT Route Progress Event Reporting service is called. The value of this element must not be changed by the extensibility business process.
Parameters added to AFTExtensionsCustomer.xml	Any parameters you supply as part of your customer protocol are available in process data.

Example Adding Filtering to Consumer by Filename as Policy

This is an example of a consumer identification policy. This displays as a list box option when you create or edit an AFT partner who initiates connections. This enables the filename to route data. The filename or a portion of the filename must match the name of the consumer. With this policy, separator characters are defined that bracket the portion of the filename that is the consumer's name. These separator characters can be different for each producer.

For example, if Left Separator = "(" and Right Separator = ")", then if a producer sending to "Research" sends a file named "reconc(Research).xml" to the Router, it is routed successfully to “Research”.

If Left Separator is empty, then the left separator is assumed to be the start of the filename. If Right Separator is empty, the right separator is assumed to be the end of the filename. If both are empty, the filename as a whole must match the name of the consumer.

This policy creates an element <AFTROUTECONSUMERNAME> that will be used by AFTRoute to invoke the consumer’s protocol BP used for that consumer.

The BPML for this example is:

```
<process name="AFTRouteFilenameSubstring">
   <!--    A policy implementation that extracts the consumer's name from the
filename more flexibly than the standard policy "use filename". With this policy,
separator characters are defined that "bracket" the portion of the filename that is
the consumer's name. These separator characters can be different for each producer.
   <rule name="is-left-boundary-char-empty">
      <condition>separator-character-from-left = ""</condition>
   </rule>
   <rule name="is-right-boundary-char-empty">
      <condition>separator-character-from-right = ""</condition>
   </rule>
   <sequence>
      <choice>
         <select>
            <case ref="is-left-boundary-char-empty"
               activity="filename-is-candidate"/>
            <case ref="is-left-boundary-char-empty" activity="rhs-is-candidate"
               negative="true"/>
         </select>
         <assign name="filename-is-candidate" to="candidate-portion"
            from="PrimaryDocumentName"/>
         <assign name="rhs-is-candidate" to="candidate-portion"
```

```
            from="substring-after(PrimaryDocumentName,
            separator-character-from-left)"/>
      </choice>
      <choice>
         <select>
            <case ref="is-right-boundary-char-empty"
               activity="candidate-is-portion"/>
            <case ref="is-right-boundary-char-empty" activity="lhs-is-portion"
               negative="true"/>
         </select>
         <assign name="candidate-is-portion" to="portion"
            from="candidate-portion"/>
         <assign name="lhs-is-portion" to="portion"
            from="substring-before(candidate-portion,
         separator-character-from-right)"/>
      </choice>
      <assign to="AFTROUTECONSUMERNAME" from="string(portion)"/>
   </sequence>
</process>
```

AFTExtensionsCustomer.xml

This is an example of an AFTExtensionsCustomer.xml file for filtering to consumer by filename:

```
<AFTExtensions>
   <!-- Policy that extracts a consumers name from a filename-->
   <AFTExtension name="filename-substring" type="consumer-identification-policy"
      label="cip.label.fs" bp="AFTRouteFilenameSubstring">
      <GROUP title="fs.instance.group1.page1">
         <VARDEF varname="separator-character-from-left" type="String"
            htmlType="text" validator="ALPHANUMERIC"
            label="fs_policy.firstSeparatorFromLeft" size="30" maxsize="250"
            required="no"/>
         <VARDEF varname="separator-character-from-right" type="String"
            htmlType="text" validator="ALPHANUMERIC"
            label="fs_policy.firstSeparatorFromRight" size="30" maxsize="250"
            required="no"/>
      </GROUP>
   </AFTExtension>
</AFTExtensions>
```

AFTExtensionsCustomer.properties

This is an example of an AFTExtensionsCustomer.properties file for filtering to Consumer by filename:

```
#######################################################
Filename Consumer Identification
#######################################################
cip.label.fs = use filename substring
fs.instance.group1.page1 = Filename Substring Match
fs_policy.firstSeparatorFromLeft = Left Separator
fs_policy.firstSeparatorFromRight = Right Separator
```

Index