Gentran Integration Suite

Build Updates

Version 4.3

Contents

Introduction

This document provides information about fixes and enhancements provided in Gentran Integration Suite™ Version 4.3. These builds are cumulative and include all fixes and enhancements contained in the previous build.

Build 4324 or Higher

Mailbox Permissions Enhancement

The following table lists a set of permissions added in this release to enable a non-admin user to execute schedules and business processes in the Gentran Integration Suite Mailbox:

Permission Name	Description
UI BP Execution Administrator	This permission enables an operator (non-admin) to execute a business process manually by specifying a different user in the `Run as User' field in the BP Execution page.
UI Schedule Administrator	This permission allows a user to administer all schedules in the system regardless of which user is specified in the `Run As User' field. The user can create, search, edit, and execute the schedules.
UI Scheduler	This permission displays the scheduler menu in the user interface. The user can also create, search, edit, and execute the schedules that run as this user.
UI Schedule Reviewer	This permission allows a user to view all schedules and only modify the schedules that run as this user.

Build 4322 or Higher

Improvements for Large File Imports

Import Large Files

Two new options have been added to help you import large files. They are:

- Skip Generation of Backup File
- Import All Resources

When importing large files, greater than 10 MB, use the Command Line tool - import.sh (UNIX) or import.cmd (Windows).

Skip Generation of Backup File

You now have the option to skip the generation of the backup file. Skipping the generation of the backup file may reduce out of memory errors. The option to skip the generation of the backup file has been added to the Import Resources, Tuning Options. If you use this option you need to make alternate arrangements for backup of files. If the backup generation is skipped, the following warning message is displayed:

```
Backup generation has been turned off, make sure you have another form of backup.
```

The option to skip the generation of the backup file has also been added to the Import Service parameters. The Backup parameter has been added to Import Service. Import Service is used in a business process to automatically import resources exported using the Resource Manager. This optional Backup parameter identifies the path where the backup is saved. If the path is invalid during backup, the file is written to /<install>/tmp and a message is added to the Import Report indicating the location. If the Backup parameter is not specified, then the backup is not generated.

Import All Resources

The import all resources option makes it easy to import multiple resources with a single click. This option has been added to the User Interface, Import Resources, Tuning Options.

How Does Import All Resources Impact Private Keys?

Normally, if private key certificates are found in the import file, the user is prompted to choose if the keys should be imported. If Import All Resources is selected, any private key certificates in the import file will be automatically imported without any prompting.

Import Resources

To import resources:

1. From the Administration menu, select **Deployment** > **Resource Manager** > **Import/Export**.
2. On the Import/Export Resources page, next to Import Resources, click **Go!**.
3. Enter the **path** and **file name** to import, or use **Browse** to locate and select the file. If the import returns a message that the file contains errors, you can either select the file and click Next again to continue the import, or click Cancel to stop the import process.
4. On the Import Resources page, under Tuning Options, if you want to **Skip Backup Generation**, select the checkbox. The following warning message is displayed:

   ```
   Backup generation has been turned off, make sure you have another form of backup.
   ```

   Click **OK** to continue. If you do not select backup generation, then a backup version of the files is saved and you can review it after you have completed this procedure.
5. On the Import Resources page, under Tuning Options, if you want to **Import All Resources**, select the checkbox. If you do not select this option, you will be prompted to select entries to import for each resource type. If private key certificates are found in the import file, they will be automatically imported without any prompting.
6. Click **Next**.
7. Do you want to create a resource tag for the data being imported? If Yes, enter a **Tag Name** and **Description** for the resource tag and click Next.

   If No, click **Next**.
8. Indicate whether you want to update objects that may already exist in Gentran Integration Suite with objects from the import, and click **Next**.
9. Review the information on the Confirm page.
10. Click **Finish** to import the data. The following items are displayed as links on the page:
    - **View Import Report -** Click the link to review the Import Report.
    - **View Performance Report -** Click the link to review the summary data in the Performance Report.
    - **Data in SI before Import (xml) -** Click the **Download** link to get a backup copy of the data. This link is not displayed if you selected the **Skip Backup Generation**.

Enable SSL Communication for the Admin Console

The Gentran Integration Suite Admin Console can now be deployed using the Secure Sockets Layer (SSL) protocol into a Secure HTTP Server Adapter instance. This provides the option for you to implement secure access to the Admin console web applications that are normally deployed on the base HTTP port.

In conjunction with this implementation, the Graphical Process Modeler (GPM) needs to be configured appropriately to communicate with the Admin web application using HTTPS instead of HTTP.

Note: Enabling Secure HTTP access to web applications must be done after the system has been installed.

Access to web applications deployed via the HTTP Server Adapter may be slower than when accessed on the base port.

Import Certificates into Java Web Start for Use with GPM

Java Web Start (JavaWS) is used to launch the GPM via HTTP. It supports HTTPS and the dynamic import of certificates similar to browsers. During the SSL handshake, the server provides its certificate and JavaWS handles the trust verification. If the certificate could not be verified by JavaWS, the user is prompted to accept/reject it.

In Java Version 1.5 (the current version used by JavaWS to launch the GPM), the default hostname verification does not resolve IP addresses to Domain Name System (DNS) names. As a result, when you access the GPM in HTTPS mode, you may see a warning prompt that the "`The name of the site does not match the name of the certificate`". This happens because the GPM application is configured to communicate with the server using the IP address. If the GPM is being accessed via the Admin Console application, you are assured that the IP address displayed is that of the server on which the Admin Console was deployed. Therefore, it is safe to run the application despite the prompt. This issue with Hostname Verification was fixed in Java Version 1.6.

Note: In lower versions of Java 1.5, multiple prompts may appear simultaneously when launching the GPM. To prevent this, it is recommended that you upgrade the Java Version to at least 1.5.0_11.

To import trusted root certificates into JavaWS:

1. Save the trusted root certificate to a file on your local computer.
2. Open the Java Control Panel on your local computer (javaws.exe under jre\bin).
3. Open the **Security** tab and click **Certificates**.
4. Click **Import** to browse to a trusted root certificate and select it.
5. Click **Open** to import the new trusted root certificate.

Once the trusted root certificate is checked in, JavaWS uses it for trust verification during SSL handshake.

SSL Communication Parameter Configuration

The following parameters were added to the sandbox.cfg file (/*install_dir*/install/properties) for facilitating SSL communication:

- WEBAPP_LIST_PORT - Identifies the port the GPM client should use for communication with the server. It defaults to the base port during the install. After the admin and gpm web applications have been deployed to a secure HTTP Server Adapter instance, this property should be modified to match the port of the HTTP server adapter instance.
- WEBAPP_PROTOCOL - Identifies the protocol to use for communication with the Admin web application (HTTP/HTTPS).

The following variables were added to noapp.properties.in file:

- SKIP_BASEPORT_DEPLOYMENT_WARS - Indicates which web applications should be skipped during war deployment on the base port. The list of wars is comma-delimited, case-sensitive and without the **.war** suffix. The default is to not skip any wars. After the Admin and GPM web applications are successfully deployed on a secure HTTP Server Adapter instance and are working, this property may be set to **= admin,gpm** to remove access to those web applications on the base port. The string **ALL** may be used as a wildcard to indicate that all wars should be skipped. This may not be necessary if the base port is blocked to external access.

Note: These three parameters must be specified in their respective files. Any properties specified in the sandbox.cfg file are not picked up from the customer_overrides.properities file.

Auto-Redirect to HTTPS

Support was added to the Gentran Integration Suite to allow for an automatic redirect to HTTPS to be configured for the web applications that are deployed on the HttpServerAdapter and skipped on the baseport. This is an optional, but strongly recommended, configuration.

Note: All custom properties for your environment should be set in the customer_overrides.properties file so that they are not overwritten during an upgrade or patch installation.

To enable the automatic redirect to HTTPS:

1. Navigate to the /<*install_dir*>/install/properties directory.
2. Edit the customer_overrides.properties file and enter the following parameters:

   ```
   HTTPS_REDIRECT_WARS=admin,gpm
   HTTPS_LIST_PORT=<http_server_adapter_port>
   ```

   These parameters are configured to automatically redirect a user to the HTTPS instance of the web application.

   Note: The customer_overrides.properties file is not part of the default system code. It must be created after the initial system installation and populated to match your environment.

3. Save and exit the file.

   Example implementation in customer_overrides.properties file:

   ```
   ## Identifies wars for auto-redirect to the https port. Use comma-separated
   ## list to specify multiple wars
   HTTPS_REDIRECT_WARS=admin,gpm
   ## Identifies the https port for the redirected wars. If specified, this
   ## should match the WEBAPP_LIST_PORT in sandbox.cfg
   HTTPS_LIST_PORT=<http_server_adapter_port>
   ```

   Note: The configuration mandates that all wars specified as HTTPS_REDIRECT_WARS must be deployed on the same HTTP Server Adapter instance.

Switch from HTTP to HTTPS Mode

To switch from HTTP to HTTPS mode:

1. Create a new HTTP Server Adapter instance with SSL enabled. You must configure the following parameters as specified:

   -- User Authentication Required is set to No

   -- Use SSL is set to Must
2. Deploy the admin web application (admin.war) to the HTTP Server Adapter instance with SSL enabled.

   Note: The admin.war must be picked up from /<*install_dir*>/install/noapp/deploy when configuring the HTTP Server Adapter instance. In addition, the context name of the web application must match the ADMIN_CONTEXT_PATH parameter in /<*install_dir*>/install/properties/sandbox.cfg.
3. Verify the Admin web application is accessible via the HTTP Server Adapter by accessing https://host:<*http_server_adapter_port*>/<ADMIN_CONTEXT_PATH>.
4. Deploy the GPM web application (gpm.war) to the same instance of the HTTP Server Adapter as the Admin web application.
5. Verify the GPM web application is accessible via the HTTP Server Adapter by accessing https://host:<*http_server_adapter_port*>/gpm/pmodeler/ProcessModeler.jnlp
6. Navigate to the /<*install_dir*>/install/properties directory.
7. Edit the sandbox.cfg file and modify the following parameters:

   ```
   WEBAPP_PROTOCOL=https
   WEBAPP_LIST_PORT=<http_server_adapter_port>
   ```

   Note: These parameters are used by the GPM for communication with the server.

8. **(Optional)** To turn off deployment of the Admin and GPM web applications on the base port, specify the following parameters in a customer_overrides.properties file:

   ```
   SKIP_BASEPORT_DEPLOYMENT_WARS=admin,gpm
   HTTPS_REDIRECT_WARS=admin,gpm
   HTTPS_LIST_PORT=<http_server_adapter_port>
   ```

   Example implementation in customer_overrides.properties file:

   ```
   ## Identifies the war files to be skipped during deployment on the base port.
   ## Use comma-separated list to specify multiple wars
   noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,gpm
   ## Identifies wars for auto-redirect to the https port. Use comma-separated
   ## list to specify multiple wars
   noapp.HTTPS_REDIRECT_WARS=admin,gpm
   ## Identifies the https port for the redirected wars. If specified, this
   ## should match the WEBAPP_LIST_PORT in sandbox.cfg
   noapp.HTTPS_LIST_PORT=<http_server_adapter_port>
   ```

9. Save and exit the file.
10. Navigate to the /<*install_dir*>/install/bin directory.
11. Stop the Gentran Integration Suite instance. Enter:
    `./hardstop.sh`
12. Apply the configuration changes. Enter:
    `./setupfiles.sh`
13. Deploy the new configuration. Enter:
    `./deployer.sh`
14. Restart the instance and verify that if the optional Step 7 was executed:

    -- the Admin web application access on http://host:baseport/<ADMIN_CONTEXT_PATH> is redirected to https://host:<http_server_adapter_port>/<ADMIN_CONTEXT_PATH> automatically.

    -- the GMP web application access on http://host:baseport/gpm/pmodeler/ProcessModeler.jnlp is redirected to https://host:<http_server_adapter_port>/gpm/pmodeler/ProcessModeler.jnlp automatically.

Switch from HTTPS to HTTP Mode

To switch from HTTPS back to the HTTP mode:

1. Edit sandbox.cfg and modify the following parameters:

   ```
   WEBAPP_PROTOCOL=http
   WEBAPP_LIST_PORT=<base_port>
   ```

2. **(Optional)** If the deployment of the Admin and GPM web applications on the base port was turned off when switching to the HTTPS mode, you must comment out the following parameters in the customer_overrides.properties file so that they are not applied:

   ```
   SKIP_BASEPORT_DEPLOYMENT_WARS=admin,gpm
   HTTPS_REDIRECT_WARS=admin,gpm
   HTTPS_LIST_PORT=<http_server_adapter_port>
   ```

   Example implementation in customer_overrides.properties file:

   ```
   ## Identifies the war files to be skipped during deployment on the base port.
   ## Use comma-separated list to specify multiple wars
   # SKIP_BASEPORT_DEPLOYMENT_WARS=admin,gpm
   ## Identifies wars for auto-redirect to the https port. Use comma-separated
   ## list to specify multiple wars
   # HTTPS_REDIRECT_WARS=admin,gpm
   ## Identifies the https port for the redirected wars. If specified, this
   ## should match the WEBAPP_LIST_PORT in sandbox.cfg
   # HTTPS_LIST_PORT=<http_server_adapter_port>
   ```

3. Save and exit the file.
4. Navigate to the /<*install_dir*>/install/bin directory.
5. Stop the Gentran Integration Suite instance. Enter:
   `./hardstop.sh`
6. Apply the configuration changes. Enter:
   `./setupfiles.sh`
7. Deploy the new configuration. Enter:
   `./deployer.sh`
8. Restart the instance and verify the:

   -- Admin web application is accessible on http://host:baseport/<ADMIN_CONTEXT_PATH>

   -- GPM web application is accessible on http://host:baseport/gpm/pmodeler/ProcessModeler.jnlp
9. **(Optional)** Undeploy the web applications from the SSL enabled HTTP server adapter instance.

Permissions for Limiting Access to Mailbox User Interface

The following table summarizes the permissions available to limit the access to the Mailbox user interface in Gentran Integration Suite:

Permission Name	Description
Deny UI Access to Document	The user cannot access document content from the search screens.
Deny UI Access to Document Listing	Document listings are available when more than one document is required in a step for a business process. The user cannot access a document listing.

Permission Name	Description
Deny UI Access to Mailbox Routing Rules	The user cannot access the menu items under Routing Rules (**Deployment** > **Mailboxes** > **Routing Rules**).
Deny UI Access to Mailbox Virtual Roots	The user cannot access the menu items under Virtual Roots (**Deployment** > **Mailboxes** > **Virtual Roots**).
Mailbox Access Limited to User	This permission limits the UI view to specific mailboxes. For example, if you provide this permission to /EDIInboundCollection and /EDIInboundExtraction mailboxes, the user can configure and search only the /EDIInboundCollection and /EDIInboundExtraction mailboxes. This permission applies only to the following UI screens: ◆ Mailbox Configuration (**Deployment** > **Mailboxes** > **Configuration**) ◆ Mailbox Messages (**Deployment** > **Mailboxes** > **Messages**)

PGP Profile Manager

The PGP Profile Manager enables you to add, edit, and delete PGP profiles. A PGP profile is a record stored in Gentran Integration Suite that contains information about the PGP server. The PGP Profile Manager works with the PGP Package service and PGP Unpackage service.

How Gentran Integration Suite Works with a PGP Server

Gentran Integration Suite passes documents to a PGP server, which can sign, encrypt or decrypt the payload, or verify the digital signature. After performing one of these actions, the PGP server can return the payload to Gentran Integration Suite, where it can be sent out to trading partners.

Creating a PGP Profile

1. From the Deployment menu, select **Adapter Utilities** > **PGP Profile Manager**.
2. The PGP Profile Manager displays. Next to Create a new PGP Profile, click **Go!**
3. Enter the field values as described in the following table:

Field	Description
Name	Name of this profile.

Field	Description
PGP Type	Select the type of PGP software you have installed: ◆ McAfee E-Business Server (version 8.6) ◆ McAfee E-Business Server (version 8.5.1) ◆ McAfee E-Business Server (version 8.5) ◆ McAfee E-Business Server (version 8.1) ◆ PGP Command Line Freeware (version 6.5.8) ◆ PGP® Command Line (version 9.5) - PGP Corporation **Note:** Gentran Integration Suite supports PGP Command Line (version 9.8). Select PGP® Command Line (version 9.5) - PGP Corporation to use PGP Command Line versions 9.5 and 9.8. Required.
PGP Executable	Command to be used to run PGP. Required. For example: `C:\Program Files\McAfee\McAfee E-Business Server\ebs` In the command, *ebs* is the executable command.
PGP Path	Directory where PGP Configuration file (pgp.cfg or PGPprefs.xml) is located. Required.
PGP Public Key Ring	Path and name of the PGP public key ring. Required. For example: `C:\Program Files\McAfee\McAfee E-Business Server\pubring.pkr`
PGP Secret Key Ring	Path and name of the PGP secret key ring. Required. For example: `C:\Program Files\McAfee\McAfee E-Business Server\secring.pkr`
PGP Random No. Seed	Path and name of the PGP random number seed. Required. For example: `C:\Program Files\McAfee\McAfee E-Business Server\randseed.rnd`
Secret Key Map Information	For signing purposes, you must add at least one secret key map. ◆ To add a secret key map, click **add**. The Key Map Info page displays. Enter the Key Name, Key ID, and passphrase for the key map and click **Save**. ◆ To edit a secret key map, click **edit**. The Key Map Info page displays. Update the information as necessary and click **Save**. ◆ To delete a secret key map, click **delete**. The Key Map Info page displays. Verify that this is the key map to be deleted and click **Delete**.
Conventional Key Map Information	For encryption using a conventional passphrase, you must add at least one conventional key map. ◆ To add a conventional key map, click **add**. The Key Map Info page displays. Enter the Key Name and Passphrase for the key map and click **Save**. ◆ To edit a conventional key map, click **edit**. The Key Map Info page displays. Update the information as necessary and click **Save**. ◆ To delete a conventional key map, click **delete**. The Key Map Info page displays. Verify that this is the key map to be deleted and click **Delete**.

4. After completing the Profile Manager configuration, review the settings on the last page and click **Finish**.

Editing a PGP Profile

1. From the Deployment menu, select **Adapter Utilities** > **PGP Profile Manager**.
2. The PGP Profile Manager displays. Next to List Alphabetically, click **Go!**
3. The list of PGP profiles displays. Next to the profile you want to edit, click **edit**.
4. Revise the fields displayed as necessary and click **Save** when finished.

Deleting a PGP Profile

1. From the Deployment menu, select **Adapter Utilities** > **PGP Profile Manager**.
2. The PGP Profile Manager displays. Next to List Alphabetically, click **Go!**
3. The list of PGP profiles displays. Next to the profile you want to delete, click **delete**.

Build 4321 or Higher

Add Resources without SI Restart

Dynamically Add, Remove, or Modify an XML Namespace for Web Services

Gentran Integration Suite now has the ability to dynamically add, remove, or modify an XML namespace for Web Services without restarting Gentran Integration Suite.

When Gentran Integration Suite gets a request for a namespace that it doesn’t recognize, it reloads the namespace properties, the customer_overrides properties, and all the extended properties files and checks for new namespaces. Gentran Integration Suite will store the new namespace in the cache for future use. Additionally, you can now refresh the namespaces in the properties files using a new OPS command that allows you the ability to add, modify, or remove namespaces in the properties files, you can also change these properties in the customer_overrides.properties file.

Adding a Namespace

Complete these steps to add a new namespace:

1. Create a business process similar to the example below:

```
<process name="namespaces_test_add">
<sequence>
<assign to="temp/@Algorithm" from="'http://www.w3.org/2000/09/xmldsig#test'"/>
<assign to="ds:Transforms/ds:Transform" from="temp/@*"/>
<assign to="ds1:Transforms/ds1:Transform" from="temp/@*"/>
</sequence>
</process>
```

2. Add a new namespace similar to the example below in the namespaces.properties file or in a new extended properties file.

Note: You can add a namespace to namespace.properties or namespace.properties_*_ext or customer_overrides.properties

```
ds1 = http://www.w3.org/2000/09/xmldsig_ds1#
```

3. Run the assigned business process. *namespaces_test_add* business process.
4. The following will appear in the Process Data if the business process is running successfully:

```
<ds1:Transforms xmlns:ds1="http://www.w3.org/2000/09/xmldsig_ds1#">
<ds1:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#test"/>
</ds1:Transforms>
```

Modifying a Namespace

Complete these steps to update an existing namespace:

1. Create a business process similar to the one below:

```
<process name="namespaces_test_update">
<sequence>
<assign to="temp/@Algorithm" from="'http://www.w3.org/2000/09/xmldsig#test'"/>
<assign to="ds:Transforms/ds:Transform" from="temp/@*"/>
</sequence>
</process>
```

2. Update an existing namespace similar to the following example in the namespaces.properties file.

```
ds = http://www.w3.org/2000/09/xmldsig_update#
```

3. From the install root directory, run the OPS command:

```
./bin/opscmd.sh -cREFRESHNAMESPACES -nnode1
```

4. Run the assigned business process.
5. The following will appear in the Process Data if the business process is running successfully.

```
<temp Algorithm="http://www.w3.org/2000/09/xmldsig#test"/>
<ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig_update#">
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#test"/>
</ds:Transforms>
```

Removing a Namespace

Complete these steps to remove an existing namespace:

1. Create a business process similar to the following example:

```
<process name="namespaces_test_remove">
<sequence>
<assign to="temp/@Algorithm" from="'http://www.w3.org/2000/09/xmldsig#test'"/>
<assign to="ds:Transforms/ds:Transform" from="temp/@*"/>
</sequence>
</process>
```

2. Remove an existing namespace similar to the following example in the namespaces.properties file.

```
ds = http://www.w3.org/2000/09/xmldsig_update#
```

3. From the install root directory, run the OPS command:

   ```
   ./bin/opscmd.sh -cREFRESHNAMESPACES -nnode1
   ```

4. The cache clears.
5. Run the assigned business process.
6. The business process fails because it cannot refer to the “ds” namespace.

JDBC Pools

Dynamically Add, Modify, and Remove JDBC Pools and Manage JDBC Pools with Effective Dates for Passwords

Gentran Integration Suite now has the ability to dynamically add, modify, remove JDBC Pools and Manage JDBC Pools with effective dates for passwords.

Adding JDBC Pools

Adding a New Database Pool to jdbc.properties

Complete these steps to add a new database pool to jdbc.properties:

1. From the Operations menu, select JDBC Monitor. The JDBC Monitor page appears. If you want to verify that the database you want to add does not already exist, click the link next to View JDBC Report.
2. In the *customer_overrides.properties* file, create a new database connection pool. For additional information, see *Adding New Database Pools in the Lightweight Java Database Connectivity (JDBC) Adapter.*
3. After adding the pool properties in *customer_overrides.properties*, go to JDBC monitor page and click the **Refresh JDBC Pools** button, or run the REFRESHJDBC OPS command from the install root directory:

   ```
   ./bin/opscmd.sh -cREFRESHJDBC -nnode1
   ```

Modifying a Database Pool in jdbc.properties

Complete these steps to update a Database Pool in jdbc.properties:

1. In the *install_dir*/install/properties directory, locate the *customer_overrides.properties* file.
2. Open the *customer_overrides.properties* file in a text editor.
3. Modify the properties you want to change in the customer pools list of properties.

Note: You can modify any properties for user added pools. For system pools, you cannot change the database type (for example, Oracle to MSSQL), but you can change the database type for customer pools.

4. Save the *customer_overrides.properties* file.
5. After modifying the pool properties in customer_overrides.properties, go to JDBC monitor page and click the **Refresh JDBC Pools** button, or run the REFRESHJDBC OPS command from the install root directory: ./bin/opscmd.sh -cREFRESHJDBC -nnode1

Removing Pool from jdbc.properties

Complete these steps to remove a customer pool from jdbc.properties:

1. In the *install_dir*/install/properties directory, locate the *customer_overrides.properties* file.
2. In the *customer_overrides.properties* file, delete the pool you want to remove.

Note: Verify that all the pool properties are removed for the pool you want to delete, including, jdbc.properties_*_ext, jdbc_customer.properties and customer_overrides.properties files.

3. Save the *customer_overrides.properties* file.
4. After removing the pool properties in *customer_overrides.properties,* go to JDBC monitor page and click the **Refresh JDBC Pools** button, or run the REFRESHJDBC OPS command from the install root directory: `./bin/opscmd.sh -cREFRESHJDBC -nnode1`

Controlling User and Password Credentials with Effective Dates

You can now change database passwords on a scheduled basis in Gentran Integration Suite. When you add or modify a pool, you now can control user and password credentials with effective dates. Multiple user and password credentials are associated with a pool. A date/time entry indicates to Gentran Integration Suite when to start using that credential for new connections. This applies primarily to external pools, although Gentran Integration Suite database pools will also work.

You can use the following variables for the date format:

- 15:00:00 3/16/09
- 3/16/09 15:00:00
- 3/16/2009 15:00:00
- Sat, 12 Aug 1995 13:30:00 GMT
- Sat, 12 Aug 1995 13:30:00 GMT+0430

Note: Other formats may be used as long as they follow the Internet Engineering Task Force (IETF) standard date syntax. For additional information see http://www.ietf.org/rfc/rfc3339.txt

Pool Property	Description
newDBPool.password.1= <new password>	You can specify alphabets and combination of alphabets and numbers for the password. You can use numbers for newDBPool.password.1 or newDBPool.password.2 as well as following examples: ◆ newDBPool.password.a=password_a ◆ newDBPool.effective.a=1/01/2005 09:35:00 ◆ newDBPool.password.b=password_b ◆ newDBPool.effective.b=02/01/2009 09:35:00 ◆ newDBPool.password.c=password_c ◆ newDBPool.effective.c=06/18/2009 11:07:00
newDBPool.effective.1= <The date for the new password starts to take affect>	You can specify alphabets and combination of alphabets and numbers for the password. You can use numbers for newDBPool.password.1 or newDBPool.password.2 as well as following examples: ◆ newDBPool.password.a=password_a ◆ newDBPool.effective.a=1/01/2005 09:35:00 ◆ newDBPool.password.b=password_b ◆ newDBPool.effective.b=02/01/2009 09:35:00 ◆ newDBPool.password.c=password_c ◆ newDBPool.effective.c=06/18/2009 11:07:00

System Logs and Error Logs

System Logs

When applicable, the following items are logged in system logs:

- Logging the switch from one credential to the next, as well as the initialization of the pool dates and user IDs being used (not the passwords).
- Logging if the connection is expired when it returns to the pool.
- Logging if two passwords have the same effective dates. In this case, the system randomly selects a password and log that two passwords had the same effective dates. Additional logs on passwords and effective dates may be added.
- Logging when pool properties are changed. If you changed the pool related property like maxSize, or lifespan the following message appears in the system log: "for pool name ***** <PROPERTY> is changed".

Error Logs

The following list provides descriptions of the different types of errors that can be logged:

- Failed to add the pool <pool name>
- Failed to delete the pool <pool name>
- Failed to modify the pool <pool name>
- Failed to create the connections from the pool <pool name>

Log Changes Made During System Patch

Patch Changes Report

This new report will be used by customers to obtain information if they need to rollback a patch. The patch report can be found in the <install>/patch_reports folder. The report contains the following patch information:

- Patch ID
- Patch Changes
- Number of files deleted
- Number of JARs removed
- Number of JARs added
- Number of files added
- Number of files changed
- Number of properties added
- Number of business processes added
- Number of service instances added
- Number of service definitions added
- Number of templates added
- Number of reports added
- Number of maps added
- Number of schemas added
- Number of business rules added

For example, <install>/patch_report/<1234523962118> contains Patch_Report.html. When you open this html file, you can view the patch information.

Example: Patch Changes Report

The following is an example of a Patch Changes Report.

```
Summary of Changes
Patch ID: Platform_2.0
Patch Changes: 1287
```

```
Number of Files Deleted: 0
Number of JARs Removed: 2
Number of JARs Added: 0
Number of Files Added: 3
Number of Files Changed: 3
Number of Properties Added: 4
Number of BPs Added: 4
Number of Service Instances Added: 2
Number of Service Definitions Added: 3
Number of Templates Added: 0
Number of Reports Added: 0
Number of Maps Added: 3
Number of Schemas Added: 3
Number of Business Rules Added: 0
________________________________________
List of JARs Removed:
JAR Removed: /SAMPLE_INSTALL_1/jar/jaf/1_0_2/activation.jar
Time: Wed May 13 15:23:08 EDT 2009
JAR Removed: /SAMPLE_INSTALL_1/jar/commons_logging/1_0_3/commons-logging-api.jar
Time: Wed May 13 15:23:08 EDT 2009
________________________________________
List of Files Added:
File Added: /SAMPLE_INSTALL_1/bin/sql/fix_db2_schema.sql
Time: Wed May 13 15:21:30 EDT 2009
File Added: /SAMPLE_INSTALL_1/bin/sql/fix_db2iseries_schema.sql
Time: Wed May 13 15:21:30 EDT 2009
File Added: /SAMPLE_INSTALL_1/bin/errorQueueManager.sh.in
Time: Wed May 13 15:21:30 EDT 2009
________________________________________
List of Files Changed:
File Changed: /SAMPLE_INSTALL_1/properties/lang/en/Reports_en.properties
File Changed: /SAMPLE_INSTALL_1/properties/lang/es/Reports_es.properties
File Changed: /SAMPLE_INSTALL_1/properties/lang/fr/Reports_fr.properties
________________________________________
List of Properties Added:
Property Added: /SAMPLE_INSTALL_1/properties/filesToRemove.txt
Property Added: /SAMPLE_INSTALL_1/properties/filesToRemove.txt.in
Property Added: /SAMPLE_INSTALL_1/properties/csr.properties.sample
Property Added: /SAMPLE_INSTALL_1/properties/csr.properties.sample.in
________________________________________
List of BPs Added:
BP Added: Schedule_AssociateBPsToDocs.bpml version: 4
Time: Wed May 13 15:23:07 EDT 2009
BP Added: Recovery.bpml version: 17
Time: Wed May 13 15:23:07 EDT 2009
BP Added: Schedule_AutoTerminateService.bpml version: 10
Time: Wed May 13 15:23:07 EDT 2009
BP Added: Schedule_DBMonitorService.bpml version: 1
Time: Wed May 13 15:23:08 EDT 2009
________________________________________
List of Service Instances Added:
Service Instance Added: RetentionProcessor version: 2
Time: Wed May 13 15:23:28 EDT 2009
Service Instance Added: MESAHttpServerAdapter version: 1
Time: Wed May 13 15:25:11 EDT 2009
________________________________________
```

```
List of Service Definitions Added:
Service Definition Added: LockServiceType
Time: Wed May 13 15:22:58 EDT 2009
Service Definition Added: XAPIServiceType
Time: Wed May 13 15:22:59 EDT 2009
Service Definition Added: CleanLockServiceType
Time: Wed May 13 15:22:59 EDT 2009
```

```
List of Templates Added:
Template Added: Normalize
Time: Wed May 13 15:23:26 EDT 2009
Template Added: Derive
Time: Wed May 13 15:23:26 EDT 2009
```

```
List of Maps Added:
Map Added: IBMPutResponseToXML
Time: Wed May 13 15:24:05 EDT 2009
Map Added: http_headers
Time: Wed May 13 15:24:36 EDT 2009
Map Added: OracleHttpHeaders
Time: Wed May 13 15:24:51 EDT 2009
```

```
List of Schemas Added:
Schema Added: E5_V20_Acknowledge_Result.dtd from file: E5_V20_Acknowledge_Result
Time: Wed May 13 15:24:36 EDT 2009
Schema Added: E5_V20_Acknowledge_Submit.dtd from file: E5_V20_Acknowledge_Submit
Time: Wed May 13 15:24:36 EDT 2009
Schema Added: E5_V20_APIs_Result.dtd from file: E5_V20_APIs_Result
Time: Wed May 13 15:24:36 EDT 2009
```

Optimizing and Controlling the System Threads

Optimizing System Threads

Out of memory situations are very difficult to diagnose. Gentran Integration Suite 4.3 creates around 300 threads that can be grouped under system threads, adapter threads, common JVM threads, third party software threads, and several other threads that occur only once for different purposes.

The following table lists the threads created in Gentran Integration Suite 4.3 and their source.

Thread created by	Thread name	Count
ActiveMQ	ActiveMQ transport	80
	ActiveMQ Session Task	11
Jetty	SessionScavenger	47
	ConduitStreamListener	16
	SocketListener	10

Thread created by	Thread name	Count
JGroup	Various Jgroup Handlers	22
JetSpeed	RunnableThread	10
Perimeter PS Dispatcher	Various Adapters	13
Business process queues	ReschedulingThread	10
B2B	B2B http Servlet Thread	3
	FIFOTaskListener	10
	QueueThread:queue	11
System	RMI	7
	Timer	7
Others	From various components	30
Total		**287**

Controlling the Threads

Several threads created by Gentran Integration Suite for various purposes may not be required always and they can be controlled wherever required. This will enhance the Gentran Integration Suite's performance considerably.

Following are the concepts described in this topic:

- ActiveMQ Threads
- Jetty Threads
- JGroup Threads
- JetSpeed Threads
- Adapter Threads
- Business Process Queue Threads
- FIFOTaskListener and Queue Threads
- RMI Threads
- Timer Threads

ActiveMQ Threads

ActiveMQ threads can be controlled by running ActiveMQ broker in a separate JVM. No additional setup or configuration is necessary to run ActiveMQ in a separate JVM. Gentran Integration Suite build installation process configures the system to use it out of the box for both cluster ActiveMQ and non-cluster ActiveMQ.

However, if you plan to use clustering, you may choose a different configuration by editing the activemqconfig.xml file. Before editing this file, read the readme_cluster.txt file. It contains information about how to use the options in the activemqconfig.xml file. Both files are located in the *install_dir*/install/activemq/conf folder.

Mandatory Startup for ActiveMQ

The startActivemqMandatory parameter in the *install_dir*/install/properties/activeMQ.properties file controls the remaining processes and starts them if ActiveMQ fails to start. The default value for this parameter is false. To change this, you can create an extension file (for example, activeMQ.properties_clumpName_ext.in or customer_overrides.properties file) and specify the following entry:

```
startActivemqMandatory=true|false
```

Where:

true = If activemq fails to start, the rest of processes will not be started.

false = If activemq fails to start, continue to start the rest of the processes.

Standalone ActiveMQ Commands

You can start and stop standalone ActiveMQ server by running the following commands.

1. To start the standalone ActiveMQ server, ensure that ActiveMQ dynamic configuration file (activemqconfig.xml.in) and ActiveMQ configuration XML file (activemqconfig.xml) are present in the *install_dir*/install/activemq/conf directory. Run the following command from *install_dir*/install/bin directory:
    - For UNIX, run startActiveMQ.sh
    - For Windows, run startActiveMQWindowsService.cmd
2. To stop the standalone ActiveMQ server, run the following command from <*install_dir*>/install/bin directory:
    - For UNIX, run stopActiveMQ.sh
    - For Windows, run stopActiveMQWindowsService.cmd

Note: You can also start or stop ActiveMQ service from Windows Service Manager.

Using an External ActiveMQ Environment

ActiveMQ is bundled along with Gentran Integration Suite. However, you can use a different ActiveMQ environment by modifying certain files.

Note: It is recommended that users who are familiar with ActiveMQ environment perform this task.

To use an external ActiveMQ environment in UNIX:

1. Shut down Gentran Integration Suite.
2. Change ACTIVEMQ_PORT in sandbox.cfg and point to your own ActiveMQ environment.
3. Remove startActiveMQ.sh from install/bin/run.sh.in.
4. Remove stopActiveMQ.sh from install/bin/hardstop.sh.in.

5. Change remote.protocol_config=client connection in the install/event.properties.in file to your ActiveMQ environment.
6. Run install/bin/setupfile.sh.
7. Restart Gentran Integration Suite.

To use an external ActiveMQ environment in Windows:

1. Shut down Gentran Integration Suite.
2. Change ACTIVEMQ_PORT in sandbox.cfg and point to your own ActiveMQ environment.
3. Remove "net start "%ACTIVEMQ_SERVICE_NAME%" >NUL" from install/bin/startWindowsService.cmd.
4. Remove "net stop /y "%ACTIVEMQ_SERVICE_NAME%"" from install/bin/stopWindowsService.cmd.
5. Change remote.protocol_config=client connection in the install/event.properties.in file to your ActiveMQ environment.
6. Run install/bin/setupfile.cmd.
7. Restart Gentran Integration Suite.

Changing the Cluster Setting for Bundled ActiveMQ

The configuration file for the bundled ActiveMQ is install/activemq/conf/activemqconfig.xml. You can manually change the broker setting to fit your business requirements. You can also extend this file with activemqconfig_clumpname_ext.xml to configure your own beans.

Note: Read install/activemq/conf/readme_cluster.txt file before making any changes.

Jetty Threads

Gentran Integration Suite 4.3 uses Jetty version 4.2.24. Jetty version 4.2.24 when compared to latest versions like Jetty version 6.1.8 offers limited control on the number of threads created. However, you can control the numbers of threads created by Jetty listeners. Further, the large numbers of SessionScavenger and ConduitStreamListener threads are not controlled by listener thread parameters. They are created for web applications and HTTP Servlet adapters.

You can control the number of threads created by Jetty Listeners by modifying the following configuration parameters in noapp.properties file:

```
# specify the minimum number of threads for Socket Listeners for Jetty
jetty_min_threads = 5
# specify the maximum number of threads for Socket Listeners for Jetty
jetty_max_threads = 100
```

Note: You cannot modify the jetty_min_threads value. However, you can modify the jetty_max_threads value in the available range from 5 - 100.

JGroup Threads

JGroup is a reliable multicast communication toolkit and is used in Gentran Integration Suite cluster environment. You cannot control the number of threads created by JGroup.

JetSpeed Threads

Jetspeed is the portal engine used in Gentran Integration Suite dashboard interface. The jetspeedresources.properties file controls the number of threads created by JetSpeed.

You can control the number of threads created by JetSpeed by modifying the following configuration parameters in install/noapp/deploy/dashboard/webapp/WEB-INF/conf/JetspeedResources.properties file.

```
#Specify the initial number of threads to create
services.ThreadPool.init.count=5
#Specify the maximum number of threads to create
services.ThreadPool.max.count=20
#Specify the minimum number of threads to keep as spare until you hit the maximum
services.ThreadPool.minspare.count=5
```

Note: You cannot modify the services.ThreadPool.init.count value. However, you can modify the services.ThreadPool.max.count value in the available range from 5 - 20.

After modifying, you should remove the install/noapp/deploy/dashboard/webapp/WEB-INF/conf/JetspeedResources.properties from install/noapp/deploy/dashboard.war file to make your change take effect.

Adapter Threads

Several Jetty and Timer threads are created by adapters. You can disable the adapters that are not required to run your business processes thereby controlling the number of threads created by the adapters.

The following adapters can be disabled to reduce the number of threads created:

Note: Disabling an adapter in the following list can reduce at least one or two threads in most cases.

- FIFO Routing
- FIFO Error Queue Listener
- HTTP Communications Adapter
- B2B HTTP Communications Adapter
- SFTP Client Adapter
- FTP Client Adapter
- Map Test Http Server
- ebXML Http Server Adapter
- MBI Http Server Adapter
- SOA Http Server Adapter
- SOA SSL Http Server Adapter
- RN Http Server Adapter

- Http Server Adapter
- SWIFTNet Http Server Adapter

Business Process Queue Threads

Gentran Integration Suite creates nine regular business process queues and one internal queue called wait queue for wait service. You cannot control the number of threads created for business processes.

FIFOTaskListener and Queue Threads

The FIFORouting adapter creates and controls ten queues for FIFO processing. Each FIFO queue creates a FIFO task listener and every task listener creates a consumer at startup. You can configure the number of queues to reduce the number of threads. Additionally, you can disable the FIFORouting adapter if you are not using it thereby turning off all the queues created by the adapter.

You can control the number of threads by modifying the following configuration. The number of queues configured depends on the system load.

```
#In customer_overrides.properties, additional queues can be added by adding, for
example:
#fifo.workflow.taskqueue.11=FIFO.GIS.QUEUE.11
#fifo.workflow.taskqueue.12=FIFO.GIS.QUEUE.11
#Note, queues cannot be reduced in customer_overrides.properties but the names can be
changed and must be unique
workflow.taskqueue.1=FIFO.GIS.QUEUE.1
workflow.taskqueue.2=FIFO.GIS.QUEUE.2
workflow.taskqueue.3=FIFO.GIS.QUEUE.3
workflow.taskqueue.4=FIFO.GIS.QUEUE.4
workflow.taskqueue.5=FIFO.GIS.QUEUE.5
workflow.taskqueue.6=FIFO.GIS.QUEUE.6
workflow.taskqueue.7=FIFO.GIS.QUEUE.7
workflow.taskqueue.8=FIFO.GIS.QUEUE.8
workflow.taskqueue.9=FIFO.GIS.QUEUE.9
workflow.taskqueue.10=FIFO.GIS.QUEUE.10
```

RMI Threads

The RMI threads are system generated threads for JNDI. You cannot control the number of RMI threads.

Timer Threads

The timer threads are created when Gentran Integration Suite starts. It is not recommended to control these threads as they are necessary for Gentran Integration Suite to run smoothly.

The following timer threads are created when Gentran Integration Suite starts:

- Check Gentran Integration Suite component licenses and generate messages for users when one or more licenses is about to expire.
- Roll the log service files.

- Gather YCP statistics used by the entity framework.
- Monitor resources and detect database connections or database connection leaks.
- Schedule business processes.
- JNDI service timer.
- ActiveMQ timer.

QueueWatcher

Monitoring Queues using Queue Watcher

Queue Watcher monitors various components in Gentran Integration Suite as well as manages queue configuration settings.

Accessing Queue Watcher

To access Queue Watcher, do the following:

1. Open your web browser to http://host:port/queueWatcher, where host:port is the IP address and port number where Gentran Integration Suite resides on your system. A login page appears.

Note: Any user with Administrator privileges can login to the Queue Watcher application, provided he has all the necessary permissions or is a part of the Sterling Intergrator Administrator group.

2. Type your username and password. The Queue Watcher displays the following information:

Heading	Description
View Active Threads for All Queues	Shows a list of all active queue threads. When selected, you can review the following information: ◆ QueueName – Shows the queue name. ◆ Min – Minimum number of threads available for the queue. The threads will be honored even if they are higher than MaxThreads (global maximum queue threads). The minimum number of threads cannot be higher than the maximum number. The fairness calculation does not apply for minimum threads. ◆ Used – Number of business processes currently running on a thread. ◆ Calc – Fairshare thread calculation for the queue. Fairshare is based on concurrent activities on all queues and is dynamically updated. ◆ Pool – Number of threads in a queue’s pool. Threads timeout if they are not used. ◆ Max - Maximum number of threads used by the queue. Calc determines the maximum concurrent threads that is dynamically calculated. ◆ Queue Depth - Number of business processes waiting for a thread in the queue. ◆ List of Working Threads – List of business processes currently running on a thread.
Pause All Queues	Use this option to stop queues. Stopping individual queues is not possible.

Heading	Description
Restart All Queues	Use this option to restart queues. Restarting individual queues is not possible. DBResources will use this command if the database becomes unavailable.
View Default Queue Configuration Parms	Shows the parameters set for all of the queues.
View Active Queue Configuration Parms	Shows the current queue configuration.
View list of Workflow IDs that recover would see in the queue	Shows the workflow ID when it is run or moved to another node in the cluster. Valid values are: ◆ Executed ◆ Moved to another (cluster) node
View Context Cache Entries	Shows the coxtent cache entries. **Note:** If entries show up as invalid they are still correct and do not indicate an error. ◆ Soft Reference Cache Slots in use - Workflow Context (wfc) is saved into this queue (hashtable) and can be recovered from it. This is the fastest back queue. If required, the garbage collector can acquire more heap space from this queue. The workflow contexts are not serialized on this queue. ◆ In Memory Cache Bytes in use - This memory cache holds the workflow contexts with a size lesser than the configured threshold if it is has space. The workflow contexts are serialized on this queue. ◆ Disk Cache Bytes in use - This cache holds workflow contexts larger than the defined threshold. The workflow contexts are serialized on this queue.
Wait Queue	Shows the workflow IDs when the Wait Service is being processed. The Wait Service will only appear if the wait interval is less than 30.
Queue_1 – Queue_9	Shows running and waiting (for available thread) business processes.
View Heap Memory Level	Shows heap usage in the system. Business processes can run if heap space and CPU resources are available.
View Memory Generation	Shows JVM information specific to garbage collection and memory generation.
View System Information	Shows system level information from the JVM.
View VM Status	Shows Java Virtual Machine status.
View Manager Properties	Shows the list of properties from the noapp.properties file.
View Queue Threads	Shows a list of all queue threads.
View All Threads	Shows a list of all active threads.
View Stateful Adapters	Shows a list of stateful adapters running in the system. Stateful Adapters are adapters with an adapterType of STATEFUL, for example, the HTTP adapter.
View Stateless Adapters	Shows a list of stateless adapters running in the system. Stateless adapters are adapters with an adapterType of STATELESS, for example, the File System Adapter.
View Disabled Adapters	Shows a list of adapters that are currently marked as disabled (not running).

Heading	Description
View DB Pool Information	Shows usage information for the configured DB pools.
View Cluster Multicast Data	Shows load data broadcast from the nodes when running in a cluster.
Config Queue	Configure the queue parameters to tune performance. The parameters are not persisted and are reset when Gentran Integration Suite restarts. **Note:** The Config Queue, Reset Queue, and Step Monitor fields can only be used one at a time. To submit the data entered, you must click Enter.
Reset Queue	Resets the queue to default values. The parameters are not persisted and are reset when Gentran Integration Suite restarts. **Note:** The Config Queue, Reset Queue, and Step Monitor fields can only be used one at a time. To submit the data entered, you must click enter on your keyboard.
Step Monitor	Shows the list of business processes and workflow contexts in the queue. **Note:** The Config Queue, Reset Queue, and Step Monitor fields can only be used one at a time. To submit the data entered, you must click enter on your keyboard.
View Properties	Shows a list of all available property file names. Select a property from the list, then click Send.
View Common Properties	Shows a list of the named common property files. Select a property from the list, then click Send.

Enabling Queue Watcher

Queue Watcher allows you to enable the monitoring and management functionality from Gentran Integration Suite without having to restart the system for it to take affect.

To enable Queue Watcher without restarting Gentran Integration Suite:

1. Access the Queue Watcher tool. See Accessing Queue Watcher for additional information.
2. Click the **Enable Queue Watcher** button. The page refreshes and shows the Queue Watcher page.

Disabling Queue Watcher

Queue Watcher allows you to disable the monitoring and management functionality from Gentran Integration Suite without having to restart the system for it to take affect.

To disable Queue Watcher without restarting Gentran Integration Suite:

1. Access the Queue Watcher tool. See Accessing Queue Watcher for additional information.
2. Click the **Disable Queue Watcher** button. The Queue Watcher tool is disabled.

Reviewing System Information

Use the System Troubleshooting page to review system information and to view troubleshooting system issues in Gentran Integration Suite. To access this page, click **Operations** > **System** > **Troubleshooter**.

From the System Troubleshooting page, you can:

- Access system information on different nodes in a clustered environment.

  You can view system information on different nodes from any node in the clustered environment.
- Stop Gentran Integration Suite
- Access database usage statistics

  If you are running DB2 as your database, the database usage statistics always shows as unavailable in the System Troubleshooting page.
- Access business process queue and usage statistics
- Stop a business process
- View system classpath information
- View system JNDI tree information
- View environment statistics, including cache and memory used
- View adapter information
- View perimeter servers information
- View how long since archive, index and purge completed

This page has been redesigned to provide quicker access to system information. Instead of loading all of the system information at once, this page now provides links to key areas of system information. When accessed, a pop-up window now appears with the information you selected. This has greatly reduced the load time of the System Troubleshooting page.

The System Troubleshooting page is separated into different areas. The following table gives a general description of each area. More detail is given about each area in later sections.

Area	Information
Select Node	**Note:** The Select Node list displays only if you are working in a clustered environment. Your selection determines which node's information displays in the remainder of the System Troubleshooting page. The select node list enables you to select a node in a clustered environment triggering which node's information to display in the System Troubleshooting page. For example, if you have two nodes in a cluster (Node 1 and Node 2) and you want to view the System Troubleshooting page for Node 2, select Node 2 from the list and the System Troubleshooting page for Node 2 displays. If you want to view Node 1 information, select Node 1 from the list and the System Troubleshooting information for Node 1 displays.
Stop the System	Issues a system shutdown request.

Area	Information
Host Information	The System Status area displays the following information and options: ◆ Host Information: Includes start time, uptime, hostname, directory location, and memory usages **Note:** To refresh the system status, click **Refresh Status**.
Classpath	Displays the system classpath and DCL configuration.
JNDI Tree	Displays the content of the JNDI tree.
Database Usages	Displays the database space usage, business process eligibility for index and purge.
Business Process Queue Usage	Displays disk usage, memory usage, and queue statistics.
Business Process Usages	Displays count of business process by state.
Cache Usages	Displays size and hit rate for object caches.
Threads	Displays active processes at a thread level.
Clean-Up Processes Monitor	Displays state of system clean-up processes.
Controllers	Display list of system controller.
Adapters	Displays list of adapters and ability to manage them.
Perimeter Server Status	**Note:** The information in this area displays only after you have added a perimeter server to Gentran Integration Suite. The Perimeter Servers area displays the following information: ◆ Cluster Node name (in a clustered environment only) ◆ Whether the perimeter server is on or off ◆ State, either enabled or disabled ◆ Name of the perimeter server ◆ Last Activity

Stopping Gentran Integration Suite From the System Troubleshooting Page

You can stop Gentran Integration Suite using the System Troubleshooting page. Stopping Gentran Integration Suite in this manner stops Gentran Integration Suite using the softstop script, allowing all business processes to complete before stopping the system.

CAUTION:

Using the Stop the System option stops only the Gentran Integration Suite interface immediately, while all business processes in progress run until complete. After all business processes’ current services complete, Gentran Integration Suite stops. To stop the system and all processing immediately, in the *install_dir*/bin directory, run the hardstop script. All processes that have not completed will stop and may need to be restarted.

To Stop Gentran Integration Suite using the System Troubleshooting page:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Stop the System**.
3. In the message asking if you want to stop Gentran Integration Suite, click **OK**.
4. The interface stops immediately, but all business processes that are in progress complete before the system stops.

Viewing Host Information

Note: If you are working in a clustered installation of Gentran Integration Suite, the information that displays is determined by the node you select from the Select Node list.

Host Information displays the current operational status of the processing environment for your installation of Gentran Integration Suite. The System Troubleshooting page displays separate information for each installation.

To view Host Information:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Host Information**.

The following information is provided for each installation::

- The cluster node name, if you are working in a clustered installation of Gentran Integration Suite.

Note: The cluster node list displays only if you are working in a cluster. After you set up your cluster, the select cluster node list displays.

- Host - The name of the host on which a specific installation resides.
- Location - The location or path of the installation.
- State - The running state of the installation, either Active (available for processing) or Inactive.
- Memory in use - The amount of memory used by Gentran Integration Suite.
- Active threads - The number of concurrent threads that are active.

Viewing the System Classpath

You can view the system classpath for debugging purposes and to verify whether third-party libraries are available in the classpath.

To view the system classpath:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Classpath**.

   Information displays about the System Class Path and the Dynamic Class Loader.

Viewing the System JNDI Tree

You can view the system JNDI Tree for debugging purposes and to verify whether the expected resources are in the JNDI tree (for example, adapters or pool names).

To view the system JNDI Tree:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **JNDI Tree**.

   The system JNDI Tree displays, showing the JNDI name and class name pairs.

Viewing a Node JNDI Tree in a Clustered Environment

You can view a specific node's JNDI Tree for debugging purposes and to verify whether the expected resources (for example, adapters or pool names) are in the JNDI tree. This option is available only in a clustered environment.

To view a node JNDI Tree in a clustered environment:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **node#**, where # is the number of the node you want to view information about.

   The node's JNDI Tree displays, showing the JNDI name, class name pairs, and the node name.

Viewing Database Usage Statistics

Note: Database usage statistics are not available for DB2.

Database usage statistics show how your database is performing, including database insert information, database capacity, and environment pool usage. Gentran Integration Suite uses pools to store database connections. To change pool settings, you must manually edit the configuration files and restart the system.

To view database usage statistics:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Database Usage**.

Note: If you have the displayGraphics property located in the *install_dir*/properties/ui.properties file set to true, the Database Usage page displays in graphic format; otherwise, the Database Usage page displays in text format. The default is true for Linux, Sun, HP, and Windows operating systems. The default is false for AIX and iSeries operating systems.

The Database Usage report displays, showing the following information from a unit test of the database:

- Average time it takes to perform the number of database inserts in the unit test
- Number of inserts performed to the database in the unit test

Note: You can change the value in the dbAccessLoopCnt property in the *install_dir*/properties/ui.properties.in file. After you make your changes, in the *install_dir*/bin directory, run the setupfiles script.

- Size of inserts performed to the database in the unit test

Note: You can change the value in the dbAccessDataSize property in the *install_dir*/properties/ui.properties.in file. After you make your changes, in the *install_dir*/bin directory, run the setupfiles script.

- Size of the database and the amount of the database used in megabytes

  Green – Normal range

  Yellow – Warning range

  Red – Critical range

- Number of business processes that are waiting to be archived, indexed, or purged
- Size in megabytes of the following pools and the number of requests that had to wait for the following pools:

  gentranTPPool

  *database*ArchivePool

  *database*Pool

  *database*Pool_local

  *database*Pool_NoTrans

  *database*Pool_Select

  *database*UIPool

Note: The *database* portion of the pool names changes depending on the database you are using. For example, if the database is MySQL, you see mysqlPool.

Viewing Business Process Queue Usage

The Business Process Queue Usage page enables you to diagnose problems with your business process queues.

To view Business Process Usage:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Business Process Usage**.

The page provides the following queue information.

- The amount of memory available for cache and the amount consumed.
- The amount of disk space available for cache and the amount consumed.
- The average wait time based on priority.

- The average BP execution cycle time based on priority. The average BP execution cycle time may include the execution times of several steps. It captures the average time that BPs are active on threads before being rescheduled.
- The number of business processes in priority queues.
- The number of business processes that ran without being cached and the number that are currently in cache. Cache location is also specified so that you can determine the number of business processes that were found in the soft reference cache, in the disk cache, and in the memory cache.
- Number of business processes within the data size ranges that have been processed.

Viewing Business Process Usage

The Business Process Usages page enables you to review the state of a business process and the process count. If a link is enabled in the Process Count area, you can select it to view affected business processes and manage them.

To view Business Process Usage:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Business Process Usage**.

Viewing Cache Usage Information

Gentran Integration Suite uses caches to hold information that is frequently requested by the system. The Cache Usage report displays these statistics for each cache: count, number of requests, and number of successful hits. To change cache settings, see Performance Tuning Utility. You can view the cache usage information to monitor the use of various cache types.

To view the cache usage:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click **Cache Usage**.

   The Cache Usage report displays the following information for each cache type:

   - Cache name – Name of the cache
   - Count – Number of objects in the cache
   - Requests – Number of times an object was requested from the cache, regardless of success
   - Hits – Number of times an object was requested from the cache and found.

Viewing Threads

To view threads in Gentran Integration Suite:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click **Threads**.

   The Threads report displays.

Viewing Clean-Up Processes Monitor Details

You can view how long it has been since the completion of different cleanup processes, including archiving, purging and indexing. This helps you see on one screen whether these processes are running and completing.

To view when a cleanup process completed:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Clean-Up Processes Monitor**.

   The Clean-Up Processes Monitor Details window displays, showing the status, workflow (or cleanup process) name, the date and time when the workflow was last run, and the workflow ID.

   The Status column has the following values:

   - Red – More than four times the scheduled interval has elapsed without a successful execution.
   - Yellow – More than three times the scheduled interval has elapsed without a successful execution.
   - Green – The last scheduled instance completed successfully.
   - Gray – The process has never completed any scheduled instance or has never been scheduled.

Note: Red or Yellow status of a process may mean that the process is not able to complete data cleanup tasks. If this condition continues after you have taken steps to resolve any errors, contact IBM Customer Support.

Refreshing a Controller

You can refresh controllers running in your environment using the System Troubleshooting page.

To refresh a controller:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the System Troubleshooting page, click **Controllers**. The controller page appears.
3. Click the Refresh icons (arrows) for the Controller you want to refresh.

Viewing Adapters

You can view the adapters to verify accuracy or to plan changes as needed.

To view adapter settings:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click **Adapters**.
3. On the Adapters page, click the name of the adapter that you want to view.

Enabling an Adapter

You can enable a disabled adapter using the System Troubleshooting page.

To enable an adapter:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click **Adapters**.
3. On the Adapters page, next to the adapter that you want to enable, in the On/Off column, select the check box.

Disabling an Adapter

You can disable an enabled adapter using the System Troubleshooting page.

To disable an adapter:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click Adapters.
3. On the Adapters page, next to the adapter that you want to disable, in the On/Off column, select the check box.

Perimeter Server Status

Note: If you are working in a clustered environment, the information that displays is determined by the node you select from the Select Node list.

Note: If you are not using a perimeter server, local appears as the perimeter server name, and the server state is Enabled.

The Perimeter Servers area of the System Troubleshooting page displays the following information about your perimeter servers:

- Name of the cluster node with which the perimeter server is associated
- State of the perimeter server – Enabled or Disabled
- Name of the perimeter server
- Date and time of the last activity the perimeter server performed

Viewing Perimeter Server Settings

You can view the perimeter server settings to verify accuracy or to plan changes as needed.

To view perimeter server settings:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. In the Perimeter Servers area, in the Name column, click the name of the perimeter server that you want to view.

Enabling a Perimeter Server

You can enable a disabled perimeter server using the System Troubleshooting page.

To enable a perimeter server:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click **Perimeter Server Status**.
3. On the Perimeter Servers page, next to the perimeter server that you want to enable, in the On/Off column, select the check box.

Disabling a Perimeter Server

You can disable an enabled perimeter server using the System Troubleshooting page.

To disable a perimeter server:

1. From the Administration menu, select **Operations** > **System** > **Troubleshooter**.
2. On the Troubleshooting page, click **Perimeter Server Status**.
3. On the Perimeter Servers page, next to the perimeter server that you want to disable, in the On/Off column, select the check box.

Build 4319 or Higher

Data Sweeper Enhancement

Data Sweeper is a scheduled system service that cleans up data that is not in use. The data may not have been cleaned up by other system clean up processes due to the lack of any continued associations. Data Sweeper corrects known entity relationship issues within the database that could potentially cause performance problems and unnecessary database expansion.

How Data Sweeper Works

Data Sweeper may be run from the command line (`dataSweeper.sh` or `dataSweeper.cmd`) or used in a business process. The command line utility allows you to run the service even when Gentran Integration Suite is down. (For MySQL, it will automatically start the database.) For continued processing in the background, the Data Sweeper service may be used in a scheduled business process.

The Data Sweeper service is built to flexibly run specialized sweepers each of which have a specific task. This flexibility allows you to run some or all of the sweepers as needed. The flexible framework also allows Sterling to add and update sweepers, building on the basic structure.

When the Data Sweeper service runs, it references the `dataSweeper.properties` file for information on which sweepers to run. The properties file contains information about the parameters for each individual sweeper. It also specifies whether or not it is appropriate to run that individual sweeper in the requested mode.

Some sweepers are not recommended to be run while the affected Gentran Integration Suite instance is running. These sweepers are designated with an OFFLINE mode. Sweepers that safely complete their work in a running Gentran Integration Suite instance are designated to run in all modes. Sweepers that should only be run upon the recommendation of Gentran Integration Suite support are designated with a FORCED mode. Such sweepers can only be run via the command line and must be manually invoked. You may switch modes when allowing sweepers to run in an active instance, but always perform this action with the advice of Sterling Support.

Data Sweeper is intended to be used on a short-term basis until a resolution for the issue is applied via the standard patch cycle.

Advantages of Data Sweeper

Data Sweeper can be run on any Gentran Integration Suite version. This allows for new versions of Data Sweeper (which can have new updates) to be used on an older Gentran Integration Suite system. It will not require a system upgrade then.

The Data Sweeper service resolves the following issues:

- Database growth problems
  - Documents not getting purged from the application
  - Workflows getting stuck at long term life spans
- Database performance issues
  - Removal of unnecessary correlation set records
  - Performance statistics table
- Data integrity and stability
  - Invalid workflow context data
  - Documents not synchronous with the workflow or correlation rows not in synchronization
- Ability to restart or correct system within accepted guidelines without impacting the performance of the application

Installation and usage

Install Data Sweeper using the Gentran Integration Suite InstallService. Data Sweeper is an optional component. During installation, you are asked whether you want to install the component.

The Data Sweeper service can be executed directly from the command line. Navigate to the `<SWEEPER_INSTALL_BIN>` directory and run the `dataSweeper` (`dataSweeper.sh` for UNIX and `dataSweeper.cmd` for Windows operating systems) command.

A scheduled Gentran Integration Suite service can be created to run the Data Sweeper (for example, every Monday morning at 2 a.m.) by setting specific options.

You have to backup your database before using this utility. By default, the Data Sweeper will look for possible problems. The autoCorrect option must be selected to make any changes.

The following table describes the generic options available from the command line for the Data Sweeper service.

Note: These options override the default options defined in the `dataSweeper.properties` file.

Command Line option	Description	Default values	Notes
reportOnly	Display and do not make any modifications to the database	On	reportOnly and autoCorrect are mutually exclusive. Only one may be set to "on".

Command Line option	Description	Default values	Notes
autoCorrect	Opposite of reportOnly. Requried to modify the database	Off (commented out)	reportOnly and autoCorrect are mutually exclusive. Only one may be set to “on”.
detailedReport	Display information relative to troubleshooting the specific sweeper	Off	
healthChecksOnly	Run health check reports only	Off (not specified)	Include this option in the command line if you wish to run health checks only.
sweepersOnly	Run sweepers only	Off (not specified)	Include this option in the command line if you wish to run sweepers only.
defaultWorkflowID=[*value*]	Default workflow ID used for some sweepers	999	
defaultArchiveFlag=[*value*]	Default archive flag used for some sweepers	0	
cacheLimit=[*value*]	Number of rows to cache for sweeper lookups	500,000	
batchSize=[*value*]	Number of rows processed per sweeper (MYSQL only)	25,000	
commitSize=[*value*]	Number of rows before commit point	5,000	
maxReportLines=[*value*]	Number of lines displayed per health check report	50	
maxIterations=[*value*]	Number of sweeps executed before exit	10	
sweeperTimeout=[*value*]	Time (in milliseconds) allowed for sweeper execution	720,000	
sweeperTimeoutThreshold =[*value*]	Number of rows to process after timeout	100,000	

Specific Data Sweepers and Health Checks

The Data Sweeper consists of Data Sweeper and Health Check components. The tables provided below give the details.

Data Sweepers

Command Line option	Description	Mode
correlationSetSweeper	Clean up the CORRELATION_SET table (Removes 0 and -1 CORRELATION_SET rows)	ALL
unassociatedRowSweeper	Clean up tables without references (Removes child relationship when parent has been removed.)	OFFLINE
syncronizeWorkflowIds	Synchronizes document WFID to reference table ◆ Updates data in tables based on join from the SELECT statement. Each table has different links. ◆ Updates parent IDs based on child IDs if they are not equal.	ALL
reindexTenYearBusinessProcesses	Reflags business processes with long term (8 years) life spans but no document lifespan rows within that limit. This will remove rows from the WF_INST_S table (if they exist).	FORCED
reindexMailboxDocumentClonesSweeper	Verifies specific information about documents and flags them back to zero life spans.	ALL
resetRemovedMailboxDocuments	Looks for document lifespans that are tied to a document with a user_key of MBX but no MBX_MESSAGE row. If such a business process is found, then the lifespan for that business process is reset back to zero.	ALL
perfEngStatsSweeper	Deletes rows effectively so as to not cause long transactions	ALL
missingArchiveInfoSweeper	Creates ARCHIVE_INFO rows for records not found in parent tables.	OFFLINE
missingDocumentLifespansSweeper	Generates DOCUMENT_LIFESPAN rows for documents with WORKFLOW_ID < 1 with missing lifespans.	ALL
ediintdocSweeper	Sets the WORKFLOW_ID correctly. Synchronizes `EDIINTDOC/MSGMDNCORRELATION/MSGMDNUP`.	ALL
workflowContextSweeper	Removes any WORKFLOW_IDs in WORKFLOW_CONTEXT with ID < 1	ALL
dataTableScanSweeper	Removes rows from DATA_TABLE that might be considered orphaned	FORCED
documentRemovalSweeper (disabled out of box)	Removes remove orphan data in document tables associated with business process.	FORCED

Health Checks

Health checks may be run on demand for reporting only. They do not do any clean up. These reports provide system information even on a non-running instance of Gentran Integration Suite; so they may be helpful for troubleshooting.

Command Line option	Description
bpUsageHealthCheck	Provides high level usage about business processes currently on system

Command Line option	Description
currentDBUsersHealthCheck	Displays information about current connections to Gentran Integration Suite Database
objectSizeHealthCheck	Displays size, rows and analyzes database information
dbConfigHealthCheck	Displays Gentran Integration Suite specific database configuration information

Build 4318 or Higher

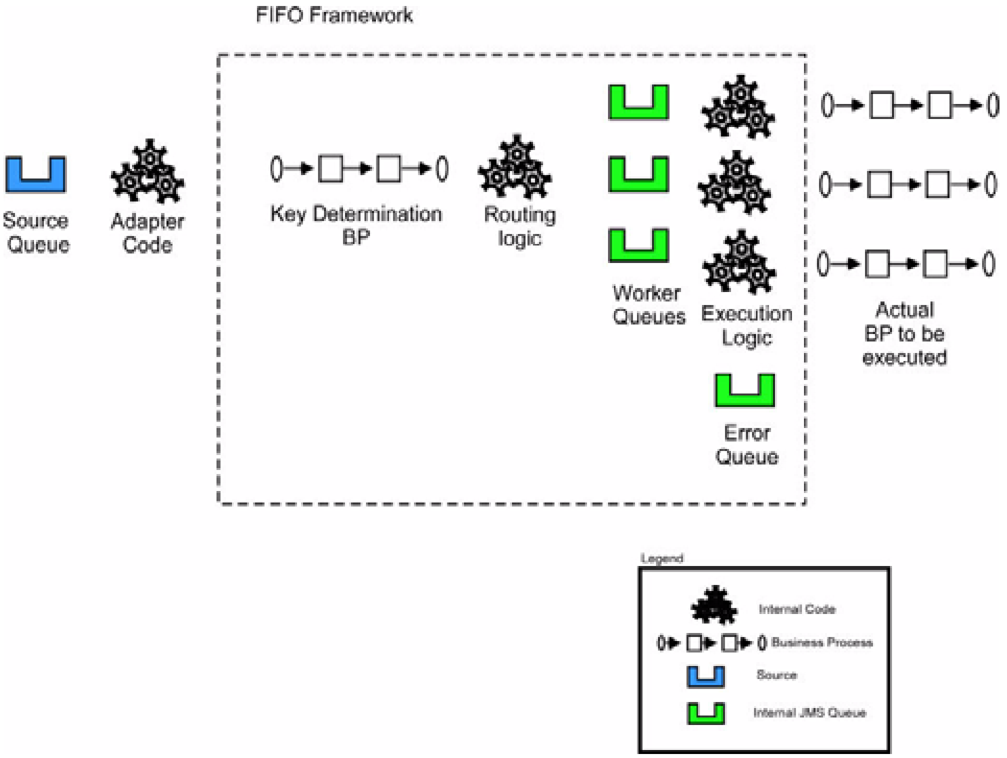
FIFO Message Processing Enhancement

Gentran Integration Suite supports ordered processing of files and messages for the following adapters:

- MSMQ adapter

The ordered processing in Gentran Integration Suite is processed by the FIFO (first in first out) framework.

The following figure demonstrates the FIFO framework:



Gentran Integration Suite supports FIFO processing of messages through adapters. The messages passed to the FIFO framework are first executed through a specialized routing key initialization business process that returns a single string value known as the routing key. The routing logic is then applied, which places all the messages with equal keys on the same internal routing queue. Messages with different routing key values process in parallel. Messages with the same routing key value maintain FIFO ordering. Each queue to user specified business process processes the message and waits for the business process to end the metadata describing the errant process, then processes the next message. If an error is encountered while processing the messages, metadata describing the errant process are routed to an error queue. Thereafter, the message processing continues.

Configuring FIFO Services

To configure FIFO services:

1. Login to Gentran Integration Suite.
2. Select **Deployment** > **Services** > **Configuration**.
3. Create new service and click **Go**.
4. In the Service Type field, enter the applicable adapter you want to use and click **Next**. You can also select it from the Tree View or List View.
5. Enter a suitable name and description in **Name** and **Description** fields.
6. Select or create a new group if required. By default, it is None.
7. Select the business process you want to execute.

Note: This business process must be set to use at least Minimal Event Processing and cannot be set to Error Only persistence level.

8. Select **FIFO** from Processing Mode drop-down list and click **Next**.
9. Select the business process that will receive the message and returns the routing key from the **FIFO Route Lookup BP** drop-down list.

   Note: You should create a business process and import it into Gentran Integration Suite.
10. Review and click **Finish**. The service is saved and the system displays *The system update completed successfully* message.

The example below demonstrates routing key business process, which executes a set of XML documents in FIFO order by OrderID field:

```
<process name=”AssignQueueKey">
  <sequence>
    <assign to=”FifoRoutingKey”    from=”DocToDOM(PrimaryDocument)/Order/@OrderId” />
  </sequence>
</process>
```

The routing information is not limited to XML documents only. Translation, Document Extraction, and other data extraction services can also be employed to retrieve routing data. In addition to the routing information in the document, the routing key business process has access to all information passed from the adapter in process data. If the routing key process fails, the error information will be placed in the *Business Process Error Queue* on page 49 as described below.

The routing key process must be configured with the *Enable Async Start Mode* disabled via the routing business process manager. If this is not configured, the routing key process will fail and the error information will be placed in the error queue.

Note: The FIFO Routing adapter must be enabled for message processing to occur. If this adapter is not enabled, messages will remain on the internal FIFO routing queues and no processing will occur.

Configuring FIFO Execution

You can customize the name and number of queues used in the FIFO framework. The number of task queues determines the number of concurrent processes that can execute in the system at a time. You can increase the number of queues, but it will consume more resources. The queue is defined in the *fifo.properties* property file in the properties directory. All settings in the *fifo.properties* configuration file can be overridden via *customer_overrides.properties*. Please see the *fifo.properties* file for additional information pertaining to customer overrides. The default queue configuration is as follows:

```
workflow.taskqueue.2=FIFO.GIS.QUEUE.2
workflow.taskqueue.3=FIFO.GIS.QUEUE.3
workflow.taskqueue.4=FIFO.GIS.QUEUE.4
workflow.taskqueue.5=FIFO.GIS.QUEUE.5
workflow.taskqueue.6=FIFO.GIS.QUEUE.6
workflow.taskqueue.7=FIFO.GIS.QUEUE.7
workflow.taskqueue.8=FIFO.GIS.QUEUE.8
workflow.taskqueue.9=FIFO.GIS.QUEUE.9
workflow.taskqueue.10=FIFO.GIS.QUEUE.10

fifo.workflow.errorqueue=FIFO.GIS.ERROR
```

Business Process Queues

The FIFO business process execution queues are defined by rows that are prefixed with workflow.taskqueue. A queue row consists of a unique ID with prefix workflow.taskqueue to the left and a unique name without spaces or punctuation to the right.

You can add a queue by adding an additional row to the existing property file or to *customer_overrides.properties*. The simplest way to add additional queues is to continue the existing numbering scheme. You can remove a queue by deleting a row.

Note: Queues cannot be reduced below their default set of ten queues using *customer_overrides.properties*. If this is required, the queues must be removed directly from *fifo.properties*.

FIFO processing must be complete and the queues must be empty to change the queue configuration. You must disable the inbound adapter while changing the queue configuration. If the inbound adapter is not disabled and the queues are not drained, it may result in message execution that is out or order.

Business Process Error Queue

The business process error queue is defined within the *fifo.properties* file. The error queue configuration defines the destination of errors within the FIFO framework. The error queue name should not contain spaces or punctuation. The default business process error queue is shown below:

```
fifo.workflow.errorqueue=FIFO.GIS.ERROR
```

Recovering Errant Data

The messages in the error queue are written in XML format. The XML format provides information to determine the nature and source of the document containing the error. The error message contains information that enables the retrieval of document data; however, contents of the document are not stored in the message. The error message format is as below:

```
<?xml version="1.0" encoding="UTF-8"?>
<FifoError ErrorMessage="" ErrorType="" TaskId="" TaskQueueId="" TaskQueueKey=""
Type="">
  <WorkFlowError PrimaryDocumentId="" WorkFlowContextId="" WorkFlowId=""
WorkFlowInitiator="">
    <FifoErrorNode/>
   <FifoInitializationBpReport AdvancedStatus="" BasicStatus="" PrimaryDocumentId=""
ServiceName="" WfdName="" WfdVersion=""
      WorkFlowContextId="" WorkFlowId="">
        <StatusReport></StatusReport>
        <ProcessData>
          <PrimaryDocument SCIObjectID=""/>
        </ProcessData>
    </FifoInitializationBpReport>
  </WorkFlowError>
</FifoError>
```

FIFO Error Elements

FifoError Element

The *FifoError Type* indicates the type of FIFO task that is being executed. At present, Async WorkFlow is the only type supported.

The table below lists the other FifoError elements:

Type	Description
TaskId	A unique ID given to each FIFO task executed by the FIFO framework.
TaskQueueId	The queue where the FIFO task was executed.
TaskQueueKey	The key that was returned through the FIFO routing key business process execution.
ErrorMessage	This element contains the information that assists in determining the cause of the failure.

WorkFlow Error Element

The table below lists the WorkFlow Error elements:

Type	Description
WorkFlowId	This element contains the workflow id that was executed.

Type	Description
WorkFlowContextId	This element contains the workflow context id for the first step of the business process. This information is used to retrieve the workflow and extract additional data in advanced scenarios.
WorkFlowInitiator	This element contains the name of the workflow initiator. In most cases, name of the adapter that started the process will be the workflow initiator name.
PrimaryDocumentId	This element contains the ID for the primary document of the business process.

FifoInitializationBPReport

This element contains metadata that describes the execution of the routing key initialization business process.

This is an optional node. It will be included both in process data of the executed business process and in the error queue XML. It is automatically included in the XML data if an error occurs during task initialization. To force the inclusion of this data, both in the error report and process data of the executed business process, ForceFifoInitializationDump to "true" in the routing key business process

The table below lists the initialization BP report elements:

Type	Description
AdvancedStatus	This element contains the advanced status for the final step of this business process.
BasicStatus	This element contains the basic status for the final step of this business process.
PrimaryDocumentId	This element contains the primary document id at the last step of this business process.
ServiceName	This element contains the service name for the last step of this business process.
wfdName	This element contains the workflow definition name for this business process.
wfdVersion	This element contains the workflow definition version for this business process.
WorkFlowContextId	This element contains the workflow context id for this business process.
WorkFlowID	This element contains the workflow id for this business process.
StatusReport	This element contains the status report, if any, at the last step of this business process.

Type	Description
ProcessData	This element contains the process data at the last step of the business process.

FifoErrorNode Element

When the routing key business process is executed, the business process author can optionally write additional metadata to the FifoErrorNode element in the process data. This element and all the child nodes will be included in the FifoError document as part of this element.

The routing key business process has access to all process data information passed onto it through the adapter. See the example below for additional information about generating an error node.

```
<process name=”AssignQueueKey">
  <sequence>
    <assign to=”FifoRoutingKey”    from=”DocToDOM(PrimaryDocument)/Order/@OrderId” />

   <assign to=”FifoErrorNode/MSMQ/@QueueName” from=”string(MSMQ/@QueueName)”
append=”true”/>
  </sequence>
</process>
```

The additional information from the adapter can be included in the element to preserve the context of the error information in an easily identifiable manner.

FIFO Error Queue Listener

An out of the box adapter is configured on each node to listen to the error queue. This adapter is named "FIFO Error Queue Listener {nodename}". The adapter will bootstrap a business process named FifoError. This process is configured to retrieve the data from the errant process, including the original document and to integrate it into this process. This allows you to automate the re-processing of the data and other activities.

The FifoError process is defined as follows:

```
<process name="FifoError">
  <sequence>
    <operation>
      <participant name="FIFORouting" />
        <output message="Xout">
          <assign to="." from="*"></assign>
          <assign to="FifoTask">FifoErrorRecord</assign>
        </output>
        <input message="Xin">
          <assign to="." from="*"></assign>
        </input>
    </operation>
  </sequence>
</process>
```

The FifoError process provides a basic implementation for error handing. A user-specified business process may be configured to allow for customized error handling. A user-specified business process must contain the FIFORouting service as configured in the default FifoError process. Details surrounding FIFORouting service are described below.

FIFORouting Service

The FIFORouting service provides a control and reporting mechanism for interaction between business processes and the FIFO subsystem.

The FifoTask parameter specifies the task that this service should execute. Currently, there are two operational tasks this service provides: FifoResponse and FifoErrorRecord.

The FifoErrorRecord parameter specifies that the FIFORouting service should parse an error record from the error queue, retrieve the errant business process data, and report on it, as described above. This parameter should be used in conjunction with a retrieval of an error record from the error queue. The primary document in this mode of operation must be an FifoError XML record.

When executed in the FifoErrorRecord mode, the FIFORouting service will retrieve data pertaining to the errant business process and include it in ProcessData for the current business process. All data, including documents, may then be used directly within the current business process. The service will generate data of the following format:

```
<ProcessData>
  ...

 <PrimaryDocument SCIObjectID=""/>

...

 <FifoProcess ErrorType="" WorkFlowContextId="" WorkFlowId=""
      WorkFlowInitiator="">
    <ProcessData>
      <FifoDetails>
        <FifoInitializationBpReport AdvancedStatus="" BasicStatus=""
            PrimaryDocumentId="" ServiceName="" WfdName="" WfdVersion=""
            WorkFlowContextId="" WorkFlowId="">
          <StatusReport>
          </StatusReport>
          <ProcessData>
            <PrimaryDocument SCIObjectID="" />
          </ProcessData>
        </FifoInitializationBpReport>
      </FifoDetails>
    </ProcessData>
  </FifoProcess>

</ProcessData>
```

Note: The first instance of ProcessData is that of the current error handler business process. The FifoProcess element contains the data from the errant business process. The ProcessData element within this element contains the data from the original errant business process. All data and documents within this ProcessData element may be used directly within this business process for error handing purposes.

The FifoReponse parameter specifies that the FIFORouting service should return a positive or negative success response to the FIFO subsystem. An optional parameter, FifoStatus, may also be specified. This status indicates whether or not the business process was a success and if it is an error, designations the FIFO subsystem to report an error. The FifoStatus parameter considers ERROR to be a failure and any other string data to be success.

The FifoResponse parameter is used to provide early response at to the success or failure of a FIFO business process. For example, assume business process A is the process that must be executed in FIFO. Business process A contains 10 steps. The first 5 steps must be executed in order; however, the last 5 steps provide data execution functionality where order is not important. In this example, optimal performance will be achieved by utilizing the FIFORouting service in FifoResponse mode to return the response at step 6. This will allow the next message to be processed immediately following the execution of this service and allow steps 7 through 11 to execute fully parallel.

Cluster Configuration

The FIFO messaging system requires an external clustered JMS provider to allow proper execution and failover in a clustered configuration. An out of the box configuration for ActiveMQ 5.2 is provided to streamline this deployment.

Configuring FIFO messaging in a cluster for ActiveMQ:

1. Download ActiveMQ 5.2 from http://activemq.apache.org/activemq-520-release.html for the appropriate OS.
2. Deploy an instance of ActiveMQ 5.2 on each node of the cluster.
3. An activemq.xml file is included the properties/fifo directory of the Gentran Integration Suite deployment of each node. For each node, take this file and copy it to the ActiveMQ deployment on that node within the "conf" directory. This file will configure ActiveMQ to use failover clustering utilizing the Gentran Integration Suite database for storage and configure its port usage. By default, ActiveMQ will be configured to listen at the Gentran Integration Suite base port + 65 and the ActiveMQ interface will be at base port + 66 (http://server:base port + 66/admin).
4. On each Gentran Integration Suite node, the queue configuration must be re-directed to utilize the ActiveMQ cluster. In each node, add the following to *customer_overrides.properties*:

   ```
   fifo.broker.username=

   fifo.broker.password=

   fifo.broker.url=failover:(tcp://node1_hostname:node1_base_port +
   65,tcp://node2_hostname:node_2_base_port + 65, ...,
   tcp://noden_hostname:node_n_base_port + 65 )
   ```
5. Start the ActiveMQ instances on each node. See http://activemq.org for additional information about running an ActiveMQ instance.
6. Restart Gentran Integration Suite.

Build 4315 or Higher

Custom Password Policy Extension

The passwordPolicyExtensionImpl property was added to the system to allow for the extension of the default acceptable password checks. These password checks prevent the use of weak, easily hacked passwords and reject non-compliant passwords. The extension allows for the use of additional customer specific password validation checks.

The extension is accomplished by implementing custom Java code via a plug-point. Once enabled, the plug-point is used for all users in the system associated with a password policy (this is a global setting).

The custom password policy extension is applied prior to the default system policy. Therefore, if a password violates more than one policy requirement (one enforced by the extension class and another enforced by the default implementation) only the error message returned from the extension class is displayed to the user.

The passwordPolicyExtensionImpl property value is set once in the customer_overrides.properties file. For the password policy extension to be applied, the user has to be associated with a password policy. For user accounts not associated with a password policy, the extension is not applied.

Code Example - IPasswordPolicyExtension Java Class Interface

The interface com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension was added to the system as follows:

```
public interface IPasswordPolicyExtension {
    /**
     * Implements extended validation on passwords and returns null if password
     * validation is successful. If validation fails, an error message key
     * that may be looked up in Login_*.properties* should be returned.
     * @param password - The password string to validate
    * @param policyId - The PWD_POLICY.POLICY_NAME of the policy associated with the
user in case the extension needs it.
     * @return String Return null if password validation was successful, the error
message key if password validation fails
     */
    public String validateNewPassword (String password, String policyName);
}
```

Returning null from the method indicates that the password was accepted. Returning anything else means the password was not valid.

Example Implementation

```
package test.policy.extension;
import java.util.regex.Pattern;
public class PwdPolExtnImpl implements
com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension {
            public String validateNewPassword(String pwd,
                  String policyName) {
            // Additional password validation checks
                  boolean match=Pattern.matches(".*[a-z].*", pwd) &&
Pattern.matches(".*[A-Z].*", pwd) && (Pattern.matches(".*[0-9].*", pwd) ||
Pattern.matches(".*[^A-Za-z0-9].*",pwd));
                  if (match==true) return null;
                  else return "nogood";
      }

}
```

Implement a Password Policy Extension

The implementation of password policy extension includes the following tasks:

- Specify the Java class implementing the password policy extension using the passwordPolicyExtensionImpl property in the customer_overrides.properties file.
- Add the implementation class jar to the classpath in the install3rdParty.sh file under the /install_dir/bin directory.
- Define error message entries in the appropriate Login_<language>.properties_<domain>_ext files available in the /*install_dir*/bin/properties/lang/ directory to localize the error messages.

Specify passwordPolicyExtensionImpl Property Value

To plug in the custom implementation, the Java class name needs to be specified in the passwordPolicyExtensionImpl property in the customer_overrides.properties file.

Note: The customer_overrides.properties file is not part of the default system code. It must be created after the initial system installation and populated to match your environment.

To specify the Java class implementing the password policy extension:

1. Navigate to the /*install_dir*/properties directory.
2. Edit the customer_overrides.properties file.
3. Add the passwordPolicyExtensionImpl property at the end of the file and enter the name of the Java class implementing the extended validation of passwords.
   The final entry should look something like this:
   `security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl`
4. Save and exit the file.

Add the Implementation class JAR to the Classpath

The extension implementation class must be compiled and jarred as follows:

1. Navigate to the directory where the password extension class files are located.
2. Enter:
   ```
   javac -cp /install_dir/jar/woodstock.jar test/policy/extension/*.java
   ```
3. Enter:
   ```
   jar cf <new_filename>.jar <path_to_class_file>/<Custom_Impl>.class
   ```
   where `<new_filename>`.jar is the name of the new Jar file to be created and
   where `<Custom_Impl>.class` is the name of the custom implementation Java class file.
   For example:
   ```
   jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class
   ```
4. Navigate to the /*install_dir*/bin directory.
5. Enter:
   ```
   Install3rdParty.sh userExit 1_0 -j <path_to_user_exit_jar>
   ```

Define Error Strings for Custom Password Policy Extension

The error strings returned from the custom implementation are localized by defining entries in the appropriate Login_<language_dir>.properties_<uniqueID>_ext files. The error strings inform the end-user of password rules and list reasons for rejected password changes.

If customer-specific text is not provided, the error message is returned to the user as is.

Note: Note: The Login_<language_dir>.properties_<uniqueID>_ext file is not part of the default system code. It must be created after the initial system installation and populated to match your environment.

To define error strings for a custom password policy extension:

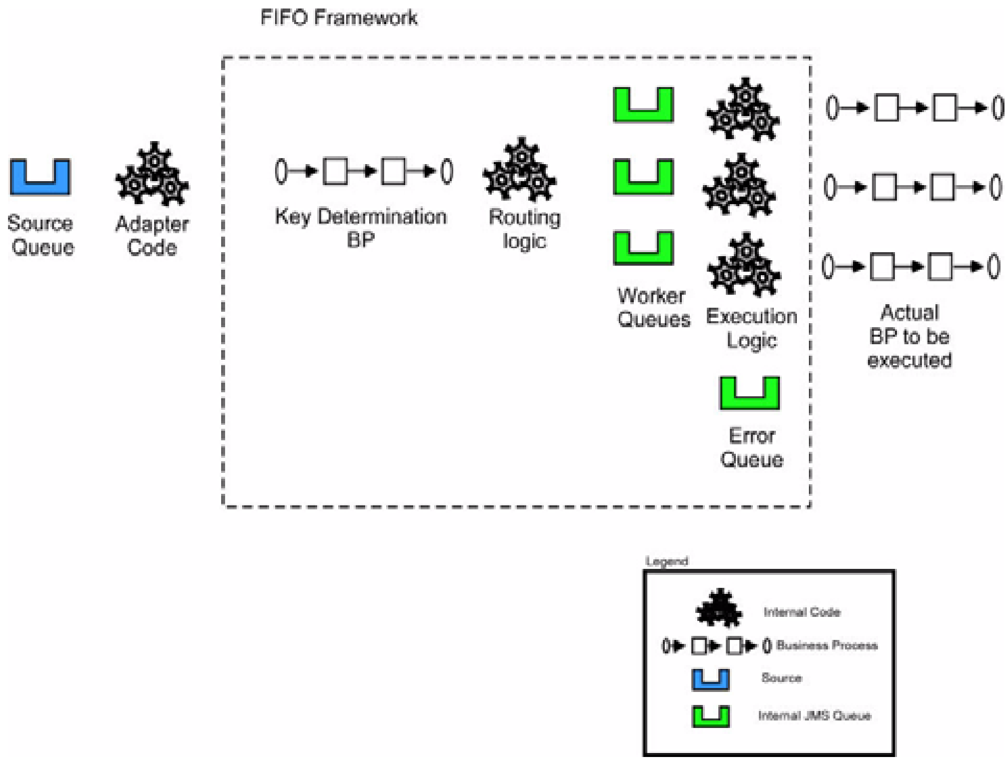
1. Navigate to the /install_dir/properties/lang/<language_dir> directory.
   where <language_dir> is the language set for the customer's locale (for example, en, ja, fr).
2. Edit the Login_<*language_dir*>.properties_<*uniqueID*>_ext file,
   where <*language_dir*> is the language set for the customer's locale and
   where <*filename*> is the unique identifier for the new custom password extension.
   For example:
   ```
   Login_en.properties_custompasswd_ext
   ```
3. Add an entry to the file for the error condition set in the custom extension file and define the descriptive string to return to the user.
   For example:
   ```
   nogood = The password must contain a minimum of one lower case character, one upper
   case character, and one digit or special character.
   ```
4. Save and exit the file.

Build 4314 or Higher

FIFO Message Processing Enhancement for MSMQ Adapter

Gentran Integration Suite supports ordered processing of files and messages. The ordered processing in Gentran Integration Suite is processed by FIFO (first in first out) framework.

The following figure demonstrates the FIFO framework:



Gentran Integration Suite supports FIFO processing of messages through MSMQ adapter. The messages passed to the FIFO framework are executed through a business process that returns a single string value known as the sequencing key. The routing logic is then applied, which places all the messages with similar keys on the same internal routing queue. Each queue has a process that executes a user specified business process, processes the message, and waits for the business process to end and processes the next message.

If an error is encountered while processing the messages, debug information along with the message can be routed to an error queue that can be configured. Thereafter, the message processing continues.

Configuring FIFO Services

To configure FIFO services:

1. Login to Gentran Integration Suite.
2. Select **Deployment** > **Services** > **Configuration**.
3. Create new service and click **Go**.
4. In the Service Type field, enter MSMQ Adapter and click **Next**. You can also select it from the Tree View or List View.
5. Enter a suitable name and description in **Name** and **Description** fields.
6. Select or create a new group if required. By default, it is None.
7. Enter the remote host name and port number in Remote Host Name and Port Number fields.
8. Enter the queue path name in the Queue Path name field if required.
9. Select the document storage type from Document Storage Type drop-down list. By default, it is System Default.
10. Select **FIFO** from Processing Mode drop-down list and click **Next**.
11. Select the business process that will receive the message and returns the routing key from the **FIFO Route Lookup BP** drop-down list.

    Note: You should create a business process and import it into Gentran Integration Suite.
12. Review and click **Finish**. The service is saved and the system displays *The system update completed successfully.* message.

The example below demonstrates routing key business process, which executes a set of XML documents in FIFO order by OrderID field:

```
<process name=”AssignQueueKey">
  <sequence>
    <assign to=”FIFO_ROUTING_KEY”    from=”DocToDOM(PrimaryDocument)/Order/@OrderId”
/>
  </sequence>
</process>
```

The routing information is not limited to XML documents only. Translation, Document Extraction, and other data extraction services can also be employed to retrieve routing data. In addition to the routing information in the document, the routing key business process has access to all information passed from the adapter in process data. If the routing key process fails, the error information will be placed in the *Error Queue* on page 60 as described belowFIFO Error ElementsError QueueError Queue.

The routing key process must be configured with the *Enable Async Start Mode* disabled via the routing business process manager. If this is not configured, the routing key process will fail and the error information will be placed in the error queue.

Configuring FIFO Queue

You can customize the name and number of queues used in the FIFO framework. The number of task queues determines the number of concurrent processes that can execute in the system at a time. You can increase the number of queues, but it will consume more resources. The queue can be defined in the *fifo.properties* property file in the properties directory. The default queue configuration is as follows:

```
fifo.taskqueue.1=GIS_fifo_queue_1
fifo.taskqueue.2=GIS_fifo_queue_2
fifo.taskqueue.3=GIS_fifo_queue_3
fifo.taskqueue.4=GIS_fifo_queue_4
fifo.taskqueue.5=GIS_fifo_queue_5
fifo.taskqueue.6=GIS_fifo_queue_6
fifo.taskqueue.7=GIS_fifo_queue_7
fifo.taskqueue.8=GIS_fifo_queue_8
fifo.taskqueue.9=GIS_fifo_queue_9
fifo.taskqueue.10=GIS_fifo_queue_10

fifo.errorqueue=GIS_fifo_error_queue
```

Execution Queue

The queues are defined by rows that are prefixed with fifo.taskqueue. A queue row consists of a unique ID with prefix fifo.taskqueue to the left and a unique name without spaces or punctuation to the right.

You can add a queue by adding an additional row to the existing property file. The simplest way to add additional queues is to continue the existing numbering scheme. You can remove a queue by deleting a row.

The FIFO processing must be complete and the queue must be empty to change the queue configuration. You must disable the inbound adapter while changing the queue configuration. If the inbound adapter is not disabled, it may result in message execution that is out or order.

Error Queue

You can define error queue in the *fifo.properties* file. The error queue configuration defines the destination of errors within the FIFO framework. The error queue configuration should not contain spaces or punctuation. An error queue is defined as shown below:

```
fifo.errorqueue=GIS_fifo_error_queue
```

Recovering Documents

The messages in the error queue are written in XML format. The XML format provides information to determine the nature and source of the document containing the error. The error message contains information that enables you to retrieve the document data. However, contents of the document are not stored in the message. The error message format is as below:

```
<FifoError Type=”AsyncWorkFlow”  TaskId=”” TaskQueueId=”” TaskQueueKey=””
ErrorMessage=””>
    <WorkFlowError WorkFlowId=”” WorkFlowContextId=””
            WorkFlowInitiator=”” PrimaryDocumentId=””>
        <FifoErrorNode/>
    </WorkFlowError>
</FifoError>
```

FIFO Error Elements

FifoError Element

The *FifoError Type* indicates the type of FIFO task that is being executed. At present, Async WorkFlow is the only type supported.

The table below lists the other FifoError elements:

Type	Description
TaskId	A unique ID given to each FIFO task executed by the FIFO framework.
TaskQueueId	The queue in which the FIFO task was executed.
TaskQueueKey	The key that was returned through the FIFO routing key business process execution.
ErrorMessage	This element contains the information that assists in determining the cause of the failure.

WorkFlow Error Element

The table below lists the WorkFlow Error elements:

Type	Description
WorkFlow Id	This element contains the workflow id that was executed.
WorkFLowContextId	This element contains the workflow context id for the first step of the business process. This information is used to retrieve the workflow and extract additional data in advanced scenarios.
WorkFlowInitiator	This element contains the name of the workflow initiator. In most cases, name of the adapter that started the process will be the workflow initiator name.
PrimaryDocumentId	This element contains the ID for the primary document of the business process. This document ID is used along with GetDocumentInfo service to retrieve the document from the database. **Note:** The document remains in the system for the lifespan of the Schedule_AssociateDocToBP process. In the case of failure, it may not be associated with a business process.

FifoErrorNode Element

When the routing key business process is executed, the business process author can optionally write additional metadata to the FifoErrorNode element in the process data. This element and all the child nodes will be included in the FifoError document as part of this element.

The routing key business process has access to all process data information passed onto it through the adapter. An example to generate an error node with additional information is as shown below:

```
<process name=”AssignQueueKey">
  <sequence>
    <assign to=”FIFO_ROUTING_KEY”    from=”DocToDOM(PrimaryDocument)/Order/@OrderId”
/>

   <assign to=”FifoErrorNode/MSMQ/@QueueName” from=”string(MSMQ/@QueueName)”
append=”true”/>
  </sequence>
</process>
```

This additional information from the adapter can be included in the element to preserve the context of the error information in an easily identifiable manner.

Web Services Enhancements

Gentran Integration Suite 4.3, Build 4314 provides support for these Web services enhancements:

- Limiting the process data elements that are sent as a part of the SOAP response
- Validating a SOAP message against input schema and output schema
- Including an output schema for a business process in the WSDL

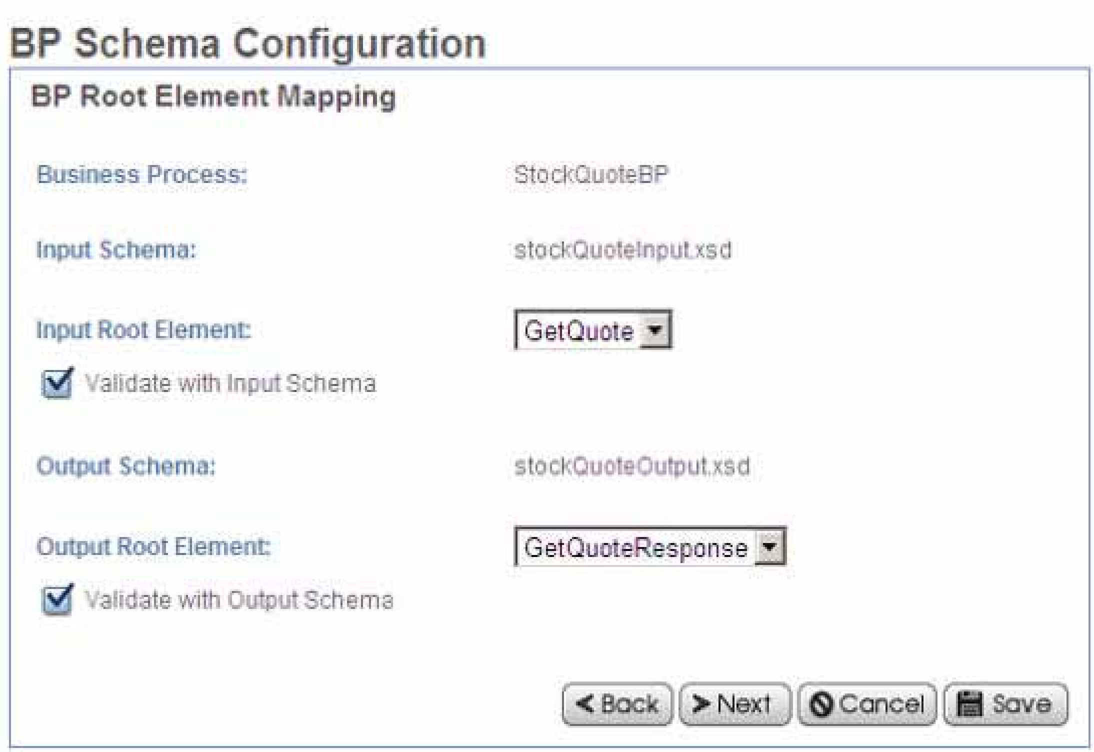
For basic Web Services procedures, see the documentation (including updates) in the Gentran Integration Suite 4.3 Documentation Library.

Limiting the Process Data Elements Sent in the SOAP Response

The application provides a default output schema for use if no other schema is provided. However, the default output schema contains one parameter, process data, and passes the whole of process data in the response. Use of an output schema for each business process in a Web service restricts what process data is passed to the consumer in the SOAP response.

Validating a SOAP Message Against an Input and/or Output Schema

When mapping a business process to a non-default XML input schema and/or an output schema, you have the additional option of validating the SOAP message against the schema(s):



BP Schema Configuration

BP Root Element Mapping

Business Process: StockQuoteBP

Input Schema: stockQuoteInput.xsd

Input Root Element: GetQuote

☑ Validate with Input Schema

Output Schema: stockQuoteOutput.xsd

Output Root Element: GetQuoteResponse

☑ Validate with Output Schema

These are the new fields on the BP Schema Configuration screen:

Field	Description
Validate with Input Schema	Validate the SOAP body content against the input schema. Send as SOAP body content if validation is successful, or send a fault if errors are encountered. Displays if Input Schema is specified.
Validate with Output Schema	Validate the content of the response against the output schema. Send as SOAP body content if validation is successful, or send a fault if errors are encountered. Displays if Input Schema is specified.

Note: There may be times when sending a blank SOAP body is desired. To send a blank SOAP body and have it validate successfully, do the following:

- Do not select Validate with Output Schema.
- Do not create the WebserviceResponseNode element in process data (or create it and leave the node empty).

Including an Output Schema in the WSDL

If an output schema is checked in and the user selects the use of the output schema, the elements of the schema are inserted into the “types” section of the WSDL. This is an example of the types section of a WSDL with those schema elements inserted:

```
…
<wsdl:definitions ...
<wsdl:types>...
<xs:schema ...
…
<xs:complexType name="CustomElement">
   <xs:sequence>
        <xs:element name="ele1" type="xsd:string"/>
        <xs:element name="ele2" type="xsd:string"/>
        <xs:element name="ele3" type="xsd:string"/>
   </xs:sequence>
</xs:complexType>
<xs:element name="outputData" type="tns: CustomElement" />
…
```

The type is then inserted into the definition of the output message of the corresponding operation. This is done in a new message that corresponds to the business process. The syntax for the unique name of the message element consists of the name of the business process concatenated with the word “Response”:

`*business_process_name*Response`

For example:

```
…
<wsdl:message name="BP1Response">
   <wsdl:part element="mesa: CustomElement" name="outputData" />
</wsdl:message>
…
<wsdl:portType name="GISPortType">
   <wsdl:operation name="executeBP1">
         <wsdl:input message="mesa:BP1" />
         <wsdl:output message="mesa: BP1Response" />
   </wsdl:operation>

</wsdl:portType>
```

XML Schemas in Web Services

An *XML schema* describes the structure of an XML document. A valid XML document must be well formed and must be validated. A schema defines data types. Data types can be anything from simple to complex.

An XML schema defines:

- What elements can appear in the document
- What attributes can appear in the document

- What elements are child elements, sequence in which they appear, and the number of child elements
- Whether an element can be empty
- Default values for attributes

Input and Output Schemas

Every business process that can be run by a Web services provider can be associated with an input and/or an output schema:

- The *input schema* is a schema object (XSD) that defines the structure of the XML element(s) present in the body of the incoming SOAP request. This element in the SOAP body is inserted “as is” into the process data of the business process to be run.

  The input schema is also used in the WSDL generated for the Web service hosting the business process, as a type definition for the input part of the operation corresponding to the business process.
- The *output schema* is a schema object (XSD) that defines the structure of the XML element(s) to be sent as the body of the outgoing SOAP response. This element is extracted from the process data of the business process that was run by the Web service provider and inserted into the SOAP body of the response. Mapping to an output schema provides a way, if desired, to restrict what process data is passed to the consumer in the SOAP response.

  The output schema is also used as a type definition in the WSDL generated for the Web service hosting the business process, in the output part of the operation corresponding to the business process.

The application provides a default input and output schema. These are included for use by the application if no other schema is provided. They do not contain any restrictions on the structure or type of data in the message.

- Default input schema – Contains two parameters: process data and primary document.
- Default output schema – Contains one parameter, process data. It passes the whole of process data in the response.

The best practice is to create input and output schemas for each business process you want to use in a Web service to ensure that data is structured correctly.

The user can also select whether to validate incoming or outgoing data, each against its respective schema.

See the Mapping XML Schemas to Business Processes topic for mapping and validation procedures.

Naming Conventions for Schemas

When creating schemas, give them descriptive names that include information such as the business function or consumer name/type. Include the direction (input or output) if the schema will be used for only one direction.

Schema Limitations for Business Processes

The following limitations apply to business process schemas:

- Each business process can have only one root element mapped to it per input or output schema.

- Valid schemas need to have one or more root elements.
- You cannot map the same root element to multiple business processes. There should always be a one-to-one mapping relationship between a business process and a root element.
- If a schema/root element combination has already been used with a business process, you cannot use the same combination again, even with a different business process.
- Target namespace must be present in the schema for the WSDL to generate properly.

Note: You must add an XML schema to the application before you can map it to an existing business process.

Schema Limitations for Web Services

XML schemas for Web services have the following constraints:

- The schemas must contain a targetNamespace.
- The schemas must contain only one root element.

The basic structure must include the following:

Node	Description
Type of data	String, other types accepted. Required. Default is String.
Document encoding type	Required. Default is UTF8. Also accepts UTF16 (this is a SOAP specification).

WSDL Example

If an output schema is checked in and the user selects the use of the output schema during Web service creation, the elements of the schema are inserted into the “types” section of the WSDL. This is an example of the types section of a WSDL with those schema elements inserted:

```
…
<wsdl:definitions ...
<wsdl:types>...
<xs:schema ...
…
<xs:complexType name="CustomElement">
   <xs:sequence>
        <xs:element name="ele1" type="xsd:string"/>
        <xs:element name="ele2" type="xsd:string"/>
        <xs:element name="ele3" type="xsd:string"/>
   </xs:sequence>
</xs:complexType>
<xs:element name="outputData" type="tns: CustomElement" />
…
```

The type is then inserted into the definition of the output message of the corresponding operation. This is done in a new message that corresponds to the business process. The syntax for the unique name of the message element consists of the name of the business process concatenated with the word “Response”:

*business_process_name*Response

For example:

```
…
<wsdl:message name="BP1Response">
   <wsdl:part element="mesa: CustomElement" name="outputData" />
</wsdl:message>
…
<wsdl:portType name="GISPortType">
   <wsdl:operation name="executeBP1">
         <wsdl:input message="mesa:BP1" />
         <wsdl:output message="mesa: BP1Response" />
   </wsdl:operation>
</wsdl:portType>
```

Creating an XML Schema for Web Services

To create a input or output XML schemas for Web services:

1. Create the input or output XML schemas for your business process using an XML text editor.

   Note: You can use only XML schemas (.xsd) with Web services; you cannot use DTD (.dtd) files.
2. Check in the XML schema to your application.
3. Map the XML schema to its business process in your application.

Mapping XML Schemas to Business Processes

To map an XML schema to a business process:

1. In your application, select **Deployment** > Web Services > **Schema Mappings**.
2. Under Create, next to **Create a New BP Schema Mapping**, click **Go!**
3. Complete the fields displayed in the wizard and click **Next** to advance.
4. Confirm that the choices displayed are correct and click **Finish** to add the BP schema mapping.
5. You have finished this procedure. Click **Return** to continue.

Creating a Blank SOAP Body

There may be times when sending a blank SOAP body is desired. To send a blank SOAP body and have it validate successfully, do the following:

- Do not select Validate with Output Schema.
- Do not create the WebserviceResponseNode element in process data (or create it and leave the node empty).

BP Schema Mapping Field Definitions

Field	Description
Business Process	If this is a new mapping, select a business process to associate input and/or output schemas with. Required. If editing an existing relationship, this field is unavailable.
Input Schema	Select an XML schema to be used as the input schema for the business process or service. By default, Web services layer does not validate the input data to a business process against the input schema. It just passes the received data to the business process or service. **Note:** An Input Schema or an Output Schema must be specified. If you select only an output schema, the system will use the generic input XML Schema with it.
Output Schema	Select an XML schema to be used as the output schema for the business process or service. By default, Web services layer does not format the response based on the output schema before sending the response to the sender. **Note:** An input schema or an output schema must be specified. If you select only an input schema, the system will use the generic output XML schema. The generic output XML schema outputs the whole of the process data for the business process as the SOAP response.

BP Root Element Mapping Field Definitions

Field	Description
Input Root Element	Select a Root Element for the input schema to define the input formats for a business process. Required if Input Schema previously specified.
Validate with Input Schema	Validate the SOAP body content against the input schema. Send as SOAP body content if validation is successful, or send a fault if errors are encountered.
Output Root Element	Select a Root Element for the output schema to define the output formats for a business process. Required if output schema previously specified.
Validate with Output Schema	Validate the content of the response against the output schema. Send as SOAP body content if validation is successful, or send a fault if errors are encountered.

Build 4309 or Higher

Using Single Sign On

Single sign on (SSO) is an authentication process enabling a person accessing several applications to type only one user name and one password to access all applications that the person has permission to. Previously, a person logged in to each application individually and may have required several user names and passwords to manage. Single sign on solves this problem.

Note: User authentication does not require the LDAP adapter, which is used with business processes and enables Gentran Integration Suite to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).

Gentran Integration Suite allows SSO through integration with Netegrity SiteMinder and allows you to customize SSO implementation through customized plug-ins.

Single sign on in Gentran Integration Suite is limited to the following components:

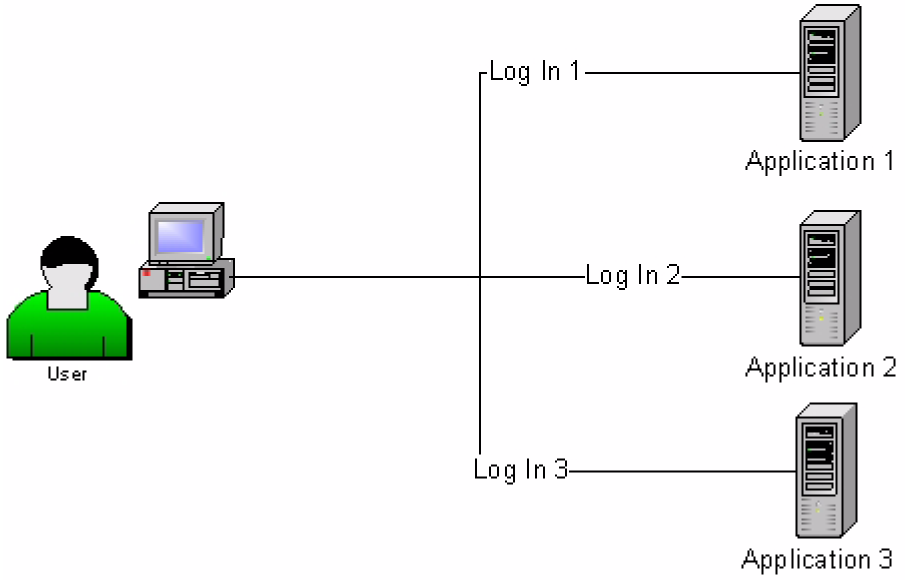
- Administration Interface
- Mailboxing Interface
- Dashboard Interface
- Advanced File Transfer (AFT) Interface
- MyAFT Interface

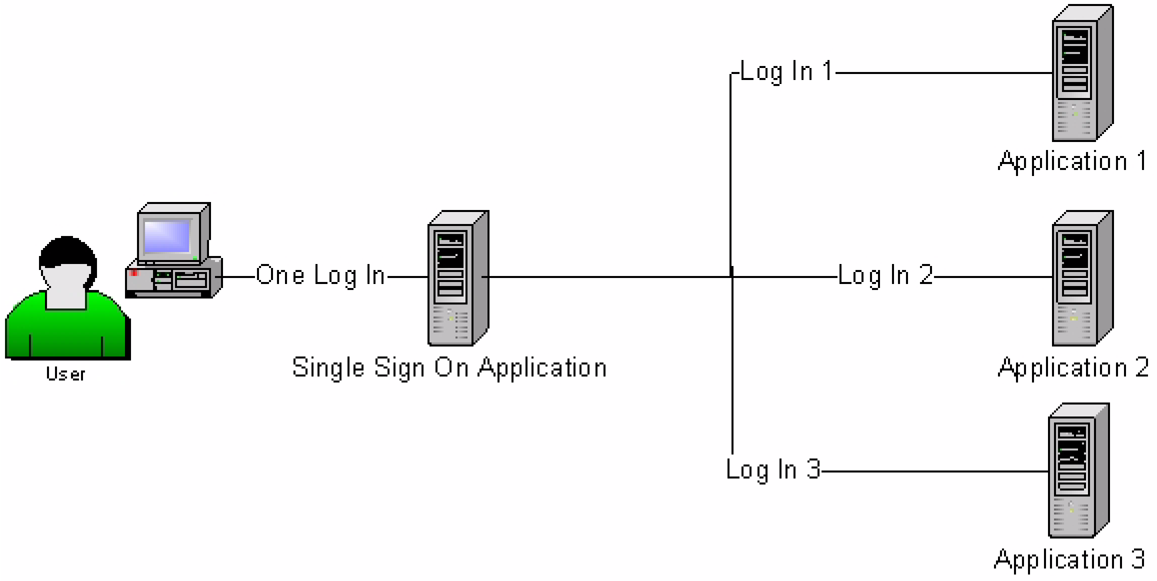
Before Using Single Sign On

Before you can use single sign on with Gentran Integration Suite, you must have:

- Knowledge of SSO.
- Knowledge of Netegrity SiteMinder or your Single Sign On application.
- Netegrity SiteMinder installed and configured with a reverse proxy server (if you are using Netegrity SiteMinder for Single Sign On).
- Edited the security.properties file in your *install_dir*/properties directory for Gentran Integration Suite to use single sign on.

The following figures show an authentication process without single sign on capability and an authentication process with single sign on capability:





Before you can use single sign on with Gentran Integration Suite, you must edit the neo-ui.properties and security.properties files in your *install_dir*/properties directory for Gentran Integration Suite to use single sign on.

To edit the neo-ui.properties file:

1. Stop Gentran Integration Suite.
2. In your *install_dir*/properties directory, locate the neo-ui.properties file and open the file in a text editor.

3. In neo-ui.properties, provide the associated SSO entry for each interface.

   The following code sample shows the associated entry to the same HTTP sites:

```
url.host=%(host)
url.port=10200
url.cm=http://%(host):10200/communitymanagement/
url.cm.sso=http://%(host):10200/communitymanagement/
url.ob=http://%(host):10233/onboard/
url.ws=http://%(host):10200/ws/
url.ws.sso=http://%(host):10200/ws/
url.dash.sso=http://%(host):10233/dashboard/
url.ds=http://%(host):10200/datastore/
url.help=http://%(host):10200/help/index.htm?context=webhelplocal&single=true&topic=
url.help.ja=http://%(host):10200/help_ja/index.htm?context=webhelplocal&single=true&
topic=
url.dash=http://%(host):10233/dashboard/
portlet.refresh.interval.seconds=60
url.aft=http://%(host):10200/aft/
url.aft.sso=http://%(host):10200/aft/
url.dmi=http://%(host):10200/dmi/
url.dmi.sso=http://%(host):10200/dmi/
```

4. Save the neo-ui.properties file using the same name in the same directory.

To edit the security.properties file:

1. In your *install_dir*/properties directory, locate the security.properties file and open the file in a text editor.
2. In security.properties, locate the ## SSO Authentication configuration entry.

   The following code sample shows the SSO Authentication configuration parameters:

```
## SSO Authentication configuration

## enable sso authentication  (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true

## enable sso authentication on each Page (true, false) default=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false

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

## List of SSOProvider Classes that are supplied to use - If SSO Authentication is
## enable, should have at least one class, the following is the default one that we
## supplied.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Will try to use this first
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Will try to use this if first
## one failed
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Will try to use this if second
## one failed too
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Will try to use this if all
## first n-1 classes failed
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS
OProviderDefault

## External Page for SSO when Logout (Specify the SSO Server external page for each of
## the cases)
## Example: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## After SSO User logout from Mailbox, instead of display the Mailbox Login Screen
## display Sterling Commerce Web page.
SSO_FORWARD_URL.AFT.LOGOUT=
SSO_FORWARD_URL.MYAFT.LOGOUT=
SSO_FORWARD_URL.MAILBOX.LOGOUT=
SSO_FORWARD_URL.WS.LOGOUT=
SSO_FORWARD_URL.DASHBOARD.LOGOUT=

## Default handling for LOGOUT if don't know source
SSO_FORWARD_URL.LOGOUT=

## External Page for SSO when Timeout (Specify the SSO Server External page for each
## of the case)
SSO_FORWARD_URL.AFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MYAFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MAILBOX.GIS_TIMEOUT=
SSO_FORWARD_URL.WS.GIS_TIMEOUT=
SSO_FORWARD_URL.DASHBOARD.GIS_TIMEOUT=

## Default handling for TIMEOUT if don't know source
SSO_FORWARD_URL.GIS_TIMEOUT=

## External Page for SSO on Validation/Authentication failure (SSO User Validation
## Failed - At login or Page Validation)
SSO_FORWARD_URL.AFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=
SSO_FORWARD_URL.WS.VALIDATION_FAILED=
SSO_FORWARD_URL.DASHBOARD.VALIDATION_FAILED=

## Default handling for VALIDATION FAILED if don't know source
SSO_FORWARD_URL.VALIDATION_FAILED=
```

3. Below the ##SSO Authentication configuration entry, make the following changes to the SSO parameters:

Parameter	Description	Shipped Value	Change to
SSO_AUTHENTICATION_ENABLED	Enables or disables the use of SSO.	False	True
SSO_USER_HEADER	User header name from Netegrity SiteMinder or your SSO application configuration.	SM_USER This is the value in Netegrity SiteMinder.	Must match the entry in Netegrity SiteMinder, or your SSO application.

Parameter	Description	Shipped Value	Change to
SSO_PAGE_AUTHENTICATION_ENABLED	Enables or disables SSO authentication on every page	False	True to authenticate SSO on every page. Change only if custom SSO Provider Class is provided.
SSO_AUTHENTICATION_CLASS.n	Implementation class to provide authentication support.	com.sterlingcommerce.woodstock.security.authentication.SSOProviderDefault	Select from the list of supplied SSOProvider classes.
SSO_FORWARD_URL <type the URL>	Displays the URL page provided after you log off from Mailbox. Else, displays the default.	Commented Displays default page.	Provide the URL.

4. Save the security.properties file using the same name in the same directory.
5. Start Gentran Integration Suite.

The changes to the security.properties file are applied and you can now begin using SSO to authenticate users.

Netegrity Secure Proxy Server 1.1 Configuration

Before you can use Single-Sign On with Gentran Integration Suite, you must configure your secure proxy server to work with Gentran Integration Suite.

Before you configure the Netegrity Secure Proxy Server, you must:

- Install Gentran Integration Suite on a server such as acme.gis.com
- Note the port number that the Gentran Integration Suite Administrator (ws) user interface and the Mailbox Browser Interface (MBI) are installed on. You must use this information in the appropriate forwarding rules.
- Note the port number that the Gentran Integration Suite Dashboard user interface is installed on.You must use this information in the appropriate forwarding rules.

This document contains the following sections:

- Configuring the Netegrity Secure Proxy Server
- Configuring Netegrity Policy Server

Configuring the Netegrity Secure Proxy Server

To configure the Netegrity Secure Proxy Server:

1. Add the necessary forwarding rules for Gentran Integration Suite to the /opt/netegrity/proxy-engine/conf/proxyrules.xml file.

   The following example shows how the completed proxyrules.xml file should look after you add the forwarding rules to access the Gentran Integration Suite components:

```
<?xml version="1.0"?>
<?cocoon-process type="xslt"?>
<!DOCTYPE nete:proxyrules SYSTEM
"file:////home/netegrity/proxy-engine/conf/dtd/proxyrules.dtd">

<!-- Proxy Rules-->
<nete:proxyrules xmlns:nete="http://acme.com/">
   <nete:cond criteria="beginswith" type="uri">
<nete:case value="/ws">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/gbm">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/help">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/certwiz">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/webxtools">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/ssdk">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/mailbox">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/dashboard">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/communitymanagement">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/portlets">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/datastore">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:default>
   <nete:forward>http://acme.portalserver.com$0</nete:forward>
</nete:default>
</nete:cond>
</nete:proxyrules>
```

2. Add the following to the lines to the proxyrules.xml file to turn off the Cross Server Scripting checking in the secure proxy server, since Gentran Integration Suite does not support Netegrity Cross Server Scripting policy enforcement.

```
# Web Agent.conf
<WebAgent>
...." existing web agent configuration parameters"
badurlchars=""
badcsschars=""
CSSChecking="NO"
</WebAgent>
```

3. Save the proxyrules.xml file in the same location and using the same file name to complete the configuration.

Configuring Netegrity Policy Server

For Gentran Integration Suite to work with Netegrity Secure Proxy Server, the Netegrity Policy Server Administrator must create Secure Realms around each of the URL patterns being forwarded by the Secure Proxy Server. These Security Realms must have the necessary rules assigned for authentication and authorization. In addition, the Web agent in the Secure Proxy Server must be configured to communicate with the Policy Server.

The following table describes the URL patterns that require secure realms:

URL Pattern	Enables Access To
/ws/*	Standard Gentran Integration Suite interface, using the http://host:port/ws format
/mbi/*	Gentran Integration Suite Mailbox interface
/dashboard/*	Gentran Integration Suite dashboard interface, using the http://host:port/dashboard format
/communitymanagement/*	Gentran Integration Suite community management interface through the dashboard interface
/datastore/*	Datastore components
/portlets/*	Gentran Integration Suite portlet components in the dashboard interface
/ssdk/*	Service Developer’s Kit components
/help/*	Context-sensitive help components
/webxtools/*	Web Extensions Utilities
/certwiz/*	Certificate Wizard components
/gbm/*	Graphical Process Modeler components

Single Sign On Plug-in Components

Gentran Integration Suite allows custom implementation class for SSO plug-in on other single sign on applications and servers.

You must add a new implementation class `SSO_AUTHENTICATION_CLASS.<n>=<New class entry>` in security.properties file to implement SSO plug-in.

You can write custom implementation class for SSO plug-in based on the following ISSOProvider.java interface class.

ISSOProvider.java interface class

```
import javax.servlet.*;
import javax.servlet.http.*;
public interface ISSOProvider {
public static final int REASON_UNKNOWN = -1;
public static final int REASON_SSO_SESSION_EXPIRED = 1
public static final int REASON_HTTP_SESSION_EXPIRED = 2;
public static final int REASON_LOGOUT = 3;
public static final int REASON_SSO_AUTHENTICATION_FAILURE = 4;
public static final int REASON_GIS_AUTHENTICATION_FAILURE = 5;

public String authenticate(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;

public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
throws SSOAuthenticationException;

public boolean authenticatePage(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
}
```

The SSOException and SSOAuthenticationException classes are as below.

SSOException class

```
public class SSOException extends Exception {
private int reason = -1;
public int getReason() { return reason; }
public void setReason(int reason) { this.reason = reason; }
}
```

SSOAuthenticationException class

```
public class SSOAuthenticationException extends SSOException { }
```

Authenticating the Users

The authenticate method will be initialized during login. The authenticate method returns the user ID after successful authentication. The SSOAuthenticationException is thrown for unsuccessful authentication. The exception should contain an appropriate reason code and a redirecting page to handle if SSO headers are present. If SSO headers are not present, the control is passed back to the Gentran Integration Suite normal login screen.

Authenticating the Pages

The authenticatePage method will be initialized on each page. Any additional validation during page transition from the SSO server is handled in this method. For example, you can ping SSO server to check if the SSO session has timed out. For unsuccessful authentication, an exception should be thrown, which should contain an appropriate reason code and a redirecting page.

Invalidating SSO Requests

The invalidate method will be initialized when the user logs off, fails to authenticate login or page, or when the session expires. The HTTP redirection method should be performed for invalidating SSO requests. The following methods are initialized for unsuccessful authentication:

- If the SSO server authentication is successful and the Gentran Integration Suite authentication is unsuccessful, the REASON_GIS_AUTHENTICATION_FAILURE method is initialized with the reason code.
- If the SSO server authentication is unsuccessful, the REASON_SSO_AUTHENTICATION_FAILURE method is initialized with the reason code.
- If the user logs off, the REASON_LOGOUT method is initialized with the reason code.
- If the HTTP session expires, the REASON_HTTP_SESSION_EXPIRED method is initialized with the reason code.
- If the user's SSO session expires, the REASON_SSO_SESSION_EXPIRED method is initialized with the reason code.

Default SSOProvider Class

The SSOProviderDefault interface is included for SSO plug-in to handle the single sign on function for Netegrity SiteMinder. The SSOProviderDefault interface provides SSO authentication for the following interfaces:

- Administration Interface
- Mailboxing Interface
- Dashboard Interface
- Advanced File Transfer (AFT) Interface
- MyAFT Interface

The SSO login URL for all interfaces except dashboard is similar to the normal login interface. The dashboard interface URL is http:<Host>:<port>/dashboard/sso.jsp. The request header for dashboard interface must have the value SM_USER=<SSO User Name> (or the value can be configured in security.properties file under SSO_USER_HEADER).

You can configure the SSO to redirect to an external HTTP page after the user logs off from SSO session instead of Gentran Integration Suite logoff page. The external page from SSO server can be either login or logoff page.

The following example shows the SSOProviderDefault.java class:

```
package com.sterlingcommerce.woodstock.security.authentication;

import javax.servlet.*;
import javax.servlet.http.*;
import com.sterlingcommerce.woodstock.security.SecurityManager;
import com.sterlingcommerce.woodstock.util.frame.log.Logger;
import java.util.Properties;
import com.sterlingcommerce.woodstock.util.frame.Manager;

import java.util.*;

/**
 * Default Single Sign On implementation for ISSOProvider that will use
 * Request Header to get SSO_USER
 *
 * @author Mach Le
 */

public final class SSOProviderDefault implements ISSOProvider  {

    private static final String CLASS_NAME = "SSOProviderDefault";
    private static final Logger LOG = SecurityManager.getInstance().getLogger();
    private static final Logger AUTHLOG =
            SecurityManager.getInstance().getAuthenticationLogger();
/**
* Authenticate SSO processing (login)
*
* @param Request : The http request.
*
* @return String : The SSO User ID if the authentication is passed
*                 : null if authentication is denied
* << No Exception thrown for the default SSO Provider - Either have value or null >>
*/
public String authenticate(HttpServletRequest request)
                         throws SSOAuthenticationException, SSOException
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());

    if (AUTHLOG.debug) {
          AUTHLOG.logDebug(CLASS_NAME + " Authenticate user tag : " +
              SecurityManager.getInstance().getSSOAuthenticationHeader() +
              " value : " + sso_user);
    }
    return sso_user;
}

/**
 * AuthenticatePage SSO processing (Page)
 *
 * @param Request : The http request.
 *
 * @return boolean : True if the SSO authentication on the Page is passed or no Page
 *                   authentication is needed because not enable or not SSO User.
 *                 : False if authentication is denied
 *                   (Must throw SSOException if return false!!!!)
 */
public boolean authenticatePage(HttpServletRequest request)
                          throws SSOAuthenticationException, SSOException
{
    return true; // Always pass Page Validation for SSOProviderDefault

    /*****  Uncomment if want to do SSO_USER_HEADER (SM_USER) check on Page
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (sso_user != null) {
       passed = true;
    } else {
       passed = false;
       throw new
   SSOAuthenticationException(ISSOProvider.REASON_SSO_AUTHENTICATION_FAILURE);
    }
    return passed;   ******/
}

/**
 * When user logs out, calling this to do any extra actions
 *
 * @param Request : The http request.
 * @param Response : The http response
 * @param int reason : An id to to tell where we called from
 * @param String : The String identify the session type: WS, DASHBOARD, MAILBOX,
 *             AFT, MYAFT, or null if don't know
 *
 * @return boolean : True if executes sucessfully,
 *            False if not & should use default logout logic
 *
 */
public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
{
    HttpSession session = request.getSession(false);
    String forward = "SSO_FORWARD_URL";

    if (sessionType != null)   {
       forward = forward + ".";
       forward = forward + sessionType;
    }

    if (reason == REASON_GIS_SESSION_EXPIRED) {
       forward = forward + ".GIS_TIMEOUT";
    }
    else if (reason == REASON_LOGOUT)  {
       forward = forward + ".LOGOUT";
    }
    else {  // Others reason : send all to VALIDATION_FAILED
       forward = forward + ".VALIDATION_FAILED";
    }

    String forwardUrl = getForwardURLParameter(forward);
    if (AUTHLOG.debug) {
       AUTHLOG.logDebug(CLASS_NAME + " Forward properties: " + forward +
" is forwardUrl: " + forwardUrl);
    }
    if (forwardUrl != null) {
       try {
           // Dashboard Timeout - Use JSP to kick out of IFrame
           if ((reason == REASON_GIS_SESSION_EXPIRED) &&
  (sessionType != null) &&
                (sessionType.equalsIgnoreCase(DASHBOARD_SESSION))) {
               if (AUTHLOG.debug) {
                    AUTHLOG.logDebug(CLASS_NAME + " Set ExternalSsoUrl = "
                                                + forwardUrl);   }
               request.setAttribute("ExternalSsoUrl", forwardUrl);
               return false; // Set to false, we need to handle redirect in JSP
```

```
            } else {
                response.sendRedirect(response.encodeRedirectURL(forwardUrl));
            }
        } catch (Exception e) {
            return false;
        }
        return true;
    }
    return false;   // Use default logic (ie: GIS Logout/Login Page)
}
}
```

Build 4307 or Higher

Connect:Direct Server Adapter Certificate Common Name Validation

Remote Connect:Direct Server authentication can be enhanced with common name (CN) validation. During the TLS/SSL handshake, the common name field from the remote node's certificate is compared with a value that has been preconfigured on the Connect:Direct Server adapter. If the values match, the remote node is authenticated.

Common Name validation is optional. If no value for comparison is configured, no validation occurs.

How Common Name Validation Works

The Connect:Direct Server Adapter (CDSA) secures document (file) transfer using the Connect:Direct Secure+ protocol.

The Secure+ protocol is implemented using TLS/SSL. Each session begins with a handshake, or exchange of messages. The handshake allows the server to authenticate itself to the client by using public key techniques. Optionally, the handshake allows the client to authenticate itself to the server.

A digital certificate binds a public key together with an identity and is used to verify that the public key belongs to the individual or organization. The certificate's identity component consists of the organization's (or individual's) name, address, and contact information. These are specified using name/value pairs for the following keywords: country (C), state/province (ST), locale (L), owner (O), distinguished name (DN), organizational unit (OU) and common name (CN).

Note the common name in the following example of a certificate from a remote node:

```
X509 Certificate SerialNumber: 123
  Issuer: O=SCI, L=Irving, ST=Texas, C=US
  Subject: C=US, ST=Texas, O=SCI, OU=SV, CN=remote.common.name.com,
EMAIL=user@domain.com
  Valid from: Tue Jun 20 12:00:18 EDT 2006   to: Fri Jun 17 12:00:18 EDT 2016
  Signature Algorithm: MD5withRSA
  Thumbprint Algorithm: sha1
  Thumbprint: E40E DF02 B0BB 9346 3FB2 13F3 6460 0F7A E555 1AD7
```

Plan for Configuration

When configuring a Connect:Direct Server adapter, you can specify a value to be compared with the common name field from a digital certificate. The common name value can come from the server certificate (when the CDSA is the PNODE, or primary node) or a client certificate (when the CDSA is the SNODE, or secondary node).

The value for the Common Name field can be configured per adapter, during the configuration of each CDSA, or on a node-by-node basis when NetMap Override is configured.

Configure Certificate Common Name Validation for an Adapter

Before you begin, check in any CA Certificate needed.

Configure the Connect:Direct Server adapter, including the following steps:

1. For Enable Secure+, select Yes.
2. Enter the Common name value to be compared with the CN field on the certificate of the remote node.

   The value entered should match the common name specified in remote Connect:Direct server node’s system certificate.

Configure Certificate Common Name Validation on a Per-node Basis

Before you begin, check in any CA Certificate needed.

Configure the Connect:Direct Server adapter, including the following steps:

1. On the Encryption page, for Enable Secure+, select Yes.
2. For Enable Netmap Node Override select Yes and click Next.
3. (Required) On the Secure+ Configuration page, select the applicable CA Certificates, System Certificate, and Cipher Suites.
4. On the Secure+ Configuration page, choose SSL (default or TLS). (Criteria?)
5. For Require Client Authentication, select Yes (default) or No and click Next.
6. On the Nodes page, select or add the node for which you want to configure CN validation.
7. On the Nodes: Specification page, enter the Connect:Direct Server Node Name, Connect:Direct Server Host, and Connect:Direct Server Port:
8. (Optional) For Secure+ Option, select Disabled (default) or Enabled and click Next.
9. Enter the Common name value to be compared with the CN field on the certificate of the remote node.

   The value entered should match the common name specified in remote Connect:Direct server node’s system certificate.

View the Common Names Being Compared

To see the common names that are actually being compared, set the Perimeter Services logging level to ALL.

This is a log file example:

```
[timestamp] DEBUG <Thread-594> 000000000000 GLOBAL_SCOPE
[TLSCheck.certificateCallback] Domain name provided by the user: cdwopsxp01
[timestamp] DEBUG <Thread-594> 000000000000 GLOBAL_SCOPE
[TLSCheck.certificateCallback] Common Name does not match
cdwopsxp01.csg.stercomm.com:cdwopsxp01
```

Install MSMQPrime

To install MSMQPrime, complete the following steps:

1. Locate the msmqbundle_2006.jar in Gentran Integration Suite under *install_dir*/client/msmq.

Note: The msmqbundle_2006.jar used to create the MSMQPrime component must be from the same version of Gentran Integration Suite as the MSMQAdapter it will communicate with.

2. On the Windows MSMQ server host, create a folder for MSMQPrime. Example: `C:\MSMQ`
3. Copy the msmqbundle_2006.jar to the folder you just created.
4. Change directory to that folder, and use winzip to unbundle the .jar file.
5. Install the Java JDK version 1.5.0_11, noting the installation path.
6. Modify start_msmqPrime.cmd located in the folder you created in step 2.
7. Set the MSMQADAPTER parameter to the folder you created in step 2.
8. Set the JAVA parameter to point to the bin directory in the Java path created in step 5. Example: `C:\jdk1.5.0_11\bin`

Note: \If Java is installed in the default installation folder in `C:\Program Files\Java\jdk1.5.0_11`, you will need to reference it as `C:\Progra~1\Java\jdk1.5.0_11\bin`

9. The default port number for msmqPrime is 8085. If there is a need to change it, edit the msmqprim.properties file in the folder created in step 2.
10. Run start_msmqPrime.cmd located in the directory created in step 2. This script should be run by the user who has permission to create queues, read, and send messages to the MSMQ server.

    This process must be running continually if your MSMQ adapter needs to access it. It is recommended to convert it to an automatically started Windows service (see below).
11. Create a configuration of the MSMQ adapter in GIS and configure it to point to this instance of msmqPrime.
12. Verify that the MSMQ adapter configuration is talking to this msmqPrime by including it in a business process and running it.

    If desired for testing purposes, turn on debug mode in msmqPrime with this command:

```
start_msmqPrime.cmd debugon
```

The debugon option generates detailed logs.

13. To start msmqPrime with the debug mode turned off, use this command:
```
start_msmqPrime.cmd
```

Patch Installation

The msmqbundle_2006.jar must be redeployed to the Windows MSMQ server host when a Gentran Integration Suite patch is installed, as new code changes need to be synchronized with msmqPrime.

Install MSMQPrime as a Windows Service

1. Unbundle the msmqbundle_2006.jar file. This creates a directory called installJavaService.
2. Modify the installJavaService\InstallJavaService.cmd script to set the Java parameter to the bin directory in the Java path (see step 8 above) and set the MSMQINSTALLDIR parameter to the folder created in step 2 above.
3. To turn on debug mode, set the PARAMS to debug. Default is “not set” (debugging off).
4. From a command prompt, run the `installJavaService.cmd` script. This installs the MSMQPrime as a Windows service.

Run MSMQPrime as a Windows Service

To start MSMQPrime as a Windows service, from the Windows Services applet select the New MSMQAdapter and select **Start**.

To stop the service, from the Windows Services applet, select the MSMQAdapter and select **Stop**.

Uninstall the Service

To uninstall MSMQPrime as a Windows Service, run this script:

```
installJavaService\uninstallJavaService.cmd
```

Configuring SSL Enhancements for IBM® WebSphere MQ

Configuration to support SSL consists of two steps:

- Configure server for authentication
- Configure client for authentication

Plan for Configuration

The cipher suites and specifications in the following table are supported by IBM WebSphere MQ. However, not all are supported on WebSphere MQ versions below 6.0.

Cipher Suite	Cipher Specification	Supported below MQ v6.0?
SSL_RSA_WITH_NULL_MD5	NULL_MD5	NO
SSL_RSA_WITH_NULL_SHA	NULL_SHA	NO
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RC4_MD5_EXPORT	NO
SSL_RSA_WITH_RC4_128_MD5	RC4_MD5_US	NO
SSL_RSA_WITH_RC4_128_SHA	RC4_SHA_US	NO
SSL_RSA_WITH_DES_CBC_SHA	(v6.0 and above) DES_SHA_EXPORT (v 5.3) TLS_RSA_WITH_DES_CBC_SHA	YES
SSL_RSA_WITH_3DES_EDE_CBC_SHA	(v6.0 and above) TRIPLE_DES_SHA_US (v5.3) TLS_RSA_WITH_3DES_EDE_CBC_SHA	YES

Configure Your Server for Server Authentication

Server authentication is configured in the IBM Key Manager Tool.

1. Open the IBM Key Manager Tool. To create the key Database for the queue manager, go to **Key Database** > **New** > **key.kdb**
2. Select CMS for the Key database type.
3. Create and save an SSL key store file for the queue manager.

   Example: For a queue manager named MyQueueManager, the SSL key store would be located at `C:/ProgramFiles/IBMwebsphereMQ/qmgrs/MyQueueManager/ssl/key.kdb`
4. Enter the password for this key database file and stash the password to a file.
5. Select **Personal Certificate Requests** from the pulldown. Click on **New**.
6. Enter the information required to get the csr request file. This file will be sent to the CA to get the signed certificate for this queue manager.

   Alternately, you can create a self-signed certificate instead of using CA signed certificate.

Note: While generating the csr, make sure that the title for the certificate is ibmwebspheremq*queuemanagername* in lowercase letters. Example: ibmwebspheremqmyqueuemanager.

7. Before Checking in the certificate received from the CA, make sure the root certificate of the CA should be checked in as the Signer Certificate.

8. Select **Personal Certificates** from the pulldown. Click on **Receive** to add the certificate received from the CA for this queue manager. Example: cert.der
9. Open the IBM MQ Explorer. Right-click on the ***Queue manager in use***> **Properties > SSL**.
10. Set the key repository to the path of the key.kdb file generated above. Example:

```
C: /ProgramFiles/IBM/WebSphereMQ/Qmgrs/MyQueueManager/ssl/key
```

Note: No file extension is required for a kdb file.

11. Select **Queue Manager > Advanced > Channels**. Navigate to the server Connection Channel that is being used on the application side in the configuration of our adapter, and right-click it. Example: SYSTEM_ADMIN_SVRCONN
12. Right-click this channel, go to **SSL**, and select the correct SSL CipherSpec from the dropdown.
13. For Server Authentication, set **Authentication of parties initiating connections** to **Optional**. This completes the SSL settings for server authentication on the server side.
14. Use the IBM Key Management Tool to extract the certificate we created above from the **Personal Certificates > extract**. Example: The certificate is extracted as myqueuemanager.der)
15. To import this certificate into our application (to use the certificate for the authentication of this queue manager, go to **Trading Partner > Digital Certificates > CA** in your application.
16. Add the certificate extracted above here.
17. Configure the WebSphereMQ Adapter, WsmqSuite Aysnc Adapter to set this certificate as the CA certificate. Using wsmqSuite to send the messages, this can be chosen from the pulldown menu using GPM.

CLIENT AUTHENTICATION

In client authentication, not only does the client authenticate the server, but the server also authenticates the client. To do this, repeat the above steps to create a platform for server authentication. For client authentication, follow these steps:

1. On your application, go to **Digital Certificates > System Certificates**. Create a self-signed certificate, or run the certificate wizard to create a CA signed certificate.
2. Send the csr to the CA and get the client certificate.

Note: In this case, there is no restriction on the label name as it there was for server authentication.

3. The generated certificate can be viewed in the text format under System Certificates. Extract this file and import inside the key repository key.kdb you created above for the queuemanager. Import it bychoosing the Signer Certificates in the IBM Key Management Tool.
4. Under **MQ Explorer > *MyQueueManager* > Advanced > Channels > Properties > SSL**, set **Authentication of parties initiating connections** to **Required**.
5. Shutdown and restart it to initiate some security updates.
6. On the SSL page in the services configuration of WebSphereMQ adapters in your application, choose the trusted certificates and Key Certificates for the client authentication.

SSL Enhancements for WebsphereMQ Suite and WebSphereMQ Adapter

The WebSphereMQ Suite and the WebSphere adapter now support SSL with these enhancements:

- SSL cipher specification at channel level for the WebsphereMQ Suite Async Receive adapter
- Parameters for server and client authentication

WebSphereMQ Server

When configuring the Websphere MQ server to communicate with a WebsphereMQ Suite adapter with SSL enabled, the SSL cipher is specified at the channel level.

WebSphereMQ Suite Async Receive Adapter

The following settings are configured in the user interface to enable SSL for the WebSphereMQ Async Receive adapter:

Parameter	Value(s)
SSL_SETTING_ca_cert_ids	For server authentication. For MQ, only one certificate may be selected. Example: MBradley1:1decdec:11159ba495b:-583c,frcppe03z3:1037c71:11584abf184:-7c4d,MBradley1:1decdec:11159ba495b:-5837 MBradley1:1decdec:11159ba495b:-5837
SSL_SETTING_keyCertID	For client authentication. Example: frcppe03z3:1df073d:1153772f2cb:-66de mg2sdsb:1a679b7:116218d328a:-5e84
SSL_SETTING_cipherSuite	A valid SSL Version 2 or Version 3 cipher specification, chosen from the dropdown. Example: SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_SETTING_ssl_option	Whether SSL is or is not active. Valid values: SSL_MUST SSL_NONE

WebSphere MQ Adapter

The same parameters are configured in the user interface for the WebSphere MQ adapter.

WebSphere MQ Suite Adapter

To send messages using the WebSphere MQ Suite adapter, set the parameters in a business process. Example:

```
<PARM>
<name>SSL_SETTING_ca_cert_ids</name>
<value>MBradley1:1decdec:11159ba495b:-583c,frcppe03z3:1037c71:11584abf184:-7c4d,MBra
dley1:1decdec:11159ba495b:-5837</value>
</PARM>
<PARM>
<name>SSL_SETTING_cipherSuite</name>
<value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</value>
</PARM>
<PARM>
<name>SSL_SETTING_keyCertID</name>
<value>frcppe03z3:1df073d:1153772f2cb:-66de</value>
</PARM>
<PARM>
<name>SSL_SETTING_ssl_option</name>
<value>SSL_MUST</value>
</PARM>
```

Using nCipher and SafeNet/Eracom Network and PCI Devices with Gentran Integration Suite

Gentran Integration Suite currently supports Safenet/Eracom ProtectServer Orance PCI card and Orance External network device. With this enhancement, we’re adding support for nCipher. For additional information see System Certificates and Hardware Security Modules (HSM).

Manufacturer	Device Types Supported
nCipher	◆ nShield series of PCI cards ◆ NetHSM network devices
Safenet/Eracom	◆ ProtectServer Gold PCI card ◆ ProtectServer Orange PCI card ◆ ProtectServer Orange External network device

Configure your Hardware Security Module (HSM)

Install and configure cards or HSMs according to the vendor's instructions. Ensure that java runtime components are available to interact with the device.

Gentran Integration Suite Features for HSM Support

An entry is stored in the CERTS_AND_PRI_KEY table by Gentran Integration Suite for each key pair and certificate. This entry contains information about:

- Keys and certificates, including the validity period, serial number, usage restrictions, issuer and subject used by the UI to display to the user without having to actually access the key or certificate
- Normalizations of the distinguished name used by the system in searches
- Modifications to the record
- Certificate revocation status information
- Keystore type
- References to a binary keystore object stored in the DATA_TABLE. When a software keystore is used, the referenced object may contain key material. In the case of an HSM, it contains either reference information (nCipher) or a placeholder (Eracom).

Using the KeyStoreProviderMap

Because Gentran Integration Suite has the keystore type that is unique across cryptographic service providers, it is able to define a mapping between keystore types and providers required for implementing the keystore object itself, signature algorithms, and key transport algorithms.

The key and key information abstraction object contains this information with a reference to a com.sterlingcommerce.security.PrivateKeyInfo.

This allows Gentran Integration Suite to use a combination of keys on HSMs and in software stores in the database at the same time without additional configuration beyond the initial loading of the key or key information into the database. To Gentran Integration Suite, the keys all look the same, regardless of where they are stored.

Mapping is implemented as a property called KeyStoreProviderMap in security.properties. It consists of a set of entries delimited by semi colons (;). Each entry has six fields delimited by commas and follow this format:

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

Element	Description	Additional Information
KeyStoreType	The string type of the keystore	
KeyStoreProvider	The name of the cryptographic service provider that implements the keystore	

Element	Description	Additional Information
DoesAliasMatter	Whether the alias of keys must be unique for this keystore type	This can be either true or false. Keys have to have unique aliases in the case where there is only one keystore per device.
SignatureProvider	The name of the cryptographic service provider to use to create signatures using keys from the keystore	
EncryptionProvider	The name of the cryptographic service provider to use when decrypting information using keys in the keystore	This is mostly for RSA key transport operations
KeyOnHSM	Whether the keystore is on an HSM	

The string null is an acceptable value and will be treated as though no provider has been specified. An entry must have at least two values. If an entry contains less than six values, the values will be assigned from left to right to the keystore provider, whether the alias matters when storing the key, signature provider, encryption provider, and whether the key is on an HSM for the KeyStore type. The others will be treated as nulls and no specific provider will be requested for operations with keys of that type.

The default KeyStoreProviderMap is currently:

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;nCipher.sworld,nCipher
KM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM,true,ERACOM,ERACOM,true
```

Managing HSM Keys and Key Information for Gentran Integration Suite

Gentran Integration Suite has several java scripts for managing keys on HSMs. The java programs are listed below.

Program	Purpose
com.sterlingcommerce.db.RemoveSystemCert	Both list and delete Gentran Integration Suite system certificates. During a delete, the program makes a best effort to clear the key from the keystore and overwrite the keystore object in the database.
com.sterlingcommerce.db.CreateCertEx	Generate a key pair on an HSM and a self-signed certificate containing the public key of the key pair.
com.sterlingcommerce.security.util.CertificateSigningRequest	Generate a key pair on an HSM and create and manage an associated PKCS10 certificate signing request. The PKCS10 can be provided to an authority to get a certificate signed by the authority. This program can be used to then load that certificate into the keystore and associate it with the right key pair.
com.sterlingcommerce.db.ImportSystemCert	Import a private key and certificate in a supported format (PKCS12 or PEM) into a keystore on an HSM. Import information about a private key and certificate on an HSM into the Gentran Integration Suite database.

JDK Changes for nCipher HSM Support

In order for Gentran Integration Suite to utilize nCipher HSMs, you must install the nCipher java cryptographic service providers. To install, copy the following jar files in the jre/lib/ext subdirectory of your JDK. Modify java.security to load the nCipher providers. The following files are placed in */opt/nfast/java/classes* by the nCipher installation program:

- rsaprivenc.jar
- nfjava.jar,
- kmjava.jar
- jutils.jar
- kmcsp.jar

You should add the nCipher providers after the IBM JCE provider and before the Certicom provider. For example:

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
```

On Solaris systems with the SUN JDK, you should place the nCipher providers after the Sun JCA and JCE providers and before the Certicom provider. For example:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.4=com.ncipher.provider.km.nCipherKM
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=com.sun.net.ssl.internal.ssl.Provider
security.provider.7=com.sun.rsajca.Provider
security.provider.8=sun.security.jgss.SunProvider
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
```

7. Set up a TLSProvider policy using the sample in security.properties. For example:

```
TLSProviderPolicy=TLS:MD:MD5:P:Certicom;TLS:MD:SHA1:P:Certicom;TLS:MAC:HmacMD5:P:Cer
ticom;TLS:MAC:HmacSHA1:P:Certicom;TLS:SIG:MD2withRSA:P:Certicom;TLS:Cipher:RawRSA:P:
Certicom;TLS:*:ECDH:P:Certicom;TLS:*:ECDSA:P:Certicom;TLS:*:*:P:nCipherKM
```

JDK Changes for Eracom HSM Support

In order for Gentran Integration Suite to utilize Eracom HSMs, you must install the Eracom java cryptographic service provider. To install, place the appropriate.jar files in the *jre/lib/ext* subdirectory of your JDK and then modify java.security to load the nCipher providers. These files are placed in */opt/nfast/java/classes* by the nCipher install program:

- jcprov.jar
- jprov.jar

You should add the Eracom provider after the Certicom provider. For example:

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=au.com.eracom.crypto.provider.ERACOMProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.8=com.sterlingcommerce.security.provider.SCI
```

Note: Eracom has a provider that can be specified for each slot on the card. For the provider for slot 8, use:

```
security.provider.3=au.com.eracom.crypto.provider.slot8.ERACOMProvider
```

(Linux) Environment Changes for nCipher HSM Support

nCipher recommends that you create a special user account for running the nCipher hardserver. The account from which you run Gentran Integration Suite needs to have equivalent permissions, or you need to run Gentran Integration Suite from the nCipher special account or as root. If you do either of these and are using MySQL, you must change the permissions for MySQL, or start MySQL from your normal account before invoking run.sh.

(Linux) Environment Changes for Eracom HSM Support

To use the Eracom device, you must supply additional information in environment variables to the session that will access the device. Recommended changes to PATH, LD_LIBRARY_PATH, and MANPATH are as follows:

```
PATH=$PATH:/opt/Eracom/bin
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/Eracom/lib
MANPATH=$MANPATH:/opt/Eracom/man
```

In addition, if you are using a network device rather than a local PCI card, you must supply ET_HSM_NETCLIENT_SERVERLIST, as follows:

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

You should export these variables in tmp.sh.

Build 4303 or Higher

Web Services Enhancements

Gentran Integration Suite 4.3, Build 4303 contains these enhancement to Web services (WS) as provider and consumer:

- HTTPS supported as transport binding in Web services / Dynamic service creation now platform-independent
- MesaAuth element generation optional
- UI pages enhanced for WS-I Basic Profile and Basic Security Profile 1.0 compliance
- SOAP generation enhanced to add encoding type
- Valuetype attribute added to STR_KEY_IDENTIFIER SOAP in message encryption and signing
- XML encryption and decryption supported
- Encryption algorithm encrypts complete contents of SOAP message body
- Public key encryption supported
- Flexible ordering of signature and encryption
- New Services
- New tables
- Properties file changes

Note: New security services do not support signing an attachment.

New properties were added to the soa.properties file to support HTTPS and encryption.

Overall considerations for the Web services enhancements included backward compatibility with existing customer Web services instances, compatibility of all enhancements with the Stercomm JCE, elimination of Bouncy Castle as a JCE provider, and interoperability with Web service clients such as Axis and XFire.

HTTPS supported as transport binding in Web services / Dynamic service creation now platform-independent

The Web services layer in Gentran Integration Suite supports HTTPS (HTTP with SSL), in addition to HTTP, as its transport binding.

Formerly, Gentran Integration Suite as a Web service consumer called SOAInbound, HTTP Client Adapter, and SOAOutbound at the API level. This restricted users to the HTTP Client adapter for transport. The dynamic service creation process has been refactored to make it transport-independent and allows you to use either an HTTP or HTTPS adapter instance to send the SOAP message to the Web service provider.

You can initiate a transport choice by creating a new Web service (**Admin console > Deployment > Web Services > Manager > Web Services Management: Create)**. On the **SOAP Transport Option** page, you can enable HTTP or HTTPS for the configured Web service. See *Revised Web service creation procedure* for details.

Note: Customers can continue to use existing instance configurations. To ensure backward compatibility, a new HTTP Server adapter instance for HTTPS (“SOA SSL Http Server adapter”) and new URIs (for the existing HTTP Server adapter) have been added for use when the settings on the new Security page are enabled. Customers also have the option to keep the HTTP default, which generates the dynamic service and configures the associated business processes and URIs.

Transport selection requires you to:

- Use the GPM to configure the SOAOutboundMessageProcessing and (if desired) the SOAOutboundSecurityService manually at the business process level for use after the Dynamic Service Generation generates the SOAP message. You must provide an end point address and port to send the SOAP message to the Web service provider.
- Configure the SOAInboundMessageProcessing and (if desired) SOAInboundSecurityService for use after the SOAP message is sent to the Web service provider with the transport protocol of choice.

The WSDL validation logic applied during check in can now validate HTTPS as the SOAP transport mechanism. A new wizard guides you during the check in process. See *Additional Field Definitions for Checking in WSDL for a Web Service Procedure* for details.

The WSDL Check-in Summary page displays dynamic service-related information. It now displays Service Type, Service Name, Service Description, and System Name for each operation in the checked-in WSDL.

MesaAuth element generation now optional

The MesaAuth Type schema element was formerly inserted into the "types" section of the generated WSDL even when Consumers were not selected. Now Consumers must be selected for the MesaAuth element to be inserted into the WSDL. This allows you to generate WS-I Basic Profile 1.1 compliant WSDL.

UI pages enhanced for WS-I Basic Profile and Basic Security Profile 1.0 compliance

The Response Security Settings page has been enhanced to inform users about the selection of Canonicalization Algorithm and Symmetric Algorithm values for Signing and Encryption, respectively. This conforms to WS-I Basic Security Profile 1.0.

The WS-I Compliance page now identifies the version of the WS-I Basic Profile to which the generated WSDL conforms.

SOAP generation enhanced to add encoding type

Response generation logic in the Security API has been enhanced to add the EncodingType attribute to the Nonce element, if not already generated.

Valuetype attribute added to STR_KEY_IDENTIFIER SOAP in message encryption and signing

The value SubjectKeyIdentifier was added to the SigningKeyIdentifier and EncryptionKeyIdentifier attributes. If selected in the Response Security Settings UI page, this value makes the response compliant with WS-I BSP1.0.

Web services business processes restructured

Two new business processes have been added to handle Web service invocation:

- WS_MessageHandler.bpml
- WS_MessageHandler_SSL.bpml

XML encryption and decryption supported

XML encryption and decryption are now supported in the WS-Security implementation. In support of this, some extraneous functionality was removed from the SOAInbound and SOAOutbound services.

Encryption algorithm encrypts complete contents of SOAP message body

The encryption algorithm encrypts the complete contents of the SOAP message body part.

Public key encryption supported

Supports public key encryption whereby elements are encrypted by a randomly generated symmetric key, which in turn gets encrypted by the public key of the recipent. In this mode, the complete encrypted key information is available inside the WS-Security header as an <xenc:EncryptedKey> element.

Flexible ordering of signature and encryption

Documents can be signed either before or after encryption.

New Services

The following new services have been added to support the new security framework:

Service	Function
SOAInboundMsgProcessingService	Handles processing of an incoming SOAP Message and extracts any MIME attachment parts from incoming message and uploads the attachments in the process data. Also extracts the SOAP Envelope from the message and uploads it in the process data as a primary document.
SOAOutboundMsgProcessingService	Constructs the final SOAP Response (MIME or without MIME) using the output of the end point invocation.
SOAInboundRMDecisionService	Determines if the incoming SOAP message carries WS-RM header. This service always expects a SOAP Envelope as an input.
SOAInboundSecurityService	Processes WS-Security Headers (including timestamps, username token, signature verification and decryption) in an incoming SOAP message. The input to this service is a SOAP document carrying WS-Security Header and the output is a valid/decrypted SOAP document.
SOAOutboundSecurityService	Creates a WS-Security Header that can carry security timestamps, username token, signature and encryption. The input to this service is a SOAP document without any WS-Security header and the output is a signed, encrypted SOAP document carrying a WS-Security header.
WSConfigInfoService	Loads configuration data from the database for a specific web service configuration and populates those values in the process data.

New tables

Two new tables, WEB_SERVICES_INBOUND_SECURITY (primary key WEB_SERVICE_CONFIG_ID) and WEB_SERVICES_OUTBOUND_SECURITY (primary key WEB_SERVICE_CONFIG_ID), have been added to the database.

Properties file changes

The following new properties have been added to the soa.properties.in file in support of https and WS-encryption.

Note: CAUTION: Back up your soa.properties file to avoid overwriting it when a patch is installed. Some Web services-specific configuration information was formerly included in soa.properties.

Property	Function
defaultBaseURL_SSL	Default SOAP URL for accessing Web services with SSL transport (HTTPS). Additional HTTP/HTTPS Server adapters can be configured. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT; Example: http://00.00.00.12346

Property	Function
defaultSoapURL_SSL	Default SOAP URL for accessing Web services in synchronous mode with SSL transport (HTTPS). Additional HTTP/HTTPS Server adapters can be configured. **Note:** Does not use new security settings. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT;/soap Example: http://00.00.00.12346/soap
synchBPSOAPURL_SSL	Default SOAP URL for accessing Web services in synchronous mode with SSL transport (HTTPS). Additional HTTP/HTTPS Server adapters can be configured. **Note:** Does not use new security settings. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT;/soap-sync Example: http://00.00.00.12346/soap-sync
SoapURL	Default SOAP URL for accessing Web services in asynchronous mode with new security settings. Additional HTTP Server adapters can be configured. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT;/soap-new Example: http://00.00.00.12345/soap-new
SoapURL_SSL	Default SOAP URL for accessing Web services in asynchronous mode with SSL transport (HTTPS) and new security settings. Additional HTTP/HTTPS Server adapters can be configured. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT;/soap-new Example: http://00.00.00.12346/soap-new
SoapURLSync	Default SOAP URL for accessing Web services in synchronous mode with new security settings. Additional HTTP Server adapters can be configured. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT;/soap-sync-new Example: http://00.00.00.12345/soap-sync-new
SoapURLSync_SSL	Default SOAP URL for accessing Web services in synchronous mode with SSL transport (HTTPS) and new security settings. Additional HTTP/HTTPS Server adapters can be configured. **CAUTION**: Do not change this property. Format: http://&HOST_ADDR;:&SOA_PORT;/soap-sync-new Example: http://00.00.00.12345/soap-sync-new

Revised Web service creation procedure

The Field Definitions in this procedure to create a Web service have been updated to include the new transport and security options.

To create a new a Web service:

1. From the Deployment menu, select **Web Services** > **Manager**.

2. Under Create, next to **Create a Web Service Configuration**, click **Go**!
3. Complete the fields in the displayed in the wizard and click **Next** to advance.

Note: Sterling Commerce recommends you to use the new Web services request and response settings to take the full support of the WS-Security specifications.

4. Confirm your selections and click Finish.
5. You have finished this procedure. Click Return to continue.

Web Service Name Field Definitions

Field	**Description**
Name	Unique name for the Web services group. Required.
Description	Description for the Web services group. Required.
Use Synchronous Mode	Check the box if you want to invoke Web services in a synchronous mode.
Use New Security Settings	Check if you want to use new security settings

SOAP Transport Binding Settings

Field	**Description**
Use HTTP as SOAP transport	Use HTTP as the transport protocol.
Use HTTPS as SOAP transport	Use HTTP with SSL as the transport protocol.

Request Security Settings Field Definitions

These are the settings for the default Request Security Settings page. These settings display when the new security settings have not been selected.

Field	**Description**
Verification Certificate	To use a verification certificate (trusted) with the security header, type the certificate name or click the list icon to access available certificates. Select a certificate from the list and click Save. Required if Security Header is yes and Username token is not used.
Security Header	Select Yes if you want to include a security header in the request. If selected, a verification certificate or UserName token, or both, must also be added. Optional.
UserName Token	To add a UserName token with the security header, check the box and select a UserName token from the list. Required if Security Header is yes and verification certificate is not used.

These are the field definitions for the Request Security Settings page with new security settings selected.

Field	Description
Verification Certificate	To use a verification certificate (trusted) with the security header, type the certificate name or click the list icon to access available certificates. Select a certificate from the list and click Save. Required if Security Header is yes and Username token is not used.
Decryption Certificate	Select to decrypt the encrypted body in an incoming request.
UserName Token	Select to verify a username credential in an incoming request.

Response Security Settings Field Definitions

When creating a Web service as a provider, you may select either the default security settings or elect new security settings.

Note: The new security settings are recommended.

The default security settings field definitions (Old implementation) are:

Field	Description
Signing Certificate	To use a signing certificate (system) with the security header, type the certificate name or click the list icon to access available certificates. Select a certificate from the list and click Save. Required if Security Header is yes and Username token is not used.
Security Header	Select Yes if you expect a security header in the response. If selected, a signing certificate (X.509) or UserName token, or both, must also be added. Optional.
Refer X.509 Certificate as	If you use a signing certificate (system), it is in X.509 format. Select how the certificate should be embedded in the Security Header. Required if Security Header is Yes. Valid values are: ◆ BinaryToken - Sends the signing X.509 certificate as a BinarySecurityToken. ◆ IssuerSerial -Sends the issuer name and serial number of a certificate to the receiver. This is the default. ◆ X509KeyIdentifier-Sends the X.509 certificate used to encrypt the symmetric key.
UserName Token	To use a Username token with the security header, check the box and select a UserName token from the list. Required if Security Header is yes and signing certificate is not used.

The new Web service response security settings field definitions are:

Field	Description
WS-Security Header Settings	
Mustunderstand	Check this box to
Actor:	
UserNameToken	Check this box to

Field	Description
UserName Tokens:	
Insert Time Stamp	Check this box to allow creation and expiration times in a message in accordance with WS-Security specification 1.0 (<wsu: Timestamp> element). This allows the recipient of a SOAP message to decline processing a WS-Security header if the associated timestamps are expired.
TimeStampInterval	
SignatureSettings	
Signing Certificate	To use a signing certificate (system) with the security header, type the certificate name or click the list icon to access available certificates. Select a certificate from the list and click Save. Required if Security Header is yes and Username token is not used.
Signing Algorithm	
SigningKeyIdentifier	
CanonicalizationAlgorithm	
EncryptionSettings	
EncryptionCertificate	Type or select
KeyEncodingAlgorithm	
SymmetricAlgorithm	
SigningEncryptionOrder	Select Sign First

Assign Business Processes Field Definitions

Field	Description
Filter by name	To filter the list of available business processes, type part of the business process name into the Filter field and click the Filter icon. Optional.
Available and Selected lists	Select one or more business processes from the list of available business processes on the left to be associated with this Web services group and click the right arrow. To select all available business processes, click the double right arrow. Optional.

Web Service Assign Service Instances Field Definitions

Field	Description
Filter by name	To filter the list of available services, type part of the service name into the Filter field and click the Filter icon. Optional.
Available and Selected lists	Select one or more services from the list of available services on the left to be associated with this Web services group and click the right arrow. To select all available services, click the double right arrow. Optional.

Web Service Assign Consumers Field Definitions

If you select a consumer, the mesaAuth element is inserted into the input message of the generated WSDL. If you do not select a consumer, the mesaAuth element is not inserted into the input message of the generated WSDL and the output is WS-I compliant.

Field	**Description**
Filter by name	To filter the list of available users, type part of the user name into the Filter field and click the Filter icon. Optional.
Available and Selected lists	Select one or more users from the list of available users on the left to be associated with this Web services group and click the right arrow. To select all available services, click the double right arrow. Optional.

Reliability Settings Field Definitions

Caution: You cannot send the same reliable message (with the same groupID and sequenceNo) to two different web services configured in the same application instance, or the operation will fail.

Field	**Description**
Reliability Settings	Select one of the following options: ◆ AutoDetect – Both reliable and non-reliable messages are accepted. This is the default. ◆ ReliableOnly – Only reliable messages are accepted. ◆ NonReliableOnly – Only non-reliable messages are accepted.

Web Service WS-I Conformance Settings Field Definitions

Field	**Description**
Conforming WSDL	Adds a WS-I claim element in every conforming node of WSDL. Optional.
Conforming SOAP Response	Adds a WS-I claim element in the header of a SOAP response. Optional.

Web Service Attachment Settings Field Definitions

Field	**Description**
Input Attachment	Request can have an attachment. Optional.
Output Attachment	Response can have an attachment. Optional.
Inline Attachment	No attachments. Information must be contained inline in the message. Optional.

Additional Field Definitions for Checking in WSDL for a Web Service

Procedure

Naming: WSDL Transport Binding Settings

During the WSDL check-in process, a new page provides options to specify the transport protocol and provide for backward compatibility.

Field	Description
Default Transport (HTTP)	Generates the service dynamically, using the previous implementation of the application. SOAInbound and SOAOutbound services (message processing and security services) do not have to be configured at the business process level. Allows for backward compatibility. The GPM configuration would appear as follows: `Some required service --> Dynamic Service --> Some required service`
Other Transport (HTTP/HTTPS)	The dynamic service is created for the checked-in WSDL. You must configure the business process. Configure the business process as follows and configure the transport protocol (HTTP or HTTPS) of choice. `DynamicService --> SOAOutboundSecurity Service` (optional) --> `SOAOutboundMessageProcessingService --> Transport --> SOAInboundMessageProcessingService --> SOAInboundSecurityService` (optional)