Sterling Integrator

Build Updates

Version 5.0

Sterling Integrator

Build Updates

Version 5.0

Note

Before using this information and the product it supports, read the information in "Notices" on page 69.

Copyright

This edition applies to Version 5 Release 0 of Sterling Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction to Build Updates

This document provides information about fixes and enhancements provided in Sterling Integrator Version 5.0. These builds are cumulative and include all fixes and enhancements contained in the previous build.

Chapter 2. Build 5008 or Higher

Shared and Linked Mailbox Enhancement

The Shared mailbox functionality allows you to instantly share real-time data with the trading partners. You can use the Linked mailbox functionality to link individual trading partner's mailboxes with one or more shared mailboxes. Linking trading partner mailboxes to shared mailboxes allows the trading partners to view the real-time data stored in the shared mailboxes. In other words, a linked mailbox provides a link to view the data in a shared mailbox. The linked mailbox is a read-only copy of the shared mailbox and the data in the mailbox cannot be modified or deleted.

To enable the shared and linked mailbox functionality, set the mailbox.enableSharedLinkedMailboxes property to true in the `customer_overrides.properties` file. By default, this property is set to false.

A linked mailbox can be related to only one shared mailbox. Multiple linked mailboxes can point to the same shared mailbox. Adding data to a shared mailbox immediately makes that data available to all links.

A Regular or a Shared mailbox can be the parent of a Shared mailbox. A Regular or a Linked mailbox can be the parent of a Linked mailbox. A sub-mailbox under a Shared or Linked mailbox must be the same mailbox type as its parent.

A user's regular mailbox can contain a combination of regular, linked, and shared mailboxes. Shared mailboxes and linked mailboxes need not be in the same directory. User permissions can be explicitly applied to linked mailboxes. Routing rules cannot be applied to linked mailboxes. However, virtual roots can be applied directly to linked mailboxes.

The following are some of the limitations when converting a regular mailbox to a shared or linked mailbox and converting a shared or linked mailbox to a regular mailbox:

- A regular mailbox can be converted to a shared or linked mailbox type.
- A shared mailbox can be converted to a regular mailbox type only if the parent of the shared mailbox is a regular mailbox type. The links to the shared mailbox should be removed before converting the shared mailbox to a regular mailbox.
- A linked mailbox can be converted to a regular mailbox type only if the parent of the linked mailbox is a regular mailbox type.
- A shared mailbox cannot be converted to a linked mailbox.
- A linked mailbox cannot be converted to a shared mailbox.
- A regular mailbox with sub-mailboxes can be converted to a linked mailbox type when all the sub-mailboxes are of the linked mailbox type.
- A regular mailbox with sub-mailboxes can be converted to a shared mailbox type when all the sub-mailboxes are of the shared mailbox type.

View a List of Mailboxes

To view a list of mailboxes:

1. From the **Deployment** menu, select **Mailboxes** > **Configuration**.
2. Open the configuration data of the mailbox you want to view using one of the following methods:
   - In the By Mailbox Name field of the Search section, type the name or partial name of the mailbox you want to view and click **Go!**
   - In the Alphabetical section, select the letter the mailbox starts with or select all to pull a list of all mailboxes and click **Go!**
3. A list of available mailboxes opens. The following table describes the content of each column:

Title	**Description**
Select	Contains the icons for: • Editing a mailbox • Deleting a mailbox • Creating a sub-mailbox
Mailbox Name	Displays the name and path of the mailbox
Description	Displays the short description of the mailbox
Type	Displays the type of Mailbox: • R – Regular - Standard mailbox that cannot be linked to any other mailbox • S – Shared - Mailbox that can be linked from other mailboxes • L – Linked - Mailbox whose data is stored in a shared mailbox
Linked To	Displays the shared mailbox path where linked mailboxes are pointing to **Note:** You must remove links to the shared mailboxes before deleting a shared mailbox
Last Modified	Displays the timestamp to indicate when the mailbox was last modified

Create a Shared Mailbox

To create a shared mailbox:

1. From the **Deployment** menu, select **Mailboxes** > **Configuration**.
2. In the **Create** section, click **Go**!
3. In the Mailbox: Name page, select the parent mailbox in which the mailbox you are creating will be embedded. You can type a partial name in the **Filter by Name** field and click the filter button for a filtered list. The root mailbox is denoted by a slash (/).
4. In the **Name** field, type a name for the mailbox you want to create. This name is used to identify the mailbox in the application.
5. In the **Description** field, type a short description for the mailbox. Use this field to describe the mailbox. This is a required field. This field is not used by any other resource in the system.

6. In the Mailbox Type field, select Shared as the type of the mailbox you want to create from the following options:
   - Regular (Default)
   - Shared
   - Linked

   When creating linked sub-mailboxes, the available shared sub-mailboxes will be restricted to those belonging to its parent's shared mailbox.
7. Click **Next**.
8. In the Assign Groups page, use the arrows to add the groups to the Selected Groups list and click **Next**. All groups in the **Selected Groups** list will have permissions on this mailbox.
9. Click the first double arrow to add all available groups to the **Selected Groups** list. You can type a partial group name in the **Filter by Name** field and click the filter button for a filtered list. No groups are required. Groups can be added from the **Accounts** menu.
10. Use the arrows to add users to the Selected Users list and click **Next**. All users in the **Selected Users** list will have permissions on this mailbox. Click the double arrow to add all available users to the **Selected Users** list. You can type a partial user name in the **Filter by ID** field and click the filter button for a filtered list. No users are required. Users can be added from the **Accounts** menu.
11. In the **Confirm** page, verify your mailbox configuration and click **Finish**.

Create a Linked Mailbox

To create a linked mailbox:

1. From the **Deployment** menu, select **Mailboxes** > **Configuration**.
2. In the **Create** section, click **Go!**
3. In the Mailbox: Name page, select the parent mailbox in which the mailbox you are creating will be embedded. You can type a partial name in the **Filter by Name** field and click the filter button for a filtered list. The root mailbox is denoted by a slash (/).
4. In the **Name** field, type a name for the mailbox you want to create. This name is used to identify the mailbox in the application.
5. In the **Description** field, type a short description for the mailbox. Use this field to describe the mailbox. This is a required field. This field is not used by any other resource in the system.
6. In the Mailbox Type field, select Linked as the type of the mailbox you want to create from the following options:
   - Regular (Default)
   - Shared
   - Linked

   When creating linked sub-mailboxes, the available shared sub-mailboxes will be restricted to those belonging to its parent's shared mailbox.
7. Click **Next**.
8. In the Linked To page, select the name of the shared mailbox to link to the mailbox. You can type a partial shared mailbox name in the **Filter by Name** field and click the filter button for a filtered list to select from.
9. Click **Next**.

10. In the Assign Groups page, use the arrows to add the groups to the Selected Groups list and click **Next**. All groups in the **Selected Groups** list will have permissions on this mailbox.
11. Click the first double arrow to add all available groups to the **Selected Groups** list. You can type a partial group name in the **Filter by Name** field and click the filter button for a filtered list. No groups are required. Groups can be added from the **Accounts** menu.
12. Use the arrows to add users to the Selected Users list and click **Next**. All users in the **Selected Users** list will have permissions on this mailbox. Click the double arrow to add all available users to the **Selected Users** list. You can type a partial user name in the **Filter by ID** field and click the filter button for a filtered list. No users are required. Users can be added from the **Accounts** menu.
13. In the **Confirm** page, verify your mailbox configuration and click **Finish**.

SFTP with Mailbox Login without Virtual Root Permission Enhancement

Using SFTP with Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself is stored in Sterling Integrator as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named "/" serving as the root.

Mailboxes in Sterling Integrator are analogous to the familiar directory structure offered by operating systems' file systems. A Mailbox is a directory and messages correspond to files in the directory.

Mailboxes are more feature rich than the normal file system. A mailbox can be configured to invoke a business process when a message is sent to it. Messages have well defined extractability policies that govern the conditions under which messages can be successfully extracted (retrieved).

The SFTP Server adapter uses system Mailboxes as the repository. The prerequisites to using SSH/SFTP are:

- One or more Mailboxes set up as the repository for SFTP
- Users with appropriate permissions to SFTP mailboxes
- Users configured with virtual root or with the *MailboxLoginWithoutVirtualRootPermission* permission

Using SCP with Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself is stored in Sterling Integrator as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named "/" serving as the root.

Mailboxes in Sterling Integrator are analogous to the familiar directory structure offered by operating system file systems. A Mailbox is a directory and messages correspond to files in the directory.

Mailboxes are more feature rich than the normal file system. A mailbox can be configured to invoke a business process when a message is sent to it. Messages have well defined extractability policies that govern the conditions under which messages can be successfully extracted (retrieved).

The SFTP Server adapter uses Sterling Integrator Mailboxes as the repository. The prerequisites to using SSH/SCP in Sterling Integrator are:

- One or more Mailboxes set up as the repository for SCP
- Users with appropriate permissions to SCP mailboxes
- Users configured with virtual root or with the *MailboxLoginWithoutVirtualRootPermission* permission

SFTP Mailboxes

The SFTP Server adapter uses Mailboxes as the repository. To use SSH/SFTP:

- Set up one or more Mailboxes as the repository for SFTP
- Assign users appropriate permissions to SFTP mailboxes
- Configure users with virtual root or with the *MailboxLoginWithoutVirtualRootPermission* permission

Chapter 3. Build 5007 or Higher

Standards Enhancement

Applying Sterling Integrator, Release 5.0 Build 5007 automatically includes Sterling Standards Library 6.2. Your specific standards implementation will depend upon the terms of your licensing agreement.

Sterling Standards Library version 6.2 adds support for the following standards and versions:

- All SWIFTNet 2010 message types
- SWIFT Proxy Voting version 1.2

Additionally, the Image Cash Letter Split and Image Cash Letter Join services were added to aid in the processing of X9.37 data.

Applying Sterling Integrator, Release 5.0 Build 5007 allows you to install a new version of the Map Editor. You cannot open a map saved in this new version of the Sterling Integrator, Release 5.0 Build 5007 Map Editor in the older versions of the Sterling Integrator, Release 5.0 Map Editor.

e-Invoicing Enhancement

Applying Sterling Integrator, Release 5.0 Build 5007 includes Sterling e-Invoicing version 1.2, Build 1207 if you have a Sterling e-Invoicing license. Your specific implementation will depend upon the terms of your licensing agreement.

Sterling e-Invoicing version 1.2, Build 1207 adds support for the following:

- Additional legal content not in the human readable detail report
- Free form notes loop at the header and line item details
- Numerical values in the human readable detail report and calculations
- Allowance and charges loops at the header and line item level in the detail report
- Display of the taxable amount by tax rate
- Display of the total VAT tax amount in the currency of the country of supply
- Custom duplicate settings
- Buyer and supplier tax representative information and VAT identifiers

Change Permissions Enhancement

If you have upgraded from a previous version of the system, the existing permissions are set to Other by default. You may need to edit each permission to apply a new permission type.

Before you begin you need to know the following information:

Field	Description
Permission ID	Permission ID for the permission you are creating. Permission ID is the name of the business process, XSLT document, Web template, or resource for which you are setting the permission. Include the extension for the resource after the ID. Required. Permission IDs: • They must be unique. • They are case-sensitive. • The permission ID must match the name of the business process, XSLT document, Web template, or resource. If the permission ID and the name of the resource do not match exactly, you cannot lock down the resource.
Permission Name	Name of the permission you are creating. Required. A permission name does not need to be unique. Permission names are case-sensitive.
Permission Type	Permission type of the permission you are creating. Required. Permission types include: • UI – Allows access to specific menu items in the interface. UI Permissions with a Permission ID prefixed by _DENY_ deny access to that particular resource or action. For example, if you add a permission, _DENY_BPMANAGE to a user or a group, the user or group will not be able to access BP Management UIs. • Mailbox – Allows access to specific mailboxes in the application. • Template – Allows access to specific Web templates. • BP – Allows access to specific business processes. • Tracking – Allows access to specific document tracking options. • Community – Allows access to specific community management options. • Web Service • Service • eInvoicing • Other – Allows access to resources that are not identified by one of the preceding types.

To create a permission:

1. From the **Administration** menu, select **Accounts** > **Permissions**.
2. Next to **Create a new Permission**, click **Go**!
3. In the **Permissions** page, enter the **Permission ID**.
4. Enter the **Permission Name**.

5. Select the **Permission Type**.
6. Click **Next**.
7. Review the permission settings.
8. Click **Finish**.

nCipher and SafeNet/Eracom Support Enhancement

Sterling Integrator supports the following nCipher and Safenet/Eracom devices:

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

Sterling Integrator Features for HSM Support

An entry is stored in the CERTS_AND_PRI_KEY table by Sterling Integrator 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).

OCSP Support Enhancement

Online Certificate Status Protocol (OCSP) Support in Sterling Integrator

The Online Certificate Status Protocol (OCSP) is a set of ASN.1 defined data structures for requesting and receiving information about certificate revocation status. These data structures can be sent and received by many transport protocols in principle. In practice, HTTP is used.

An OCSP client sends questions and processes responses. An OCSP responder answers questions and generates responses.

OCSP Client Functionality

An OCSP client implementation consists of the following:

- Data structures for managing information about OCSP responders
- Functionality for generating OCSP requests
- Functionality for processing OCSP responses
- Functionality for transmitting OCSP requests and receiving OCSP responses

How Sterling Integrator Performs an OCSP Check

About this task

An OCSP check for a certificate in Sterling Integrator is determined when the OCSP check within Sterling Integrator is implemented as a part of internal system APIs used by services for getting certificates and keys from the database. OCSP checks are performed by Sterling Integrator when methods are called to get certificates and keys from the objects that encapsulate them in the database.

The following steps describe how the OSCSP check is implemented in Sterling Integrator:

Procedure

1. The system examines the object that encapsulates the certificate to determine if OCSP checking is enabled. This allows the system to decide with no additional database calls whether to attempt an OCSP check.
2. If OCSP checking is enabled, the system gets the encoded issuer name from a certificate.
3. The system hashes the encoded issuer name with SHA1.
4. The system attempts to find an authority configured in the system that has a name whose hash matches that of the certificate.
5. If no authority is found, no check is performed.
6. If an authority is found, the system checks the OCSP policy for the authority. If the policy permits or requires OCSP checks, see the CERT_AUTHORITY table for more information. The system attempts to find an OCSP responder for the authority.
7. If no OCSP responder is found for the authority, one of the following happens:
   - If the authority policy is set to always check, an exception is thrown and the check fails.
   - If the authority policy is to only check when a responder is configured, no check is performed.
   - If an OCSP responder is found for the authority, an OCSP check is attempted.

Database Tables

Two new database tables have been added to manage OCSP-related information:

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

The CERT_AUTHORITY table maintains information about certificate authorities.

Column	Type	Description
OBJECT_ID	VARCHAR (255)	This is a GUID that constitutes a unique ID for a record. This is the primary key. Cannot be null.
NAME	VARCHAR (255)	A name for a record. Null allowed.
CREATE_DATE	DATETIME	A create date for a record.
MODIFIED_DATE	DATETIME	The date a record was last modified.
MODIFIED_BY	VARCHAR(255)	Information about who modified a record.
ISSUER_NAME	BLOB	The RDN of the authority taken from its certificate.
HASH_ALG	VARCHAR(128)	The hash algorithm used to compute name and key hashes. Only SHA1 is supported.
RDN_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the DER encoded issuer RDN taken from the authority's certificate. This column is indexed.
KEY_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the encoded public key in the issuer's certificate
CERT_OID	VARCHAR(255)	The OBJECT_ID of the authority's certificate in the CA_CERT_INFO table. Each authority must have a CA certificate in the database. Nulls not allowed.

OCSP_POLICY	VARCHAR(128)	The OCSP policy for the authority. This consists of two comma separated values. The values describe when to use OCSP and what to check. Possible values are: **OCSP_When** • never – never use OCSP • resp – use OCSP only if a responder is configured when a request is made • always – always use OCSP when a request is made. This requires a responder to be configured and will cause certificate checking to fail if no responder is configured **OCSP_What** • none – never check any certificates • end-user- Check only end user certificates • both – check both end-user and intermediate certificates. Currently not supported • Null is not allowed in this column
CRL_POLICY	VARCHAR(128)	Currently not used.

OCSP_RESPONDER

The OCSP_RESPONDER table maintains information about OCSP responders.

Column	Type	Description
OBJECT_ID	VARCHAR (255)	This is a GUID that constitutes a unique ID for a record. This is the primary key. Cannot be null.
NAME	VARCHAR (255)	A name for a record. Null allowed.
CREATE_DATE	DATETIME	A create date for a record.
MODIFIED_DATE	DATETIME	The date a record was last modified.
MODIFIED_BY	VARCHAR(255)	Information about who modified a record.
ISSUER_NAME	BLOB	The RDN of the authority taken from its certificate.

HASH_ALG	VARCHAR(128)	The hash algorithm used to compute name and key hashes. Only SHA1 is supported.
RDN_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the DER encoded issuer RDN taken from the authority's certificate. This column is indexed.
KEY_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the encoded public key in the issuer's certificate
CERT_OID	VARCHAR(255)	The OBJECT_ID of the authority's certificate in the CA_CERT_INFO table. Each authority must have a CA certificate in the database. Nulls not allowed.
CACHE_TTL	VARCHAR(64)	The time in seconds to allow OCSP responses to live in the internal response cache If the column is NULL, OCSP responses will only be cached for 1 second, which in practice means not at all.
TRANS_PROF_OID	VARCHAR(255)	OBJECT_ID of a profile in the GIS database. You have to create a profile for the OCSP responder that includes the correct URL for the responder.
COMM_BP	VARCHAR(255)	Name of a business process to use to communicate with the OCSP responder. This has to be a business process that does HTTP communication. Services in the business process have to be configured to not require or present HTTP headers when sending and receiving, respectively. The process HTTPClientSend that comes with the system can be used and is recommended
COMM_WAIT	VARCHAR(24)	The number of seconds to wait for communication with the OCSP responder to take place before inferring that something is wrong.

OCSP Configuration

About this task

When configuring the system, you can create as many authorities and responders as you like.

To configure the system to use OCSP:

Procedure

1. Check the certificate for the certificate authority who issues the certificates you want to check in with OCSP into Sterling Integrator to verify it is a CA certificate.
2. List the CA certificates in the system and get the object ID for the certificate you just installed.
3. If the authority’s OCSP response signing certificate is different than the authority’s certificate issuing certificate, check the authority’s OCSP response signing certificate into Sterling Integrator as a Trusted certificate.
4. If you checked in an additional OCSP signing certificate, list the CA certificates in the system and get the object ID for the certificate you just installed.
5. Go to the bin directory of the Sterling Integrator installation.
6. Start the database if necessary.
7. Start the bash or sh shell.
8. Source the file tmp.sh
9. Create an authority using the utility in the class com.sterlingcommerce.security.ocsp.SCICertAuthority.
10. Create an OCSP responder using the utility in the class com.sterlingcommerce.security.ocsp.SCIOCSPResponder
11. Update the certificates for the authority or individual certificates to enable OCSP. The utility com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo will configure all trusted and system certificates for an authority. The utility com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo will configure 1 system certificate. The utility com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo will configure 1 trusted certificate.

OCSP Configuration Scripts

The following scripts have been included with the OCSP hotfix to run the OCSP configuration utilities. There is a Unix/Linux and Windows version of each script. The scripts take the same command-line arguments as the utility programs they invoke. The scripts are located in the bin directory of the product install. The information about the command-line arguments is essentially just repeated in this section describing the scripts.

ManageCertAuthority.sh and ManageCertAuthority.cmo

Argument	Description

-a, -r, -d	Operation to perform -a add -l list -d delete The –l option takes no additional arguments. The –d option takes a single argument: the object ID of the record to delete
Name	Name of the authority. Required with -a.
Modified_by	User who modified or created the identity. Required with –a.
Hash_alg	Hash algorithm for the authority. Only the value "SHA1" is supported. Required with –a.
Certificate_id	Object ID of the CA certificate associated with the authority. Required with –a.
OCSP_policy	The OCSP policy string for the authority. This is a comma-delimited string as described in the section on the CERT_AUTHORITY table. Required with –a. For the first element of the string, the following are permitted: • never – never use OCSP • resp – use OCSP only if a responder is configured when a request is made • always – always use OCSP when a request is made. This requires a responder to be configured and will cause certificate checking to fail if no responder is configured For the second element of the string, the following are permitted: **OCSP What** • none – never check any certificates • end-user- Check only end user certificates • both – check both end-user and intermediate certificates. Currently not supported. Examples: • never,none • always,end-user
Crl_policy	CRL policy string for the authority. Required with –a. A value is required for this argument, but it is not currently used. "None" is acceptable.
Object_ID	An object ID to use when creating this record. Optional with -a.

ManageOCSPResponder.sh and ManageOCSPResponder.cmd

Argument	Description
-l	Gets a list of the currently configured OCSP Responders. This option takes no additional arguments.
-d	Deletes the configured OCSP Responder with the provided object ID for responders configuration data. This option takes object_id as an additional argument.
-u2	Updates existing records in the database with the correct information about the public key of the authority certificate and the subject DN of the authority certificate. This needs to be run against all existing records for both Cert Authority and OCSP Responders, or you need to delete and recreate the records to get the proper information into the database. This option takes object_id as an additional argument.
-a	Adds configuration data for a new OCSP Responder to be used for checking the status of certificates issued by the provided authority. Additional arguments are name, modified_by, hash_alg, authority_cert_oid, response_signing_cert_oid, resp_signing_cert_in_ca_store, cache_ttl, trans_prof_oid, comm_bp, comm_wait, send_nonce, require_nonce, and object_id.
name	(Required with -a) Name of the authority.
modified_by	(Required with -a) User who modified or created the identity.
hash_alg	(Required with -a) Hash algorithm for the authority. Only the value “SHA1” is supported.
authority_cert_oid	(Required with -a) Object ID of the CA certificate associated with the authority.
response_signing_cert_oid	(Required with -a) Object ID of the certificate that the provider of the OCSP services used to sign the response providing the status for the certificates. This certificate must be added to the CA Digital Certificate store or the Trusted Digital Certificate store. This is the System Certificate ID for the certificate as it appears in the store.

resp_signing_cert_in_ca_store	(Required with -a) Flag indicating if the previous value for the response_signing_cert_oid argument is found in the CA Digital Certificate Store in Sterling B2B Integrator.
cache_ttl	(Required with -a) The time-to-live in seconds for OCSP responses in the internal cache.
trans_prof_oid	(Required with -a) The object ID of a transport configured for communicating with the OCSP responder.
comm_bp	(Required with -a) Name of a business process to use to communicate with the OCSP responder. This has to be a business process that does HTTP communication. Services in the business process have to be configured to not require or present HTTP headers when sending and receiving, respectively. The process HTTPClientSend that comes with the system can be used and is recommended.
comm_wait	(Required with -a) The number of seconds to wait for communication with the responder until inferring that an error has occurred.
send_nonce	(Required with -a) Indicates if a NONCE value will be sent to the OCSP service. The NONCE value is used to prevent replay attacks by some OCSP providers.
require_nonce	(Required with -a) Indicates if the server should require that the OCSP service provide a NONCE value in the response.
object_id	(Optional with -a) An object ID to use when creating this record.

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

This utility will set the OCSP information in the database for a single system certificate

Argument	Description
-o, -n	How to interpret the second argument: -o object_ID -n name
Object_ID/Name	Object ID or name of the authority as determined by argument 1.

SetSystemCertOCSPInfo.sh and SetTrustedCertOCSPInfo.cmd

This utility will set the OCSP information in the database for a single system certificate

Argument	Description

This utility will set the OCSP information in the database for a single system certificate

-o, -n	How to interpret the second argument: -o object_ID -n name
Object_ID/Name	Object ID or name of the authority as determined by argument 1.

Run an OCSP Script

About this task

Use the following example to learn how to run the OCSP configuration scripts. These scripts assume that you have already checked in the CA certificates for the authority, started the database, are in the bin directory of your Sterling Integrator install and have sourced the file tmp.sh in the bin directory.

After getting the object ID of the CA certificate from the authority, in Sterling Integrator from the Administration menu, select Trading Partners > Digital Certificates-CA. Select a certificate. The Certificate Summary dialog box appears with the certificate information, including its object ID.

Complete the following steps to run an OCSP Script:

Procedure

1. Run a command similar to the following to create an authority in the system:

   ```
   ./ManageCertAuthority.sh -a VPCA admin SHA1 "sedna:a1807c:11dc6d53ba4:-7b4b"
   "always,end-user" "none"
   ```

2. After creating an authority, and creating a profile for communicating with an OCSP responder, run a command similar to the following to create an OCSP responder in the system:

   ```
   ./ManageOCSPResponder.sh -a VPCA admin SHA1 "sedna:a1807c:11dc6d53ba4:-7b4b"
    "2400" "a1807c:11dc79aacbd:-7570" HTTPClientSend 3600
   ```

3. Run a command similar to the following to list all of the authorities in the system:

   ```
   ./ManageCertAuthority.sh -l
   ```

   Return output for each authority displays:

   ```
   CERT_AUTHORITY:
   OBJECT_ID: sedna:1ded0fd:11dc9d22929:-7fbd
   NAME: VPCA
   CREATE_DATE: 2008-11-23
   MODIFIED_DATE: 2008-11-23
   MODIFIED_BY: null
   ISSUER_NAME: Country=US, StateOrProvince=Dublin, OrganizationUnit=GIS
    Development, Organization=Sterling,
   CommonName=Test CA
   HASH_ALG: SHA1
   RDN_HASH: 24E63F8AE9F51497529EA0CC34467A4680737A9F
   ENCODED_RDN_HASH: JOY/iun1FJdSnqDMNEZ6RoBzep8=
   KEY_HASH: C96F2FF442EBFA07672DCEC49B729D4D24898313
   ENCODED_KEY_HASH: yW8v9ELr+gdnLc7Em3KdTSSJgxM=
   CERT_OID: sedna:a1807c:11dc6d53ba4:-7b4b
   OCSP_WHEN_POLICY: always
   OCSP_WHAT_POLICY: end-user
   CRL_POLICY: null
   ```

4. Use a command similar to the following to enable OCSP for all trusted and system certificates issued by the authority:

```
./SetAuthorityCertsOCSPInfo.sh -o sedna:1ded0fd:11dc9d22929:-7fbd yes
```

OCSP Check Logic

About this task

The following steps describe the logic of OCSP checking in Sterling Integrator:

If the certificate status is ok, the OCSP check succeeds. Otherwise, it fails.

Procedure

1. If an existing response whose time-to-live has not expired is found, than that response is used as the OCSP response.
2. If no existing response is found in the cache or the time-to-live has expired for a response in the cache, an OCSP request is created.
3. If the system creates an OCSP request, it launches the business process configured for the OCSP responder to send the request and get the response. Requests will include a nonce value if the responder was configured to have one sent.
4. If the business process completes successfully, the system attempts to parse its primary document as an OCSP response. The business process used to send OCSP requests and receive OCSP responses strips the HTTP headers from the response.
5. If the primary document can be parsed as an OCSP response, the system checks the status of the response.
6. If the response status indicates that the request generated a valid response, the system attempts to verify the signature on the OCSP response using the certificate configured for the OCSP responder.
7. If the signature is verified and the responder was configured to require nonce, the system attempts to get and check the nonce from the response.
8. If all other verifications passed, then the system looks for certificate status information for the certificate for which the request was constructed and sent.
9. If the status information is found, then the system updates the internal cache for an existing OCSP response for the certificate.

Producer/Consumer Relationship Report Enhancement

The producer/consumer relationship reports are used to view the mailbox producer and consumer relationships. This report provides information on the:

- Producer Partner Name
- Producer Mailbox
- Consumer Mailbox
- Policy Settings
- Routing Rules

The following table lists the available producer/consumer relationship reports:

Report Name	Description
ConsumerProducerRelationships	Organized by consumer name. All other available criteria is reported according to the defaults.
ProducerConsumerRelationships	Organized by producer name. All other available criteria is reported according to the defaults.

To Run This Report

Use **Operations** > **Reports** to run this report.

Chapter 4. Build 5006 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 Sterling Integrator is down. For continued processing in the background, the Data Sweeper service is 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 Sterling Integrator instance is running. These sweepers are designated with an OFFLINE mode. Sweepers that safely complete their work in a running Sterling Integrator instance are designated to run in all modes. Sweepers that should only be run upon the recommendation of Sterling Integrator 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 Sterling Integrator version. This allows for new versions of Data Sweeper (which can have new updates) to be used on an older Sterling Integrator 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 Sterling Integrator InstallService. DataSweeper is installed when you install Sterling Integrator. The schedule service will be inactive out of the box.

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.

The scheduled Sterling Integrator service can be turned on to run the Data Sweeper (for example, every Monday morning at 1 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"
autoCorrect	Opposite of reportOnly. Required 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

Command Line option	Description	Default values	Notes
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	
sweeperTimeout Threshold=[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

Command Line option	**Description**	**Mode**
synchronizeWorkflowIds	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
reindexTenYear BusinessProcesses (disabled out of box)	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
reindexMailbox DocumentClonesSweeper	Verifies specific information about documents and flags them back to zero life spans.	ALL
resetRemoved MailboxDocuments	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
missingArchive InfoSweeper	Creates ARCHIVE_INFO rows for records not found in parent tables.	OFFLINE
missingDocument LifespansSweeper	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 (disabled out of box)	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 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 Sterling Integrator; so they may be helpful for troubleshooting.

Health Checks:

Command Line option	Description
bpUsageHealthCheck	Provides high level usage about business processes currently on system.
currentDBUsersHealthCheck	Displays information about current connections to Sterling Integrator Database.
objectSizeHealthCheck	Displays size, rows and analyzes database information.
dbConfigHealthCheck	Displays Sterling Integrator specific database configuration information.

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 Sterling Integrator 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.

Chapter 5. Build 5004 or Higher

Add Resources Without Restart Enhancement

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

When Sterling Integrator 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. Sterling Integrator 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. If the business process runs successfully the following will appear in the Process Data:

```
<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
```

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

JDBC Pools Enhancement

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

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

Adding JDBC Pools

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 Sterling Integrator. 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 Sterling Integrator when to start using that credential for new connections. This applies primarily to external pools, although Sterling Integrator 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: Note: Other formats may be used as long as they follow the Internet Engineering Task Force (IETF) standard date syntax.

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

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 Enhancement

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. You can generate a patch report on UNIX and Windows operating systems. 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.

Optimizing and Controlling the System Threads Enhancement

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
Jetty	ActiveMQ Session Task	11
	SessionScavenger	47
	ConduitStreamListener	16
	SocketListener	10
JGroup	Various Jgroup Handlers	22
JetSpeed	RunnableThread	10
Perimeter PS Dispatcher	Various Adapters	13

Thread created by	Thread name	Count
Business process queues	ReschedulingThread	10
B2B	B2B http Servlet Thread FIFOTaskListener QueueThread:queue	3 10 11
System	RMI Timer	7 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.

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**

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.

Queue Watcher Enhancement

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 the user has all the necessary permissions or is a part of the Sterling Integrator 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: 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.
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

Heading	Description
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 Disabled Adapters	Shows a list of adapters that are currently marked as disabled (not running).

Heading	Description
View DB Pool Information View Cluster Multicast Data Config Queue	Shows usage information for the configured DB pools. Shows load data broadcast from the nodes when running in a cluster. 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**.
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.

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.

Large File Import Enhancement

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.

Note: A back up file may not be created if the file name of the document contains an underscore (_) character, for example, file_name. If the file name has an underscore character, it is recommended to manually back up the file before importing.

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.

Large File Import Performance Enhancement

The following performance improvements have been made for importing large files:

- -numberofThreads parameter, for import.sh or import.cmd, allows you to specify the number of threads that are simultaneously used during the import. This option only applies to users, groups, permissions, maps, and document envelopes. If you do not specify this option, the import will be processed in a single thread.
- -noLocks parameter, for import.sh or import.cmd, allows you to import resources without checking for or creating locks. This option should be used during a maintenance window or when you know that no other users are importing.

New Parameter for Import Tool

The following new parameter has been added to the import tool (import.sh or import.cmd):

- -perfReport allows you to store the detailed performance report in a file. If this parameter is not specified, then only summary data is provided in the system.log file.

Example: -numberofThreads Parameter

The following is an example of setting the -numberofThreads.

You have a file called newresouces.xml to import and it contains the following resources:

- 150 Users
- 100 Maps
- 15 Business Processes

You set the number of threads to 10 by using the following command:

```
import.sh -numberofThreads 10 -input newresource.xml
```

Since you specified 10 threads, 15 users are imported across each of the 10 threads, and 10 maps across each of the 10 threads. As for Business Processes, they are just imported one at a time, as they are not one of the resources supported for the multi-threaded import.

Performance Report

The New Performance Report identifies how long it took to import resources. The summary performance report includes resource type, number of resources, and time in seconds and is available from the user interface and from the command line option. You can also generate a more detailed version of the report from the command line. Two versions of the performance report are provided:

- **Summary Performance Report** - The performance report summary is available through the user interface and is also saved in a log file.
- **Detailed Performance Report** - The detailed report can be saved in a file using the -perfReport parameter (import.sh). The default time is seconds. If the time to import is less than one second, then the time is zero in the report. You can change the default time format from seconds to milliseconds in the customer override property file (tp_import_export.properties file) by updating the import.perfReport.timeformat=milliseconds parameter.

The Summary Performance Report includes:

- Resource types
- Number of entries
- Time to import in seconds

The following is an example of a Summary Performance Report:

Resource Type	**#Entries**	**Time (seconds)**
Users	1	0
Groups	1	0
Permissions	3	0
Total Import Time		0

The Detailed Performance Report includes:

- Listing of resource types, number of resources, and resource names
- Import order generated from configured dependencies
- Estimate of how many passes are required
- Progress as each resource type is processed

The following is an example of a Detailed Performance Report:

```
Started Import at Tue Aug 04 14:34:20 EDT 2009
Identified the following resources for import:
USERS[1]: [mbx_ie_user1]
GROUPS[1]: [mbx_ie_group1]
PERMISSIONS[3]: [/aftcons_pgp_enc/mbx_ie_mailbox1.mbx, mbx_ie_perm1, mbx_ie_perm3]
The resources will be imported in the following order:[PERMISSIONS, GROUPS, USERS]
The import will be completed in 3 passes as follows:
Pass 1: [PERMISSIONS]
Pass 2: [GROUPS]
Pass 3: [USERS]
Starting Pass 1 at Tue Aug 04 14:34:20 EDT 2009: Import of 3 PERMISSIONS
Importing 3 PERMISSIONS
Finished importing 3 PERMISSIONS in 2 seconds
Starting Pass 2 at Tue Aug 04 14:34:22 EDT 2009: 1 GROUPS
Importing 1 GROUPS
Finished importing 1 GROUPS in 0 seconds
Starting Pass 3 at Tue Aug 04 14:34:23 EDT 2009: 1 USERS
Importing 1 USERS
Finished importing 1 USERS in 1 seconds
Finished import at: Tue Aug 04 14:34:25 EDT 2009
Total Time for Import: 5 seconds
```

Resource Type	#Entries	Time (milliseconds)
Permissions Groups Users	3 1 1	2355 ms 956 ms 1408 ms
Total Import Time		5050 ms

Mailbox Limited Access Enhancement

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.
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 Server Manager Enhancement

The PGP Server Manager enables you to add, edit, and delete PGP servers. A PGP profile is a record stored in Application that contains information about the PGP server. The PGP Server Manager works with the PGP Package service and PGP Unpackage service.

Note: The PGP Profile Manager in versions Gentran Integration Suite 4.3 and earlier is renamed to PGP Server Manager in Sterling Integrator 5.0.

How Application Works with a PGP Server

Application 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 Application, where it can be sent out to trading partners.

Creating a PGP Server Profile

1. From the **Administration** menu, select **Trading Partner** > **PGP** > **PGP Server Manager**.
2. Click **Go!** next to Create a new PGP Server Profile.
3. Enter the field values as described in the following table:

Field	Description
Name	Name of this profile.
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 • PGP Command Line (version 9.8) - PGP Corporation 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`

Field	Description
Secret Key Map Information	For signing purposes, you must add at least one secret key map. • To add a secret key map, click **Add**. Enter the Key Name, Key ID, and passphrase for the key map in the Key Map Info page and click **Save**. • To edit a secret key map, click **Edit**. Update the information as necessary in the Key Map Info page and click **Save**. • To delete a secret key map, click **Delete**. Verify that this is the key map to be deleted in the Key Map Info page 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**. Enter the Key Name and Passphrase for the key map in the Key Map Info page and click **Save**. • To edit a conventional key map, click **Edit**. Update the information as necessary in the Key Map Info page and click **Save**. • To delete a conventional key map, click **Delete**. Verify that this is the key map to be deleted in the Key Map Info page and click **Delete**.

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

Editing a PGP Server Profile

1. From the **Administration** menu, select **Trading Partner** > **PGP** > **PGP Server Manager**.
2. Click **Go!** next to List Alphabetically.
3. Click **edit** next to the profile you want to edit.
4. Revise the fields displayed as necessary and click **Save** when finished.

Deleting a PGP Server Profile

1. From the **Administration** menu, select **Trading Partner** > **PGP** > **PGP Server Manager**.
2. Click **Go!** next to List Alphabetically.
3. Click **delete** next to the profile you want to delete.

Secure Socket Layering (SSL) Enhancement

HTTPS Configuration for the GPM

Secure HTTP access via SSL is already supported for most web applications in Sterling Integrator 5.0 on the base HTTP port + 1. This SSL enhancement:

- Enables HTTPS (HTTP w/ SSL encryption) for the Graphical Process Modeler (GPM)

- Enables disabling and redirection of web applications on the base HTTP port to another port (using HTTPS)
- Supports secure access to web applications by deploying the web applications on a secure HTTP Server Adapter instance
- Reduces security risks

You must apply patch 5004 or higher before you can enable this feature. If you use this feature, you will need to configure the Graphical Process Modeler (GPM) to communicate with the dashboard web application using HTTPS instead of HTTP. Access to web applications deployed via a secure HTTP Server Adapter may be slower than when accessed on the base port.

New SSL Parameters

Several new parameters have been added for the enhanced SSL feature. You will need to configure these parameters to facilitate SSL communication between the Graphical Process Modeler (GPM) and the server. These new parameters must be defined in their respective property files.

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. Properties defined in the sandbox.cfg file must not be defined in customer_overrides.properties, as they will be ignored in customer_overrides.properties. These properties are the only ones which are not defined in customer_overrides.properties.

The following table describes the new SSL parameters and provides the name of the property file where the parameter can be found.

Parameter Name	Definition	Property file
WEBAPP_LIST_PORT	Identifies the port the GPM client should use for communication with the server. It defaults to the base port during the installation. If the Dashboard and GPM web applications have been deployed to a secure HTTP Server Adapter instance, this parameter should be modified to match the port of the secure HTTP Server Adapter instance. If the base SSL port (base HTTP port +1) is being used for secure deployment of GPM and Dashboard, this parameter should be modified to match the base SSL port (SSL_PORT in sandbox.cfg).	sandbox.cfg file
WEBAPP_PROTOCOL	Identifies the protocol to use for communication with the Dashboard web application (http/https).	sandbox.cfg file

Parameter Name	Definition	Property 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 Dashboard and GPM web applications are successfully deployed on a secure HTTP Server Adapter, this parameter may be set to =admin,dashboard,gpm to remove access to those web applications on the base port. The complete list of web applications includes: • communitymanagement • myaft • portlets The value ALL may be used as a wildcard to indicate that all wars deployed on the base HTTP port should be skipped. This may not be necessary if the base port is blocked to external access. The value ALL must not be used with any other value.	customer_overrides.properties
HTTPS_REDIRECT_WARS	Indicates the wars that will be automatically redirected from the base HTTP port to either the secure HTTP Server Adapter or base SSL port. The value ALL may be used to redirect all skipped wars on the base HTTP port to the HTTPS_LIST_PORT (the secure HTTP Server Adapter or base SSL port). The value ALL must not be used with any other value.	customer_overrides.properties
HTTPS_LIST_PORT	Indicates the redirected destination port for requests made against the base HTTP port. Should be set to the value of the secure HTTP Server Adapter or base SSL port.	customer_overrides.properties

Parameter Name	Definition	Property file
HTTPS_CLIENT_CERTS	A comma-separated list of system certificates whose public keys need to be added to the default trust store. These certificates are used for client-side verification during the SSL handshake when HTTPS calls are initiated from the application server-independent (ASI) server back to itself. This parameter requires server certificate keys that have a **SubjectAltName**. If you use existing keys without this parameter, this functionality will fail with very obscure messages. **Note:** The certificate configured for HTTPS on baseport+1 (sslCert) is automatically added to the trust store and does not need to be added to this list.	customer_overrides.properties

When configuring this feature, if you only define SKIP_BASEPORT_DEPLOYMENT_WARS, but not HTTPS_REDIRECT_WARS and HTTPS_LIST_PORT, the web applications are inaccessible on the base port and the user is not automatically redirected to the HTTPS port. This is a valid scenario, if the user prefers not to redirect automatically for security reasons. The web applications will still be available when accessed on the secure HTTP Server Adapter or base SSL port.

Enable Auto-Redirect to HTTPS

About this task

Support was added to allow for an automatic redirect to HTTPS to be configured for the web applications that are deployed on a secure port (Http Server Adapter or base SSL port) 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:

Procedure

1. Navigate to `/<install_dir>/install/properties`.
2. Open the customer_overrides.properties file and set the following parameter values as shown:

```
HTTPS_REDIRECT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_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 close the file.

Example Implementation

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,dashboard,gpm,communitymanagement,myaft,portlets
## 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 or base_ssl_port>
```

Note: If using a secure HTTP Server Adapter instance, the configuration mandates that all wars specified as HTTPS_REDIRECT_WARS must be deployed on the same HTTP Server Adapter instance.

Trusted Certificate List

If a Secure HTTP Server Adapter instance is used, the SSL certifcate used for configuring the Secure HTTP Server Adapter instance must be added to the trusted certificate list. This is needed because some of the Dashboard screens make https calls back to the ASI server. For these calls to complete the SSL handshake successfully, the certificates must be configured in the trust store on the ASI server. This is done by specifying the certificate name in the HTTPS_CLIENT_CERTS list.

These system certificates must have the DNS names and the IP address(es) specified as alternate names when the system cert is created. The default SSL host name verification supplied by the JDK requires that the name of the certificate presented by the SSL server match the host name used in the http url, or one of the strings in the "SubjectAltName" attribute in the certificate. Some screens on the dashboard will not work without the "SubjectAltName" configuration.

Alternate names are configured through the "List of IP addresses Separated by Comma" and "List of DNS Names Separated by Comma" fields in the System Certificate creation wizard (Trading Partner -> Digital Certificates -> System).

HTTPS Support for the GPM

Java Web Start (JavaWS) is used to launch the Graphical Process Modeler (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 or reject it. SSL certificates cannot be automatically verified by JavaWS and must be verified by users.

Java Version 1.5 Impact on GPM with SSL

In Java Version 1.5, which is the current version used by JavaWS to launch the Graphical Process Modeler (GPM), the default hostname verification does not resolve IP addresses to the Domain Name System (DNS) names. As a result, when you access the GPM on a secure HTTPS Server Adapter, you may see the following warning prompt "`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 Dashboard application, you are assured that the IP address displayed is that of the server on which the Dashboard was deployed. It is safe to run the application despite the warning prompt. This issue with Hostname Verification was fixed in Java Version 1.6.

If you are using an early version of Java 1.5, multiple prompts may appear simultaneously when launching the GPM. These multiple prompts are modal and often prevent the user from choosing any dialog options. This leaves the GPM process in an unresponsive state, and it must be manually stopped. To prevent this, it is recommended that you upgrade the Java version to at least 1.5.0_11.

Import Certificates for Java Web Start

About this task

If you want to avoid an untrusted certificate prompt during Java Web Start (JavaWS) operation, you can import the certificates into the local machine store prior to launching Graphical Process Modeler (GPM). This can reduce user confusion in the event that the SSL certificate associated with the secure HTTP Server Adapter or base SSL port is not trusted by the user's local machine.

To import trusted root certificates into JavaWS:

Procedure

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

Switch from HTTP to HTTPS: Base SSL Port

About this task

To switch from HTTP to HTTPS using the base SSL port:

Procedure

1. Navigate to `/install_dir/install/properties`.
2. Open the sandbox.cfg file.
3. Modify the following parameters:

   ```
   WEBAPP_PROTOCOL=https
   WEBAPP_LIST_PORT=<base_port + 1>
   ```

   These parameters are used by the Graphical Process Modeler (GPM) for communication with the server.
4. (Optional, Recommended) If you want to turn off access to the dashboard and GPM web applications on the base port, and configure auto-redirect to the HTTPS port, specify the following parameters in a customer_overrides.properties file:

```
SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
HTTPS_REDIRECT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<base_port + 1>
```

For example:

```
## 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,dashboard,gpm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<base_port + 1>
```

5. Save and close the file.
6. Navigate to `/install_dir/install/bin`.
7. Stop Sterling Integrator.
8. Apply the configuration changes. Enter `./setupfiles.sh`.
9. Deploy the new configuration. Enter `./deployer.sh`.
10. Start Sterling Integrator.
11. (Optional) If you turned off access to the Dashboard and GPM web applications on the base port (Step 4), verify the changes your made. For example, you can verify:
    - Dashboard web application access on http://host:baseport/dashboard is inaccessible or redirected to https://host:<base_port + 1>/dashboard automatically.
    - GPM web application access on http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp is inaccessible or redirected to https://host:<base_port + 1>/gpm/pmodeler/ProcessModeler.jnlp automatically.

Switch from HTTP to HTTPS: Secure HTTP Server Adapter

About this task

To switch from HTTP to HTTPS mode:

Procedure

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 required WAR files to the HTTP Server Adapter instance with SSL enabled.

   Note: All WAR files must be picked up from the `/install_dir/install/noapp/deploy` directory when configuring the HTTP Server Adapter instance. Additionally, the context name of the admin web application must match the ADMIN_CONTEXT_PATH parameter in `/install_dir/install/properties/sandbox.cfg` file. For all the other web applications, the context name should be the name of the war file without the ".war" extension

   This is necessary so that any changes made via a patch or hotfix are automatically reflected in the HTTP Server Adapter deployment.

   The required WAR files include:
   - admin.war

- communitymanagement.war
- dashboard.war
- gbm.war
- myaft.war
- portlets.war

Additional WAR files may be required to support new functionality added by you to your Dashboard.

3. Verify the context name of the admin.war web application matches the ADMIN_CONTEXT_PATH parameter in the `/install_dir/install/properties/sandbox.cfg` file.
4. Verify the Dashboard web application is accessible via the HTTP Server Adapter by accessing https://host:<*secure_http_server_adapter_port*>/dashboard.
5. Verify the GPM web application is accessible via the secure HTTP Server Adapter by accessing https://host:<*secure_http_server_adapter_port*>/gpm/pmodeler/ProcessModeler.jnlp.
6. Navigate to `/install_dir/install/properties`.
7. Open the sandbox.cfg file.
8. Modify the following parameters:

```
WEBAPP_PROTOCOL=https
WEBAPP_LIST_PORT=<secure_http_server_adapter_port>
```

   These parameters are used by the GPM for communication with the server.
9. (Optional, Recommended) If you want to turn off the deployment of the Dashboard and GPM web applications on the base port, specify the following parameters in a customer_overrides.properties file:

```
SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
HTTPS_REDIRECT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

   For example:

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

10. (Optional) If you want to send cookies from the browser using a secure protocol like HTTPS, specify the following parameter in a customer_overrides.properties file:

```
## sending cookies as secure over https
http.useSecureCookie=true
```

11. Save and close the file.
12. Navigate to `/install_dir/install/bin`.
13. Stop Sterling Integrator.
14. Apply the configuration changes. Enter `./setupfiles.sh`.
15. Deploy the new configuration. Enter `./deployer.sh`.
16. Start Sterling Integrator.

17. If you turned off the deployment of the Dashboard and GPM web applications on the base port (Step 9), verify the following:
    - Dashboard web application access on http://host:baseport/dashboard is redirected to https://host:<*secure_http_server_adapter_port*>/dashboard automatically.
    - GPM web application access on http://host:baseport/gpm/pmodeler/ProcessModeler.jnlp is redirected to https://host:<*secure_http_server_adapter_port*>/gpm/pmodeler/ProcessModeler.jnlp automatically.

Switch from HTTPS to HTTP Mode

About this task

To switch from HTTPS to HTTP mode:

Procedure

1. Navigate to `/install_dir/install/properties`.
2. Open the **sandbox.cfg** file.
3. Modify the following parameters:
   ```
   WEBAPP_PROTOCOL=http
   WEBAPP_LIST_PORT=<base_port>
   ```
4. Save and close the file.
5. (Optional) If the deployment of the Dashboard and GPM web applications on the base port was turned off when switching to the HTTPS mode, you must open the customer_overrides.properties file and comment out the following parameters so that they are not applied:
   ```
   ## SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
   ## HTTPS_REDIRECT_WARS=admin,dashboard,gpm,communitymanagement,myaft,portlets
   ## HTTPS_LIST_PORT=<http_server_adapter_port>
   ```
6. (Optional) Save and close the file.
7. Navigate to `/install_dir/install/bin`.
8. Stop Sterling Integrator.
9. Apply the configuration changes. Enter `./setupfiles.sh`.
10. Deploy the new configuration. Enter `./deployer.sh`.
11. Start Sterling Integrator.
12. Verify the following:
    - Dashboard web application is accessible on http://host:baseport/dashboard
    - GPM web application is accessible on http://host:baseport/gpm/pmodeler/ProcessModeler.jnlp
13. (Optional) Undeploy the web applications from the SSL enabled HTTP server adapter instance.

Chapter 6. Build 5001 or Higher

Custom Password Policy Enhancement

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: 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.

FIFO Enhancement

FIFO Message Processing

Sterling Integrator supports ordered processing of files and messages for the following adapters:

- JMS Queue adapter
- JMS Topic adapter
- MSMQ adapter

The ordered processing in Sterling Integrator is processed by the FIFO (first in first out) framework.

The following figure demonstrates the FIFO framework:

Sterling Integrator 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 Sterling Integrator.
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 Sterling Integrator.
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 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` 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 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.
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.

FifoInitialization BPReport

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.
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 Sterling Integrator 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 Sterling Integrator database for storage and configure its port usage. By default,

ActiveMQ will be configured to listen at the Sterling Integrator base port + 65 and the ActiveMQ interface will be at base port + 66 (http://server:base port + 66/admin).

4. On each Sterling Integrator 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.
6. Restart Sterling Integrator.

ActiveMQ Data Storage

JDBC (Database) Master Slave is the default configuration for data storage employed to store FIFO data for ActiveMQ. In this configuration, each ActiveMQ node in a cluster is configured to utilize a single, shared database.

By default, this option is configured to make use of the existing Sterling Integrator database. As a result, this configuration option is setup out of the box and provides the simplest storage solution. For more information on ActiveMQ JDBC Master Slave configuration, see http://activemq.apache.org/jdbc-master-slave.html.

Shared File System Master Slave is an alternative data storage mechanism supported for FIFO, where a shared file system is used to store FIFO data for ActiveMQ. The shared file system option may yield better performance than when using JDBC. For more information on ActiveMQ file system based storage, see http://activemq.apache.org/shared-file-system-master-slave.html.

Configure Shared File System Master Slave for ActiveMQ

You must manually configure the Shared File System Master Slave if you are not using the JDBC (Database) Master Slave configuration option to store FIFO data for ActiveMQ.

Note: Configuring FIFO messaging in a cluster for ActiveMQ is a prerequisite to configure the Shared File System Master Slave for ActiveMQ. For information on configuring FIFO messaging in a cluster, see *Cluster Configuration*.

To configure shared file system master slave for ActiveMQ:

1. In the activemq.xml file, comment out the following section:

   XML comments consist of the symbols, '<!--' to open the comment and '-->' to close the comment.

   ```
   <!-- Database Storage Option -->

   <!-- This section has been commented.

   <persistenceAdapter>
         <jdbcPersistenceAdapter dataSource="#fifo-ds" useDatabaseLock="true">
           <statements>
             <statements tablePrefix="FIFO_"/>
           </statements>
   ```

```
      </jdbcPersistenceAdapter>
</persistenceAdapter>

-->
```

2. Uncomment the following section by removing the symbols '<!--' and '-->'.

```
<!-- File system Storage Option -->

 <persistenceAdapter>
    <journaledJDBC dataDirectory="/sharedFileSystem/broker"/>
</persistenceAdapter>
```

3. Edit the dataDirectory parameter to point to the location of the shared data directory to be used. This data directory must point to the same physical data location for all ActiveMQ instances in the network. For information on warnings about shared file system choices as a result of locking limitations, see *Shared File System Assumptions and Limitations*.
4. Restart each ActiveMQ node when you reconfigure it.

Shared File System Assumptions and Limitations

The following are some of the assumptions and limitations you must be aware of when using the Shared File System option to store FIFO data for ActiveMQ.

- Encrypted passwords for database storage are not currently supported. The file system based storage option described in this topic provides an alternative that does not require you to expose the database passwords.
- If an ActiveMQ node loses its connection to its database or file system storage, ActiveMQ will shut down. This is the intended behavior. Sterling Integrator currently does not employ out of the box monitoring for the ActiveMQ instances utilized for FIFO. To ensure seamless FIFO processing, the ActiveMQ nodes must be monitored and restarted if the instances are shut down for any reason.
- When ActiveMQ loses its database connection in conjunction with a Microsoft SQLServer database, ActiveMQ may hang during the shut down process. As a result, it may be difficult to determine if the ActiveMQ node has failed and requires to be restarted. It is recommended that you use the shared file system storage when using ActiveMQ in combination with a SQL Server database to avoid processing interruptions in failure scenarios.
- If you are reconfiguring any ActiveMQ options, ensure that you have executed all FIFO business processes. Failure to execute all FIFO business processes may result in the existing FIFO business processes remaining in an ‘Active’ state, in turn resulting in loss of FIFO ordering for the processes in the ‘Active’ state. To continue successful processing, the business processes in the ‘Active’ state will have to be manually halted and restarted.

Notices

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

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

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

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

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

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

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

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

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

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

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

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

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

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

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

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

Trademarks

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

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

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

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

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

Product Number:

Printed in USA