Sterling File Gateway

Build 4319 Updates

Version 1.1 Build 4319

Contents

What's New in Build 4319

Enhancements in This Release

The following enhancements are included in this release:

- The File Gateway Arrived File Service has been modified.
- The File Gateway Route Service has been added.

Both of these services are system services and require no action by users.

Known Issues

Consumer messages are no longer routed after patching Sterling File Gateway to Build 4319 or greater. The FileGatewayMailboxRouteArrivedFile business process is not successfully routing Producer messages to the Consumer. The problem started after patching Sterling File Gateway to a patch level 4319 or higher.

There are no error messages, but routes are not being routed.

Resolution

This is happening because Build 4319 installs a new version of the FileGatewayMailboxRouteArrivedFile business process. The new version calls the File Gateway Route Service to route the Producer message to the Consumer. If the default version of the FileGatewayMailboxRouteArrivedFile business process was modified previously, this modified version will not be overridden by the new version from the patch. Therefore, the wrong version of the FileGatewayMailboxRouteArrivedFile business process is the default and it will not run the File Gateway Route Service.

You must manually update the FileGatewayMailboxRouteArrivedFile business process default version to the new version created by the patch. You can then manually reapply your modifications if they still apply and update the business process. Once the new version of the FileGatewayMailboxRouteArrivedFile business process is selected as the default, Sterling File Gateway messages will be routed to the Consumer.

Sterling File Gateway Services

File Gateway Arrived File Service

The File Gateway Arrived File Service verifies and processes files that arrive into Sterling File Gateway. It also determines if the files need to be routed and/or deleted.

The following table provides an overview of the File Gateway Arrived File Service:

System Name	File Gateway Arrived File Service
Graphical Process Modeler (GPM) category	Not applicable
Description	This service verifies and processes files that arrive into Sterling File Gateway. It also determines if the files need to be routed and/or deleted.
Business usage	This is a system service. It is used to verify and process a file that has arrived into the File Gateway system.
Usage example	The system uses this service.
Preconfigured?	Yes
Requires third party files?	None
Platform availability	All platforms supported by the application
Related services	None
Application requirements	None
Initiates business processes?	Yes. This service may start sub-business processes.
Invocation	Yes. This service is invoked automatically in Sterling File Gateway processes and should not be modified.
Business process context considerations	None
Returned status values	0 = Success 1 = Failure
Restrictions	This service is only called by Sterling File Gateway and cannot be customized.
Persistence level	System default

Testing considerations	None

Implementing the File Gateway Arrived File Service

This is a system service. You do not need to implement this service.

Configuring the File Gateway Arrived File Service

There are no configuration parameters for the File Gateway Arrived File Service.

Parameters Passed from Business Process to Service

Field	Description
ReplayArrivedFileKey	The key that represents the original arrived file if this is a replay. Optional.
ReplayComment	The comment entered by the user on the replay. Optional.
MessageId	The message identifier that this service will route through Sterling File Gateway. Required.

Parameters Passed from Service to Business Process

Field	Description
ArrivedFileKey	The key that represents the Arrived File.
ShouldDeleteMessage	Whether or not the message should be deleted by the workflow.
ShouldRouteMessage	Whether or not the arrived file should be routed by the workflow.

Example Business Process

The following is an example of BPML that uses the File Gateway Arrived File Service:

```
<process name="Fire ACME Event">
    <sequence name="Event">
        <operation>
            <participant name=" FileGatewayArrivedFileService "/>
            <output message="Output">
               <assign to="ReplayArrivedFileKey">1234</assign>
               <assign to="ReplayComment">Replaying due to failure.</assign>
               <assign to="MessageId">1</assign>
           </output>
           <input message="Input">
               <assign to="." from="*"></assign>
           </input>
       </operation>
    </sequence>
</process>
```

File Gateway Route Service

The File Gateway Route Service processes and transforms files in order to prepare them for delivery to a consumer partner.

The following table provides an overview of the File Gateway Route Service:

System Name	File Gateway Route Service
Graphical Process Modeler (GPM) category	Not applicable
Description	This service processes and transforms files in order to prepare them for delivery to a consumer partner.
Business usage	This is a system service. It is used to transform a file that has arrived into the File Gateway system
Usage example	The system uses this service.
Preconfigured?	Yes
Requires third party files?	None
Platform availability	All platforms supported by the application
Related services	None
Application requirements	None
Initiates business processes?	Yes. This service may start sub-business processes for custom consumer identification and/or transformation.
Invocation	Yes. This service is invoked automatically in Sterling File Gateway processes and should not be modified.
Business process context considerations	None
Returned status values	0 = Success 1 = Failure
Restrictions	This service is only called by Sterling File Gateway and cannot be customized.
Persistence level	System default
Testing considerations	None

Implementing the File Gateway Route Service

This is a system service. You do not need to implement this service.

Configuring the File Gateway Route Service

There are no configuration parameters for the File Gateway Route Service.

Parameters Passed from Business Process to Service

Field	Description
ArrivedFileKey	The key that represents the arrived file created by the Arrived File Service. Required.

Parameters Passed from Service to Business Process

Field	Description
RouteDeliveries	A list of all the deliveries that the router will attempt to send to the File Gateway Delivery Service. Optional, used only when there are deliveries to make.
Delivery	Contains all the elements required by the File Gateway Delivery Service required to make a delivery. Optional, used only when there are deliveries to make.
DeliveryKey	The key that represents the Delivery. Required, one for each delivery.
DeliveryChannelKey	The key that represents the Delivery Channel that the FileGatewayDeliveryService will use to make the delivery. Required, one for each Delivery.
ConsumerFile	Contains all the elements that represent the file to be delivered. Required, one for each delivery.
DocumentId	The identifier of the document to be delivered. Required, one for each consumer file.
ContentType	The content type of the file to be delivered. Required, one for each consumer file.
FileName	The file name of the file to be delivered. Required, one for each consumer file.
Type	The type of the layer that is being delivered. Required, one for each consumer file.
MailboxPath	The mailbox path to deliver to. Required, one for each consumer file.
CreateMailboxIfMissing	Whether or not to create the mailbox if it is missing in the delivery. Required attribute on MailboxPath. Valid values are: • Y - Create a mailbox if one matching the specified pattern does not already exist • N - Do not create a mailbox

Example Business Process

The following is an example of BPML that uses the File Gateway Route Service:

```
<process name="Fire ACME Event">
    <sequence name="Event">
        <operation>
            <participant name=" FileGatewayRouteService "/>
            <output message="Output">
                    <assign to="ArrivedFileKey"
                     from=”ArrivedFileServiceResults/ArrivedFileKey/text()” />
           </output>
           <input message="Input">
                <assign to="." from="*"></assign>
           </input>
       </operation>
    </sequence>
</process>
```

Authentication Outside Sterling File Gateway

About Authenticating Users Outside Sterling File Gateway

There are two supported methods of authenticating users outside Sterling File Gateway and Gentran Integration Suite

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

Implementing Single Sign-On in Sterling File Gateway

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

To enable SSO:

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

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

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

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

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

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

   ```
   authentication_policy.SSO_AUTHENTICATION_ENABLED=true
   ```

   Note: Do not edit the authentication_policy.properties file. Make all changes in the customer_overrides.properties file.

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

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

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

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

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

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

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

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

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

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

To configure Sterling File Gateway for LDAP:

1. Create external users in Gentran Integration Suite.
2. For each external user created in Gentran Integration Suite, create a matching record in an LDAP Directory.
3. Create or modify the customer_overrides.properties file to modify the authentication_policy.properties. as in the following example:

   ```
   authentication_policy.LDAP_AUTHENTICATION_ENABLED=true
    ##########################################################
   # LDAP Server <1> Authentication Configuration
   ##########################################################
   ```

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

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

Note: Do not edit the authentication_policy.properties file. Make all changes in the customer_overrides.properties file.

---

4. If you previously set up LDAP in Gentran Integration Suite by editing your security.properties file, comment out LDAP settings as follows:

```
#LDAP_AUTHENTICATION_ENABLED=true
#LDAP_JNDI_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#LDAP_HOST=ldap://ldapserver1.local:9999
#LDAP_SECURITY_TYPE=simple
#LDAP_PRINCIPLE=cn=Manager,dc=amr,dc=stercomm,dc=com
#LDAP_CREDENTIALS=SterlingCustomer
#LDAP_USER_PASSWORD_ATTRIBUTE=userPassword
#LDAP_SEARCH_ROOT=dc=amr,dc=stercomm,dc=com
#LDAP_SEARCH_FILTER_PATTERN=(uid=<userid>)
#LDAP_AUTHENTICATE_WITH_USER_BIND=false
```

```
##LDAP_SECURITY_PROTOCOL=ssl
#LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/server2/com/sterlingcommerce/
server2/security/units/cacerts
#LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
#LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/server2/com/sterlingcommerce/
server2/security/units/keystore
#LDAP_SECURITY_KEYSTORE_PASSWORD=password
```

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

5. Restart the server for your changes to in the customer_overrides.properties file to take effect over the authentication_policy.properties file.

How Gentran Integration Suite and Sterling File Gateway Work Together

Sterling File Gateway utilizes the Sterling B2B foundation, which includes Gentran Integration Suite, Sterling Standards, and the Sterling platform, to deliver capabilities similar to those found in Sterling Advanced File Transfer and Connect:Enterprise for UNIX, while adding new features and functionality.

Within Sterling File Gateway, Gentran Integration Suite is known as the B2B Console, and is accessed from the Tools menu. Administrative functions such as creating and managing user accounts, permission groups, and security keys for Sterling File Gateway are handled in Gentran Integration Suite.

Sterling File Gateway utilizes the communication adapters of Gentran Integration Suite, which include the following:

- FTP Server adapter
- FTP Client adapter
- SFTP Server adapter
- SFTP Client adapter
- HTTP Server adapter
- HTTP Client adapter
- Connect:Direct Server adapter
- Command Line adapter 2 (for PGP)

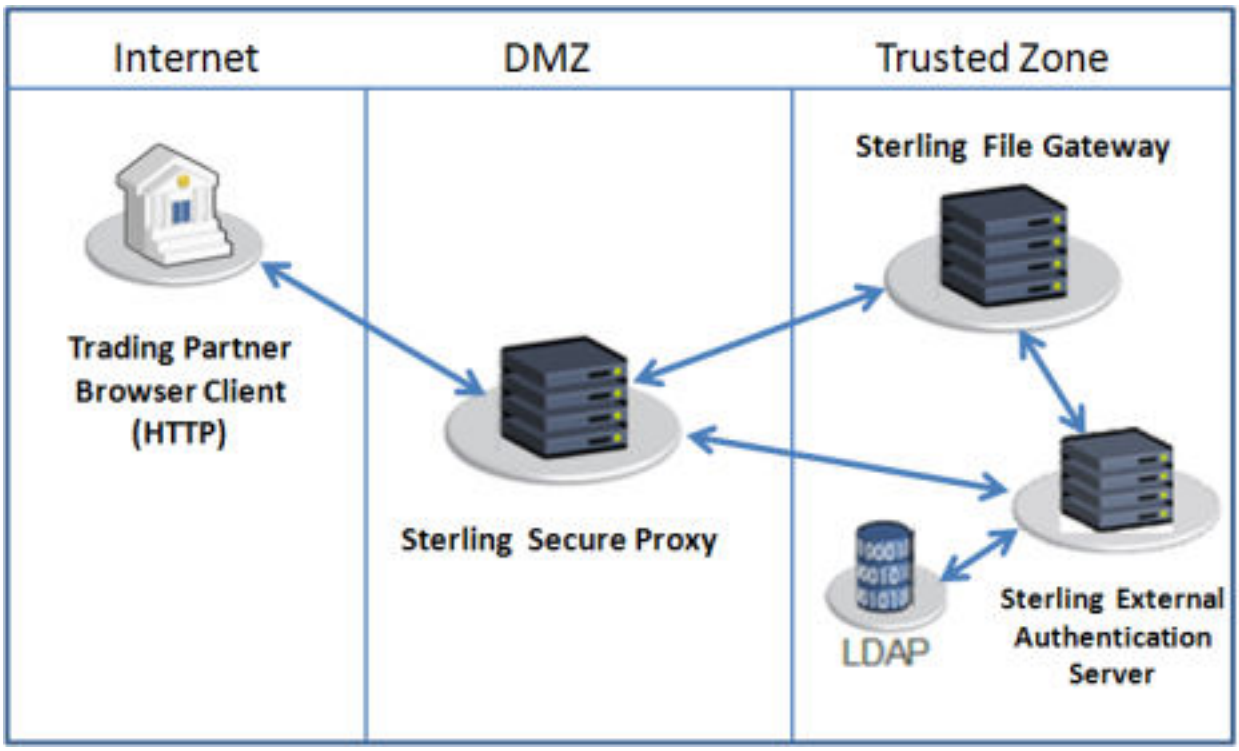
To install Sterling File Gateway, you must first install Gentran Integration Suite. After you install Sterling File Gateway on an instance of Gentran Integration Suite, when you install upgrades or new builds of Gentran Integration Suite, Sterling File Gateway upgrades and builds are automatically installed as part of the installation script.

How Sterling Secure Proxy and Sterling File Gateway Work Together

Sterling Secure Proxy can be used as a proxy with Sterling File Gateway and other HTTP applications and supports a single sign-on connection. Single sign-on (SSO) provides access control that allows a user to log in once to Sterling Secure Proxy, using the HTTP protocol, and then gain access to Sterling File Gateway without logging in again. SSO bypasses normal user authentication in Sterling File Gateway and trusts that Sterling Secure Proxy has authenticated the user.

After you set up the basic single sign-on configuration, trading partners can communicate in a secure environment that provides authentication. The trading partner first connects to Sterling Secure Proxy which then connects to Sterling File Gateway on behalf of the trading partner.

Following is an illustration of the flow of data:



For more information, see the *Sterling Secure Proxy* documentation at *http://www.ibm.com/support/docview.wss?uid=swg27023891*.

Configure a Load Balancer

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

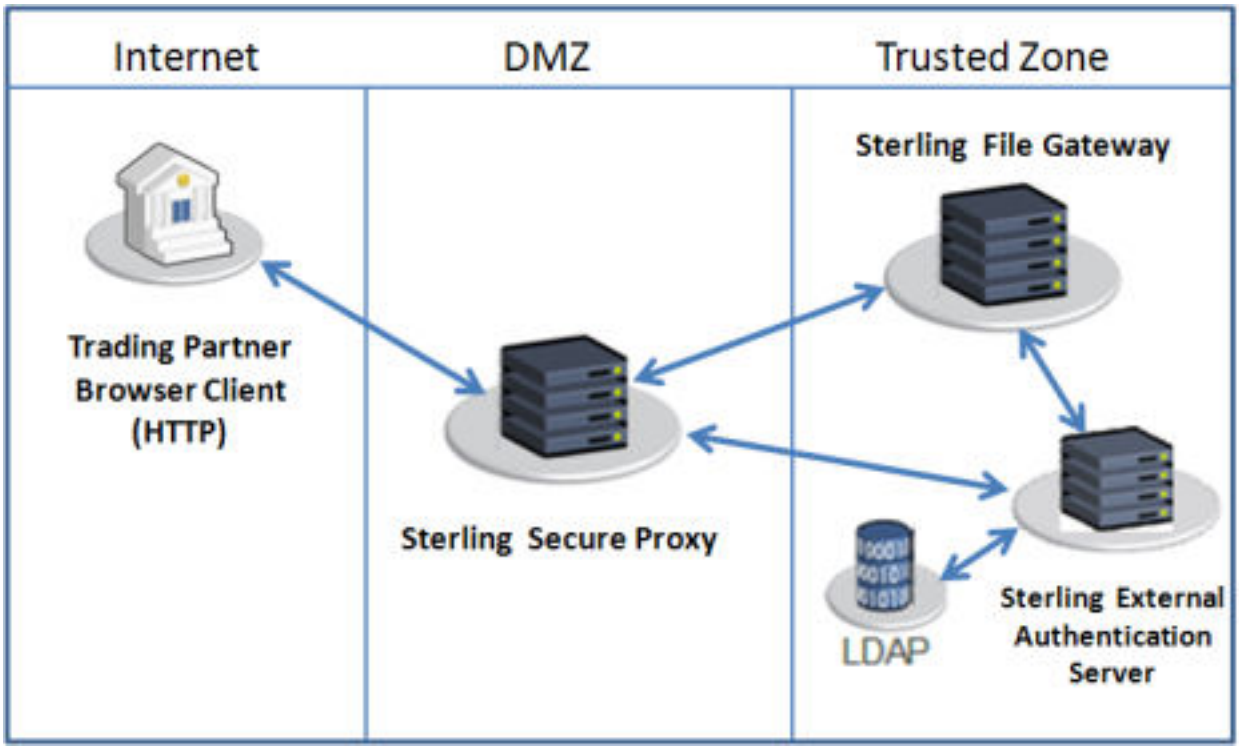
If you are using a load balancer to run multiple Sterling Secure Proxy engines, avoid login credential errors or session timeout conditions by configuring the load balancer to use "sticky sessions" (also known as persistence, server affinity, or "sticky cookies"). Refer to your load balancer documentation for details about configuring persistence.

Configure Sterling Secure Proxy

Sterling Secure Proxy can be used as a proxy with Sterling File Gateway and other HTTP applications and supports a single sign-on connection. Single sign-on (SSO) provides access control that allows a user to log in once to Sterling Secure Proxy, using the HTTP protocol, and then gain access to Sterling File Gateway without logging in again. SSO bypasses normal user authentication in Sterling File Gateway and trusts that Sterling Secure Proxy has authenticated the user.

After you set up the basic single sign-on configuration, trading partners can communicate in a secure environment that provides authentication. The trading partner first connects to Sterling Secure Proxy which then connects to Sterling File Gateway on behalf of the trading partner.

Following is an illustration of the flow of data:



If you are using a load balancer to run multiple Sterling Secure Proxy engines, avoid login credential errors or session timeout conditions by configuring the load balancer to use "sticky sessions" (also known as persistence, server affinity, or "sticky cookies"). Refer to your load balancer documentation for details about configuring persistence.

For more information, see the *Sterling Secure Proxy* documentation at *http://www.ibm.com/support/docview.wss?uid=swg27023891*.