

Sterling Integrator



# Services and Adapters Build Updates

*Version 5.1*



Sterling Integrator



# Services and Adapters Build Updates

*Version 5.1*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 93.

**Copyright**

This edition applies to Version 5 Release 1 of Sterling Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2000, 2015.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Introduction to Build Updates . . . . .</b>	<b>1</b>
Build 5104 or higher . . . . .	1
Command Line Adapter 2 (Build 5104 or higher) . . . . .	1
PGP Package Service (Build 5104 or higher) . . . . .	19
PGP Unpackage Service (Build 5104 or higher) . . . . .	32
Build 5102 or Higher . . . . .	41
EDI Encoder Service . . . . .	41
FTP Server Adapter. . . . .	46
Image Cash Letter Join Service . . . . .	57

Image Cash Letter Split Service. . . . .	60
SFTP Client GET Service . . . . .	61
SFTP Client PUT Service . . . . .	65
Build 5101 or Higher . . . . .	69
FTP Server Adapter. . . . .	69
SFTP Server Adapter . . . . .	80

<b>Notices . . . . .</b>	<b>93</b>
--------------------------	-----------



---

# Introduction to Build Updates

This document provides information about fixes and enhancements provided in Sterling Integrator Version 5.1. These builds are cumulative and include all fixes and enhancements contained in the previous build.

---

## Build 5104 or higher

### Command Line Adapter 2 (Build 5104 or higher)

The Command Line Adapter 2 (CLA2) enables Sterling Integrator® to run a program from a command line in a business process. Programs that can be run include executable programs, scripts, or operating system (OS) commands external to Sterling Integrator. The Command Line Adapter 2 also supports large files up to 12 GB and provides better memory allocation than the Command Line adapter. The Command Line Adapter 2 replaced the Command Line adapter.

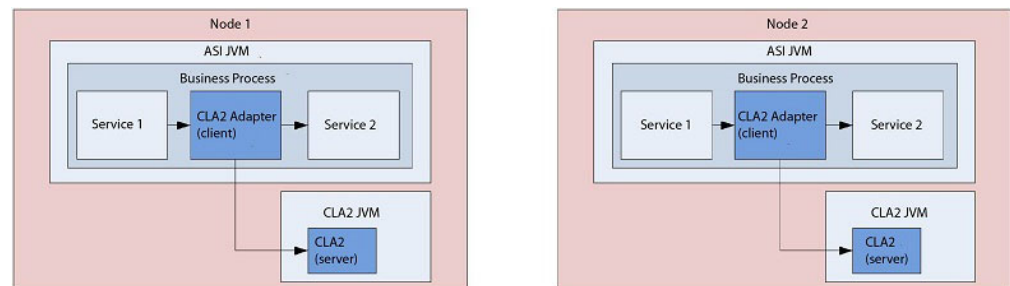
By default the Command Line Adapter 2 is disabled. Before a business process can use the Command Line Adapter 2, you must enable the adapter. For more information about enabling the adapter, see *Enabling the Command Line Adapter 2*.

The Command Line Adapter 2 supports both key based authentication and data security with SSL. For more information about how to configure these new parameters in the adapter, see *Configuring the Command Line Adapter 2*.

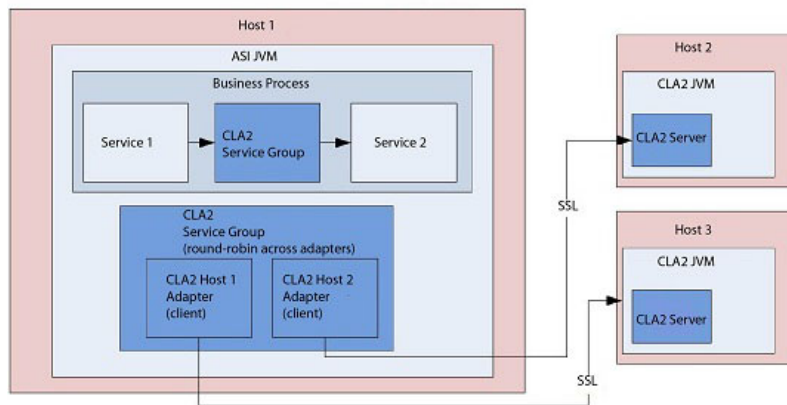
Any existing custom Command Line Adapter 2 service instances must be reconfigured to verify that authentication is enabled and the correct key (cla2auth) is selected. To verify that authentication is enabled, you can review the audit log file that contains the timestamp, the source host IP, the business process, and the full command line.

Deployment of the Command Line Adapter 2 can be done both locally and remotely. In CLA2 deployment, a CLA2 server runs on each node and only the local CLA2 client can call the CLA2 server. Business processes must be on each node that is running a CLA2 server or you can create a service group of CLA2 adapters to allow the client service to call the appropriate CLA2 server on the localhost.

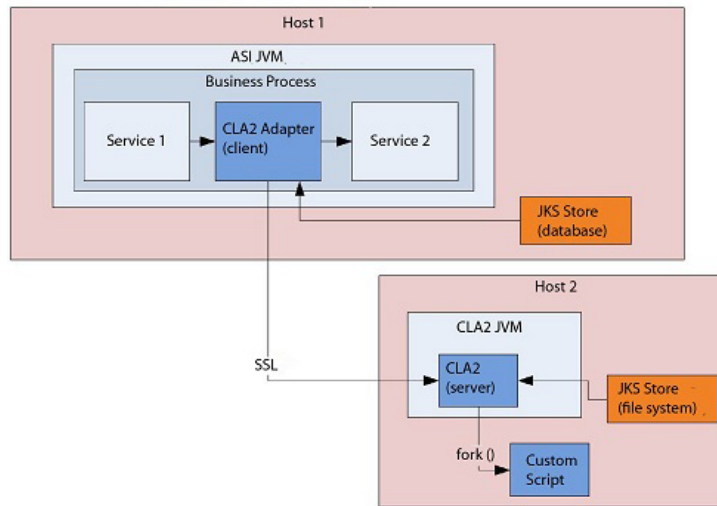
This diagram illustrates the process flow between the CLA2 adapter client and the CLA2 adapter server on the same host:



This diagram illustrates the process flow between the CLA2 adapter client and the CLA2 adapter server on different hosts with multiple CLA2 servers:



This diagram illustrates the process flow between the CLA2 adapter client and the CLA2 adapter server on different hosts that are secured with SSL:



**Remember:** Before you can use the Command Line Adapter 2 in a business process, you must enable the local Command Line Adapter server. For more information about how to enable the server, see *Enabling the Command Line Adapter 2*.

The following table provides a high-level overview of the Command Line Adapter 2:

System name	CmdLine2
GPM category	All Services
Description	Executes a program from the command line. The syntax is: cmd.exe /C <command>. This is not necessary when running scripts. Examples:cmd.exe /C dir importBPs.sh
Business usage	Used to call any program from the command line.



Usage example	<p>You could use the Command Line Adapter 2 to invoke a program that:</p> <ul style="list-style-type: none"> <li>• Encrypts and decrypts data you want to send or receive securely over the Internet</li> <li>• Manipulates data, such as change every occurrence of one letter to another</li> <li>• Pages someone</li> <li>• Initiates a business process</li> <li>• Initiates a remote system</li> </ul> <p>These are just a few examples out of many possible uses.</p>
Preconfigured?	No
Requires third party files?	No
Platform availability	All supported Sterling Integrator platforms
Related services	Command Line Adapter
Application requirements	None
Initiates business processes?	Yes, if you define a business process to start when you configure the Command Line Adapter 2. The business process starts after the output from the command line process is read.
Invocation	<p>Once you enable the Command Line Adapter 2, there are no special requirements. The Command Line Adapter 2 can either be used to start (“bootstrap”) a business process or you can include the Command Line Adapter 2 directly in a business process to perform an explicit command.</p> <p><b>Note:</b> The term “bootstrap” is used in the GPM to indicate that the Command Line Adapter 2 is used to start a business process after the output from the command line process is read.</p>
Business process context considerations	None
Returned status values	<p>Returned status values:</p> <ul style="list-style-type: none"> <li>• Success: Command Line Adapter 2 was successful.</li> <li>• Error: Command Line Adapter 2 was unsuccessful.</li> </ul>
Restrictions	<p>A configuration of this adapter is needed for each program invoked from the command line.</p> <p>Authentication is enabled by default in Sterling Integrator delivered Command Line Adapter 2 instances. Custom Command Line Adapter 2 instances need to be configured manually to ensure authentication is enabled and the cla2auth certificate is selected.</p>
Persistence level	System default (Full Persistence)
Testing considerations	Call a small command line process (without using it to invoke a business process) to perform a simple command.

## How the Command Line Adapter 2 Works

Use the Command Line Adapter 2 in a business process to run any program from the command line, including executable programs, scripts, or OS commands external to Sterling Integrator. The types of activities that can be performed include

data encryption and decryption, file manipulation, data manipulation, and initiation of a process on a remote system.

You can create multiple Command Line Adapter 2 configurations, one for each of several specific commands. Alternatively, you can use a single Command Line Adapter 2 configuration to perform different commands by specifying the command line process (cmdLine) and working directory (workingDir) in the business process. See *Command Line* for details on these parameters.

For example, your company communicates with a legacy database that is important to its daily business. You want to retrieve some customer billing information in the database and send it within a business process in Sterling Integrator to your accounting department. You can write your own executable program to communicate with your legacy system and run it using the Command Line Adapter 2.

The following steps summarize how the Command Line Adapter 2 is typically used in a business process:

1. The adapter writes the content of the current primary document to a file in the working directory specified as the value of the working directory parameter. The name of this file is specified by the value of the inputFile parameter.
2. Sterling Integrator runs an executable program that picks up the file and sends it to the legacy system.
3. The legacy system returns a file, which now includes the customer billing information, and the adapter retrieves it. The file returned is specified by the value of the outputName parameter.
4. The adapter reads the file contents into the primary document.
5. Sterling Integrator performs the next operation in the business process.

## Implementing the Command Line Adapter 2

You can implement a Command Line Adapter 2 to do the following:

- Execute commands using the command line from within a business process.
- Invoke the Command Line Adapter 2 on a schedule and then start a new business process using the output from the adapter.

**Note:** This could be used if you wanted to schedule a command line program that accessed a legacy database on a regular schedule and then used the output in a business process.

The information in this section applies to both of the above implementations.

## Before You Begin

Before you begin to implement the Command Line Adapter 2:

1. Enable the Command Line Adapter 2. For information, see *Enabling the Command Line Adapter 2*.
2. Create and test the command line program or command to make sure that it works.
3. Determine the working directory where you will be processing your commands.

## Process Overview

To implement the Command Line Adapter 2:

1. Create a Command Line Adapter 2 configuration. For information, see *Managing Services and Adapters*.

**Note:** If you are configuring a Command Line Adapter 2 to start a business process, create the business process before you configure the adapter.

2. Configure the Command Line Adapter 2. For information, see *Configuring the Command Line Adapter 2*.
3. Create and enable a business process that includes the Command Line Adapter 2.
4. Test the business process and the adapter.
5. Run the business process.

## Configuring the Command Line Adapter 2

To create a Command Line Adapter 2 configuration, you must specify field settings in Sterling Integrator and in the GPM. For general information about service and adapter configurations, see *Managing Services and Adapters*.

### The Application Configuration

The following table describes the fields used to configure the Command Line Adapter 2 in Sterling Integrator.


**Note:** The field names in parentheses represent the corresponding field names in the GPM. This information is provided for your reference. Some fields can be configured in the GPM, if not selected here. Regardless of where they are configured, they can be overridden using BPML.

Field	Description
Name	Unique and meaningful name for the adapter configuration. Required.
Description	Meaningful description for the adapter configuration, for reference purposes. Required.
Select a Group	Select a Service Group to associate with this adapter. Valid values: <ul style="list-style-type: none"><li>• None – You do not want to include this configuration in a group at this time. Default.</li><li>• Create New Group – You can enter a name for a new group in this field, which is then created along with this configuration.</li><li>• Select Group – If you have already created one or more groups for this service type, they are displayed in the list. Select a group from the list.</li></ul> <p><b>Note:</b> A Service Group is a group of services or adapters of the same type that can act as peers. A Service Group name is used in BPML in place of the Service Configuration name. Service Groups show up in the GPM as if they were Service Configurations. For more information about Service Groups, see <i>Managing Services and Adapters</i>.</p>

Field	Description
Remote Name (remoteName)	Remote host name or IP address where the remote adapter implementation is running. Required. <b>Note:</b> For backward compatibility, the CLA2 supports the Command Line adapter parameter rmiAddr (at the business process level only).
Remote Port (remotePort)	Remote port is determined by the port configuration of the Command Line Adapter 2 server. Required.  Default value: basePort+52.
Access Authentication?	Turn on authentication for this instance?  Valid values: <ul style="list-style-type: none"> <li>• Yes (true) – Default</li> <li>• No (false)</li> </ul> <p>The security default is 30 seconds (3000 milliseconds) and can be adjusted in the <code>CmdLine2server.properties</code> file.</p> <p><b>Restriction:</b> The Command Line Adapter 2 server cannot have more than one private certificate in the JKS repository. For more information, see <i>Maintaining authentication and SSL keys</i>.</p>
System Authentication Certificate	Select the authentication certificate that you want to run. Default value: cla2auth.

Field	Description
Command Line (cmdLine)	<p>Command line process you want to run. Do one of the following:</p> <ul style="list-style-type: none"> <li>• If you want to set this parameter in the GPM/business process, leave the field blank.</li> <li>• Type the command line process in this field exactly as you would from the command line.</li> <li>• If you want to use a command that redirects input or output (through the use of &gt;, &lt;, or  ), you must do so using a script file.</li> <li>• If you do not know the input or output file name, type the following parameters in the command line process as placeholders: <ul style="list-style-type: none"> <li>• \$Input</li> <li>• \$Output</li> </ul> <p>These parameters are typed directly in the command line process. You can use these parameters on the command line in any order and multiple times if necessary. At run time, they are replaced with the actual file name.</p> </li> <li>• If you want to enter user parameters, use the following placeholders: \$0 – \$9. These placeholders are resolved by the parm0 – parm9 parameters defined in the GPM or using BPML.</li> </ul> <p><b>Note:</b> If \$Input or \$Output resolves to a filename that contains one or more spaces, automatic quoting will be performed before the command line is executed. For example, If the original command line was <code>test.sh \$Input</code>, and \$Input resolves to file 1, then the final command line, before execution, will be <code>test.sh "file 1"</code>. Therefore, do not put quotes around \$Input or \$Output.</p> <p><b>Note:</b> An example of a command line entry is <code>test.sh \$Input \$Output \$0 \$1 \$2 \$3 \$4 \$5 \$6 \$7 \$8 \$9</code>. This runs the shell script <code>test.sh</code> taking an input file, using ten parameters, and producing an output file.</p>
Working Directory (workingDir)	<p>Location of the directory to use for executing the command line process. Optional. Default is the current working directory of the JVM running CLA2Client.jar.</p> <p><b>CAUTION:</b>  <b>Using this adapter to call a Unix script modifies the directory path of the environment variable LD_LIBRARY_PATH. To keep your current path, your script should include either the LD_LIBRARY_PATH path or a reference to your .profile (which includes the LD_LIBRARY_PATH path).</b></p>

Field	Description
Turn on debugging messages? (cla2_debug)	<p>Turn on debugging for this adapter instance? Valid values:</p> <ul style="list-style-type: none"> <li>• Yes (true) – Logging is turned on and the messages are written to the system log.</li> <li>• No (false) – Default.</li> </ul> <p><b>Note:</b> This turns on debugging for this specific adapter instance. These messages are logged in the system log in the <i>install_dir</i> logs directory. This parameter is read-only in the GPM.</p> <p><b>Note:</b> For backward compatibility, the CLA2 supports the Command Line adapter parameter <i>cmdl_debug</i> (at the business process level only).</p>
Wait on the process to complete before continuing? (waitOnProcess)	<p>Wait on the process to complete before continuing the business process. Valid values:</p> <ul style="list-style-type: none"> <li>• Yes (true) – If the value is Yes, a status report is created if any stdout/stderr is generated by the process. If an error occurs while the service is processing output data, the advanced status contains the error message instead of the return code value.</li> <li>• No (false)</li> </ul> <p><b>Note:</b> If <b>Use the output generated by the command line process</b> is set to Yes, the value of this parameter is assumed to be Yes because the service cannot use output if it does not wait for the process to complete. This parameter is read-only in the GPM.</p>
Does this service start a business process? (bootstrap)	<p>Whether the service starts a business process. Required. Valid values:</p> <ul style="list-style-type: none"> <li>• Yes (true)</li> <li>• No (false)</li> </ul> <p><b>Note:</b> This parameter is read-only in the GPM.</p>
Business process (initialWorkflowName)	<p>Business process you want the Command Line Adapter 2 to start. This field is required only if you selected Yes in <i>Does this service start a business process?</i> . If you prefer to configure this parameter in the GPM, select Not Applicable.</p> <p><b>Note:</b> For backward compatibility, the CLA2 supports the Command Line adapter parameter <i>initialWorkflowId</i> (at the business process level only).</p>
Create Unique working directory	<p>Command Line Adapter 2 creates a unique working directory for each invocation of a business process using the same Command Line Adapter 2 instance. Selecting this option ensures that the adapter instances do not overwrite each other when multiple files with the same name exist.</p>
Document Storage Type (docStorageType)	<p>Defines how the document is stored in the system. Required when the adapter starts a business process. Valid values:</p> <ul style="list-style-type: none"> <li>• System Default – Default</li> <li>• Database</li> <li>• File System</li> </ul> <p><b>Note:</b> For more information on document storage types, see <i>Managing Services and Adapters</i>.</p>

Field	Description
Run as User	<p>Applies to the scheduling of the business process. The Run As User field only displays as an option if <b>Does this service start a business process?</b> is set to Yes. Type the user ID to associate with the schedule, or click the  icon and select a user ID from the list. Valid value is any valid Sterling Integrator user ID.</p> <p><b>Note:</b> This parameter allows someone who doesn't have rights to a specific business process to run it. If you select <b>Admin</b> as the user ID, you will inherit Administrative rights (for this run of the business process only), and enable the scheduled run.</p>
Use 24 Hour Clock Display	<p>If selected, the adapter will use the 24-hour clock instead of the default 12-hour clock.</p>
Schedule	<p>Information about scheduling the business process invoked by the Command Line Adapter 2. The Schedule field only displays as an option if <i>Does this service start a business process?</i> is set to Yes. Valid values:</p> <ul style="list-style-type: none"> <li>• Do not use schedule If this field is selected, the adapter does not start a business process and does not run on a schedule.</li> <li>• Run based on timer Valid values are the hour and minutes at which to run the adapter. If you choose to select a time interval, the valid values are the hours and minutes for the intervals. Add or delete selections as necessary. Specify any schedule exclusions or date exclusions. Indicate whether you want the adapter to run at startup.</li> <li>• Run daily Valid values are the hour and minutes at which to run the adapter, daily. If you choose to select a time interval, the valid values are the hour and minute for the interval. Add or delete selections as necessary. Specify any date exclusions. Indicate whether you want the adapter to run at startup.</li> <li>• Run based on day(s) of the week Valid values are the day of the week, the hour, and the minute that specify when to run the adapter. If you choose to select a time interval, the valid values are the hours and minutes for the intervals. Add or delete selections as necessary. Specify any date exclusions.</li> <li>• Run based on day(s) of the month Valid values are the day of the month, hour, and minute that specify when to run the adapter. If you choose to select a time interval, the valid values are the hours and minutes for the intervals. Add or delete selections as necessary. Specify any date exclusions.</li> </ul>
Does the command line process require an input file? (useInput)	<p>Defines whether the command line process requires an input file? Required. Valid values:</p> <ul style="list-style-type: none"> <li>• Yes (true) – The primary document of the current business process context is written out to the file system in the working directory and is used as input to the process. Default.</li> <li>• No (false) – No file is written to disk even if a document exists in the business process context.</li> </ul> <p><b>Note:</b> This parameter is read-only in the GPM.</p>

Field	Description
Input File Name (inputName)	<p>Input file name, if the command line process requires an input file. Any occurrences of \$Input in the command line are replaced with this name. Optional. If you leave this field blank, the default is the primary document name.</p> <p><b>Note:</b> It is important to have a unique input file name for all concurrently running instances of Command Line adapters. If more than one instance of the Command Line Adapter 2 can be executing at the same time, you must create a dynamic, unique name to keep the instances from overwriting each other and causing the process to fail. This can be done by concatenating the current process ID on to a file's base name. This dynamic name may also need to be passed to the cmdLine.</p>
Delete input file after process completes? (inputDelete)	<p>Defines whether the input file is deleted after the process completes? Valid values:</p> <ul style="list-style-type: none"> <li>• Yes (true) – Default</li> <li>• No (false)</li> </ul> <p><b>Note:</b> To delete the input file, <b>Wait on the process to complete before continuing?</b> must also be Yes. This parameter is read-only in the GPM.</p>
Use the output generated by the command line process? (useOutput)	<p>Use output generated by the command line process? Required. Valid values:</p> <ul style="list-style-type: none"> <li>• Yes (true) – The adapter will attempt to read the output of the process. If bootstrapping a workflow, the file will become the primary document in the new workflow. If not bootstrapping, the file is collected and placed in ProcessData, not as the Primary Document. Default . For example,</li> </ul> <pre data-bbox="824 1142 1403 1220">&lt;assign name="Assign" to="PrimaryDocument" from="CLA2/document/@SCIOBJECTID"&gt;&lt;/assign&gt;</pre> <ul style="list-style-type: none"> <li>• No (false) – No file is read into the business process context even if one is generated by the command line process.</li> </ul> <p><b>Note:</b> This parameter is read-only in the GPM.</p>
Output File Name (outputName)	<p>Output file name, if you want to use the output generated by the command line process. Any occurrences of \$Output in the command line are replaced with this name. Optional. If you leave this field blank, the default is the business process primary document name.</p> <p><b>Note:</b> It is important to have a unique output file name for all concurrently running instances of command line adapters. If more than one instance of the Command Line Adapter 2 can be executing at the same time, you must create a dynamic unique name to keep the instances from overwriting each other and causing the process to fail. This can be done by concatenating the current process ID on to a file's base name. This dynamic name may also need to be passed to the cmdLine.</p>



Field	Description
Delete output file after process completes? (outputDelete)	Specifies whether the output file is deleted after it is collected? Valid values: <ul style="list-style-type: none"> <li>• Yes (true) – Default</li> <li>• No (false)</li> </ul> <b>Note:</b> This parameter is read-only in the GPM.
Use SSL (Note: User Authentication without SSL will result in a weak security configuration.)	Use SSL to secure the Command Line Adapter 2?  Valid values: <ul style="list-style-type: none"> <li>• Yes (true)</li> <li>• No (false) – Default</li> </ul> <b>Restriction:</b> The Command Line Adapter 2 server cannot have more than one private certificate in the JKS repository. For more information, see <i>Maintaining authentication and SSL keys</i> .
SSL Public CA Certificate	Select the SSL Public CA certificate for validation.

## GPM Configuration

The following screen shows a graphical view of some GPM parameters for the Command Line adapter. The dimmed values were specified using the Command Line adapter configuration. The active fields are env0 and env1, which cannot be configured in the service configuration.

**Example\_CommandLineAdapter2.bp**



**Service Editor-Command Line 2 Adapter**

**Name** Command Line 2 Adapter

**Config.** Sample\_CommandLine2\_Adapter

**Message To Service** **Message From Service**

**Output Msg** Messages Only

**Message Name** CmdLine2InputMessage

Name	Value	Use XPATH?
bootstrap	Yes	<input type="checkbox"/>
cla2_debug	No	<input type="checkbox"/>
cmdLine	/home/test.sh \$Input \$Output \$0 \$1 \$2	<input type="checkbox"/>
docStorageType	System Default	<input type="checkbox"/>
env0	VAR1=TEST	<input type="checkbox"/>
env1	USER=ME	<input type="checkbox"/>
env2		<input type="checkbox"/>
env3		<input type="checkbox"/>
env4		<input type="checkbox"/>
env5		<input type="checkbox"/>
env6		<input type="checkbox"/>
env7		<input type="checkbox"/>

The following example shows the corresponding business process solution using BPML.

```

<process name="Example_CommandLine2BP">
  <operation name="Command Line 2 Adapter Run Script">
    <participant name="Sample_CommandLine2_Adapter"/>
    <output message="CmdLine2InputMessage">
      <assign to="." from="*" />
      <assign to="parm0">VAR1</assign>
      <assign to="parm1">USER</assign>
      <assign to="parm2">10</assign>
      <assign to="env0">VAR1=TEST</assign>
      <assign to="env1">USER=ME</assign>
    </output>
    <input message="inmsg">
      <assign to="." from="*"></assign>
    </input>
  </operation>
</process>
  
```

The following table describes the fields used to configure the Command Line adapter in the GPM. This table contains the fields that are only configured in the GPM. Other fields may also be configured if they were left blank in the Sterling Integrator configuration.

Field	Description
Config (participant name)	Name of the adapter configuration. Required.
env0	An environment variable in the form name=value. Optional. Any value is valid.
env1	An environment variable in the form name=value. Optional. Any value is valid.
env2	An environment variable in the form name=value. Optional. Any value is valid.
env3	An environment variable in the form name=value. Optional. Any value is valid.
env4	An environment variable in the form name=value. Optional. Any value is valid.
env5	An environment variable in the form name=value. Optional. Any value is valid.
env6	An environment variable in the form name=value. Optional. Any value is valid.
env7	An environment variable in the form name=value. Optional. Any value is valid.
env8	An environment variable in the form name=value. Optional. Any value is valid.
env9	An environment variable in the form name=value. Optional. Any value is valid.
keepPath	Normally, any path information is stripped off the filename to allow for platform independence. This parameter allows you to keep the entire path. Optional. Valid values: <ul style="list-style-type: none"> <li>• Yes – Path information is retained</li> <li>• No – Path information is stripped off</li> </ul>
parm0	Resolves the \$0 placeholder. Optional. Any value is valid.
parm1	Resolves the \$1 placeholder. Optional. Any value is valid.
parm2	Resolves the \$2 placeholder. Optional. Any value is valid.
parm3	Resolves the \$3 placeholder. Optional. Any value is valid.
parm4	Resolves the \$4 placeholder. Optional. Any value is valid.
parm5	Resolves the \$5 placeholder. Optional. Any value is valid.
parm6	Resolves the \$6 placeholder. Optional. Any value is valid.
parm7	Resolves the \$7 placeholder. Optional. Any value is valid.
parm8	Resolves the \$8 placeholder. Optional. Any value is valid.
parm9	Resolves the \$9 placeholder. Optional. Any value is valid.

Field	Description
setSoTimeout	Specifies, in milliseconds, how long the socket will wait in receive mode without receiving anything before timing out. This is necessary to ensure that a process doesn't "hang" indefinitely. Optional. Valid value: any integer. Default is 60000 milliseconds (60 seconds). If your command line process is going to take longer than the default 60 seconds to process completely, then increase this value accordingly.
successValue	<p>If waitOnProcess is Yes (true), then this option can be used to determine what the successful return code value is. Optional. Valid value is any integer. The default is 0 . If a value is specified and does not equal the return code value of the process, the business process status is set to ERROR.</p> <p><b>Note:</b> The successValue parameter is an important parameter that is often overlooked. It is used to signal Sterling Integrator if the command line process failed. If the returned success value does not match the returned status, the process fails. Without returning a success value from an OS script, failures are not detected and the process is assumed to have passed. This creates a failure for the business functionality that is hard to correct later. In writing OS scripts, always check the return status for each call and handle it properly. This includes returning the status values to the OS shell. Error handling in scripts can cause the script to exit before the final output file is generated. Returning from the script to Sterling Integrator without an output file is a critical error that is handled before the returned successValue is examined. See <i>Use the output generated by the command line process?</i> for dealing with this issue. Many OS commands do not return a success value, instead they output errors to stderr or stdout. In these cases, the commands stderr and/or stdout text must be captured, filtered, and an error status returned if the command failed.</p>

### Output from Adapter to Business Process

The following table contains the parameters passed from the Command Line Adapter 2 to the business process:

Parameter Name and Element Value (BPML)	Description
Document (CLA2/document)	If a file is collected in non-bootstrap mode, the document is placed in ProcessData, not as the Primary Document.
DocumentId (CLA2/documentId)	If a file is collected in non-bootstrap mode, the document identifier of the document is placed here.
ProcessExitValue (CLA2/ProcessExitValue)	Sets the process data value to the exit value of the process.
FileName (CLA2/FileName)	The name of the file, if any, that was collected as part of the output from the process that ran.

## Usage Examples

This section contains an example using the Command Line Adapter 2. Examples are included using both the GPM and BPML.

### Invoking the Command Line Adapter to Run a Shell Script

The following example business process illustrates using the Command Line Adapter 2 to execute a shell script that expects an input file as the first parameter, an output file as the second parameter, and three other parameters.

- When this example configuration is used, a shell script called “test.sh” (which resides in the /home directory) is run.
- The program requires the input filename as the first parameter, the output filename as the second parameter, and three other parameters.
- Because the useInput variable is set to true and the inputName variable is blank, the name of the primary document replaces the \$Input placeholder.
- Because the useOutput variable is set to true and the outputName variable is blank, the \$Output placeholder is replaced with the name of the primary document.
- If the document name in the workflow context is “data.txt” in this example, the command line becomes /home/test.sh data.txt data.txt VAR1 USER 10 at run-time.
- The name of the primary document is passed as the input file to the shell script program on the command line.
- The name of the primary document is passed as the output file to the shell script program on the command line.

**Note:** If the inputName and outputName parameters had file names entered, these file names would replace the \$Input and \$Output placeholders.

## GPM Example

The following example illustrates the above business process using the GPM.

**Example\_CommandLineAdapter2.bp**

```
graph LR; Start((Start)) --> Adapter[Command Line 2 Adapter]; Adapter --> End((End))
```

**Service Editor - Command Line 2 Adapter**

Name: Command Line 2 Adapter

Config: Sample\_CommandLine2\_Adapter

Message To Service | Message From Service

Output Msg: Messages Only

Message Name: CmdLine2InputMessage

Name	Value	Use XPATH?
bootstrap	Yes	<input type="checkbox"/>
cla2_debug	No	<input type="checkbox"/>
cmdLine	/home/test.sh \$Input \$Output \$0 \$1 \$2	<input type="checkbox"/>
docStorageType	System Default	<input type="checkbox"/>
env0	VAR1=TEST	<input type="checkbox"/>
env1	USER=ME	<input type="checkbox"/>
env2		<input type="checkbox"/>
env3		<input type="checkbox"/>
env4		<input type="checkbox"/>
env5		<input type="checkbox"/>
env6		<input type="checkbox"/>
env7		<input type="checkbox"/>

## Business Process Modeling Language (BPML) Example

The following example illustrates the same business process using BPML.

```
<process name="Example_CommandLine2_BP">
  <operation name="Command Line Adapter 2 Run Script">
    <participant name="Sample_CommandLine2_Adapter"/>
    <output message="CmdLine2InputMessage">
      <assign to="."> from="*"/>
      <assign to="parm0">VAR1</assign>
      <assign to="parm1">USER</assign>
      <assign to="parm2">10</assign>
      <assign to="env0">VAR1=TEST</assign>
      <assign to="env1">USER=ME</assign>
    </output>
    <input message="inmsg">
```

```

        <assign to="." from="*"></assign>
    </input>
</operation>
</process>

```

## Enabling the Command Line Adapter 2

Before you can use the Command Line Adapter 2, you must enable the server by editing the `sandbox.cfg` file. For more information on installing the Command Line Adapter 2 server remotely, see *Installing the Command Line Adapter 2 server remotely*.

Also, if you have a custom Command Line Adapter 2, you must reconfigure each of your custom adapters with the authentication and SSL options, see *Configuring the Command Line Adapter 2*.

To enable the Command Line Adapter 2 locally in your environment:

1. Open `sandbox.cfg` file that is in the `install_dir/install/properties` directory.
2. Add the `LAUNCH_CLA2_SERVER` property and set the value to `true`.
 

```
LAUNCH_CLA2_SERVER=true
```
3. Run the `setupfile.sh/.cmd` to recycle Sterling Integrator.
4. Start and stop the Command Line Adapter 2.
  - Start the Command Line Adapter 2 with the `startCmdLine2.sh` (UNIX) or the `StartCLA2WindowsService.cmd` (Windows) script.
  - Stop the Command Line Adapter 2 with the `stopCmdLine2.sh` (UNIX) or the `StopCLA2WindowsService.cmd` (Windows) script.

**Tip:** To use **Operations > System > JVM Monitor > Take Thread Dump**, the default Command Line Adapter 2 must match the `CLA2_PORT` in the `sandbox.cfg` to take thread dumps from the User Interface.

## Installing the Command Line Adapter 2 server remotely

Before you begin editing the files on your remote server, you must copy the needed files to your remote server.

**Important:** For secure Command Line Adapter 2 remote deployment, ensure that only the Sterling Integrator boxes have direct network access to the remote host Command Line Adapter 2 port.

To install the Command Line Adapter 2 server remotely:

1. Run the `<install>/bin/CLA2makejar.sh`(UNIX or Linux) or `<install>/bin/CLA2makejar.cmd` (Windows) script in your Sterling B2B Integrator instance to create the `CLA2RemotePackage.jar` in your `/bin` directory.
2. Copy the `CLA2RemotePackage.jar` to your remote server.
3. Create a directory on your remote server `<remoteFolder>`.
4. Copy the `CLA2RemotePackage.jar` into your `<remoteFolder>` and extract the contents of the `CLA2RemotePackage.jar`.
5. Edit the following scripts in your `<remoteFolder>` by updating all the remote paths and ports.
  - `startCmdLine2.sh` (UNIX)

```

jvm_args="-Xms128m -Xmx512m -DcmdlineProps2="<remoteFolder>/CmdLine2server.properties" -jar"
clientJar=<remoteFolder>/CLA2Client.jar
logOutput=<remoteFolder>/CmdLine2.output

```

```
nohup <remoteFolder>/bin/java $jvm_args $clientJar <remotePort> > $logOutput 2>&1 &
cmdLine2pid=$!
echo $cmdLine2pid > <remoteFolder>/cmdline2.pid
echo CmdLine2 started with PID=$cmdLine2pid
```

- stopCmdLine2.sh (UNIX)

```
pidFile=<remoteFolder>/cmdline2.pid
```

- start\_remote\_CLA2\_console.cmd (Windows)

```
<remoteFolder>/bin/java.exe -Xss256k -Xms64m -Xmx512m -DcmdlineProps2=
<remoteFolder>/CmdLine2server.properties -Djava.io.tmpdir=<remoteFolder>
-Djava.class.path=<remoteFolder>/CLA2Client.jar; com.sterlingcommerce.woodstock.
services.cmdline2.CmdLine2RemoteImpl <remotePort> > <remoteFolder>/cla2client.log 2>&1
```

6. Edit the CmdLine2server.properties file in your <remoteFolder>.

```
keystore_location=<remoteFolder>/cla2_KeyStore.jks
```

**Tip:** The host binding property CLA2NetworkHosts is in the CmdLine2server.properties file and the host binding must include the remote host name for example: localhost,chantico.dub.usoh.ibm.com.

7. Edit the log file location in the Cmdline2server.properties file.

```
logLocation=<remoteFolder>/cla2server.log
```

8. Modify the \*.sh files to make them executable.

```
chmod 740 *.sh
```

9. Start the CLA2 server with the start script in your remote directory.

- startCmdLine2.sh (UNIX)
- start\_remote\_CLA2\_console.cmd (Windows)

10. Verify that the server started correctly by viewing the cla2client.log file.

11. Stop the Command Line Adapter 2 server with the stop script in your remote directory.

- stopCmdLine2.sh (UNIX)
- Ctrl + C (Windows)

## Stopping the Command Line Adapter 2

If Sterling Integrator is shut down with the (Windows) stopWindowsService.cmd or (UNIX and iSeries) hardstop.sh script, the Command Line Adapter 2 also shuts down.

You can also stop the Command Line Adapter 2 with these commands:

- (UNIX or iSeries) ./stopCmdLine2.sh
- (Windows service) stopCLA2WindowsService.cmd

Otherwise, once started, the adapter runs silently as configured and does not return to the command line until it is finished, interrupted, or fails. Therefore, you cannot use that command line to execute any other commands.

## Maintaining authentication and SSL keys

The Command Line Adapter 2 provides default keys. However, you can use custom keys for authentication and SSL both locally and remotely. For remote custom keys, you must update the Java™ keystore (JKS) file and the property file in your remote directory. For more information on importing keys, see *Security*.

**Restriction:** The Command Line Adapter 2 server cannot have more than one private certificate in the JKS repository.

To create an authentication key or SSL certificate:



1. Create a key pair with your preferred tool.
2. Import the key pair into the Sterling Integrator system keys table. For more information on importing keys, see *Security*.
3. Select the imported key or certificate when you configure the Command Line Adapter 2 in Sterling Integrator.
4. Add the public key to the CLA2Server.jks file with your preferred tool (example: Keytool).
5. Set the publicCertAlias = <custom\_name> in the CmdLine2servers.properties file.

To create an SSL key:

1. Create a key pair with your preferred tool.
2. Import the certificate into the Sterling Integrator CA certificate table. For more information on importing keys, see *Security*.
3. Select the imported certificate when you configure the Command Line Adapter 2 in Sterling Integrator.
4. Add the private key to the CLA2Server.jks file with your preferred tool (example: Keytool).
5. Set the SSLCertificateName = <custom\_name> in the CmdLine2servers.properties file.

## PGP Package Service (Build 5104 or higher)

*Pretty Good Privacy* (PGP) is an open standard data encryption and decryption tool. The PGP Package service, in conjunction with the PGP Server Manager, enables you to encrypt and digitally sign documents using PGP.

The following table provides an overview of the PGP Package service:

System name	PGP Package service
Graphical Process Modeler (GPM) category	All Services
Description	This service encrypts and digitally signs a document based on the Open PGP standard, using public key or conventional cryptography.
Business usage	Use this service to encrypt and sign a document in the document area of process data.
Usage example	A business process is executed to encrypt and sign a document, based on the information stored in a PGP profile.
Preconfigured?	Yes. A configuration called PGP Package Service is installed with Sterling Integrator.
Requires third-party files?	No

Platform availability	<p>All supported Sterling Integrator platforms, with the following restrictions:</p> <p><b>For NAI McAfee eBusiness Server 8.1:</b></p> <ul style="list-style-type: none"> <li>• IBM AIX 4.2 or later</li> <li>• HP-UX 10.20 or later</li> <li>• Linux x86 Red Hat 6.0 or later (2.1.3-15 or later of GLIBC)</li> <li>• SuSE Linux for IBM S/390 and IBM Zseries</li> </ul> <p><b>For NAI McAfee eBusiness Server 8.5:</b></p> <ul style="list-style-type: none"> <li>• Solaris 9 or later</li> <li>• IBM AIX 4.2 or later</li> <li>• HP-UX 10.20 or later</li> </ul> <p><b>For NAI McAfee eBusiness Server 8.5.1:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows NT Server version 4.0 or later (Service Pack 6a or later)</li> <li>• Microsoft Windows 2000 Server or Advanced Server (Service Pack 4 or later)</li> <li>• Microsoft Windows Server 2003</li> <li>• Microsoft Windows XP Professional Version 2002 Service Pack 2</li> </ul> <p><b>For NAI McAfee eBusiness Server 8.6:</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 with Service Pack 4 or later</li> <li>• Red Hat ES 3.0</li> <li>• SunOS 5.9</li> <li>• HP-UX 11.0</li> <li>• AIX 5.1 or later</li> </ul>
-----------------------	--

Platform availability	<p>All supported Sterling Integrator platforms, with the following restrictions:</p> <p><b>For Massachusetts Institute of Technology (MIT) Command Line Freeware 6.5.8:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows NT version 4.0 or later (Service Pack 3 or later)</li> <li>• Microsoft Windows 2000</li> <li>• Sun Solaris for SPARC version 2.51 or later</li> <li>• IBM AIX 4.2 or later</li> <li>• HP-UX 10.20 or later</li> <li>• Linux x86 RedHat (RPM) 5.0 or later</li> </ul> <p><b>For PGP Corporation PGP® Command Line 9.5:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2000 (SP4)</li> <li>• Microsoft Windows 2003 (SP1)</li> <li>• Microsoft Windows XP (SP2)</li> <li>• Sun Solaris 9 (SPARC only; x86 is not supported)</li> <li>• IBM AIX 5.2</li> <li>• HP-UX 11i</li> <li>• Red Hat Enterprise Linux 3.0 on x86</li> <li>• Mac OS X 10.4 or greater</li> </ul> <p><b>For PGP Corporation PGP® Command Line 9.8:</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 (SP4)</li> <li>• Windows Server 2003 (SP1)</li> <li>• Windows XP (32- and 64-bit)</li> <li>• Windows Vista (32- and 64-bit)</li> <li>• HP-UX 11i and above (PA-RISC and Itanium)</li> <li>• IBM AIX 5.2 and 5.3</li> <li>• RedHat Enterprise Linux 3.0 and above (x86 only and x86_64)</li> <li>• Fedora Core 3 and above (x86_64 only)</li> <li>• Sun Solaris 9 (SPARC only) and Solaris 10 (SPARC, x86, and x86_64)</li> <li>• Apple Mac OS X 10.4.x and 10.5.x (Universal binary)</li> </ul> <p><b>For PGP Corporation PGP® Command Line 10.1:</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 SP4</li> <li>• Windows Server 2003 (32- and 64-bit) SP2</li> <li>• Windows Server 2008</li> <li>• Windows XP (32- and 64-bit) SP3</li> <li>• Windows Vista (32- and 64-bit) SP2</li> <li>• Windows 7 (32- and 64-bit)</li> <li>• HP-UX 11i and above (PA-RISC and Itanium)</li> <li>• IBM AIX 5.3 and 6.1</li> <li>• RedHat Enterprise Linux 5.0 (x86 and x86_64)</li> <li>• Fedora Core 6 (x86_64 only)</li> <li>• Sun Solaris 9 (SPARC) and Solaris 10 (SPARC, x86, and x86_64)</li> <li>• SLES (SUSE Linux Enterprise Server 9 SP4 and 10 SP2 x86)</li> <li>• Apple Mac OS X 10.5.x and 10.6.x (Intel-based systems only)</li> </ul>
Related adapters and services	<p>The PGP Package service works with the following services:</p> <ul style="list-style-type: none"> <li>• Command Line Adapter 2</li> <li>• PGP Unpackage service</li> </ul>

Application requirements	<p>Before using this service, install one of the following:</p> <ul style="list-style-type: none"> <li>• McAfee E-Business Server (version 8.1)</li> <li>• McAfee E-Business Server (version 8.5)</li> <li>• McAfee E-Business Server (version 8.5.1)</li> <li>• McAfee E-Business Server (version 8.6)</li> <li>• PGP® Command Line Freeware (version 6.5.8)</li> <li>• PGP® Command Line (version 9.5)</li> <li>• PGP® Command Line (version 9.8)</li> <li>• PGP® Command Line (version 10.1)</li> </ul> <p><b>Note:</b> Consider the nature of your PGP usage relative to the PGP vendor's licensing terms when choosing a package.</p>
Initiates business processes?	This service does not initiate business processes. This service cannot be used without a business process.
Invocation	A user who has permission to perform this activity must execute the business process that invokes this service.
Business process context considerations	The configuration parameters and the outgoing documents are picked up by the service in the business process context. In the receiving mode, the service puts the incoming documents into the business process context.
Returned status values	<p>Returned status values:</p> <ul style="list-style-type: none"> <li>• 0 - Success</li> <li>• 1- Error</li> </ul> <p>See <i>Advanced Status Messages</i> for a list of advanced statuses. Exit Codes will be displayed in the Advanced Status column, pre-pended by [PGPErrorCode].</p>
Restrictions	None
Persistence level	None
Testing considerations	Create the profile in the PGP Server Manager. This profile stores information about the PGP server, including PGP Type, PGP Executable, PGP Path, the location of the public key ring, the secret key ring, and the random number seed. It enables you to create key maps for secret key sets and conventional key sets. A pre-defined Command Line Adapter 2 (PGPCmdlineService) is installed with Sterling Integrator. The Command Line Adapter 2 is used for large file support (streaming). Start the remote Command Line 2 client. For more information about enabling and installing the Command Line Adapter 2, see <i>Command Line Adapter 2 (Build 5104 or higher)</i> .

## Implementing the PGP Package Service

To implement the PGP Package service, complete the following tasks:

1. Activate your license for the PGP Package service. See *Managing Services and Adapters*.
2. Create a PGP profile, using the Sterling Integrator PGP Server Manager. See *PGP Server Manager*.
3. Create a PGP Package service configuration. See *Managing Services and Adapters*.
4. Configure the service. See *Configuring the PGP Package Service*.
5. Use the PGP Package service in a business process.

## Configuring the PGP Package Service

Before configuring, consider the following:

- `public_user` (if using Public Key Cryptography) or `conv_keymap_name` (if using Conventional Cryptography) must be present for PGP Package service to perform encryption.
- `secret_keymap_name` must be present for PGP Package service to perform signing.
- To perform encryption and signing, a combination of both the previous statements applies.
- If `public_user` and `conv_keymap_name` appear in the same business process, public key encryption will take precedence.

To configure the PGP Package service, specify settings specify the settings for the fields in the GPM. These fields are described in the following table:

Field	Description
<code>Config</code>	Name of the service configuration.
<code>workingDir</code>	The working directory where files used for encryption and signing will be read from or written to. Optional if the <code>cmdline2svcname</code> field is defined in the Command Line Adapter 2.
<code>remoteName</code>	Remote name or IP address where the remote adapter implementation is running. Optional if the <code>cmdline2svcname</code> field is defined in the Command Line Adapter 2.
<code>remotePort</code>	Remote port that the remote adapter implementation is listening on. Optional if the <code>cmdline2svcname</code> field is defined in the Command Line Adapter 2.
<code>profile_name</code>	Name of PGP profile from the PGP Server Manager. Required.
<code>compress</code>	Compression to be done before encryption or signing. Valid value is On. Default is On. Required for encryption and signing.
<code>public_user</code>	User name or key ID in the public key ring. Required for encryption (public key cryptography).
<code>secret_keymap_name</code>	Key name defined in the secret key ring in the PGP profile. Required for signing (public key cryptography).
<code>conv_keymap_name</code>	Key name defined in the public key ring in the PGP profile. Required for encryption (conventional cryptography).
<code>conv_cipher</code>	The symmetric cipher to use when performing a conventional encryption operation (that is, <code>conv_keymap_name</code> is used). Valid values are: IDEA, CAST5, 3DES, AES128, AES196, AES256, Twofish. Default is IDEA. Optional.
<code>DocumentId</code>	The document identifier referenced to the document to be processed specifically. The default document for processing is the primary document. Optional.
<code>cmdline2svcname</code>	If not using the default configuration of the Command Line 2 adapter (PGPCmdlineService), enter the name of the configuration to be used. Optional.
<code>ascii_armor</code>	Whether to encode the file with McAfee E-Business Server's base-64 encoding (ASCII-armored format). Valid values are On and Off. Default is On. Optional.

Field	Description
textmode	Whether the input data is ASCII text and should be converted to canonical new lines before encryption. Valid values are On and Off. Default is Off. Optional.
outputfilename	Output file name. For McAfee E-Business Server and PGP Command Line Freeware, outputfilename must have an extension of .asc or .pgp. If a different extension is used, outputfilename will be appended with .asc. For all versions, if outputfilename is not specified, the file name is retrieved from the name of the primary document or the body name of the document and is appended with the following: <ul style="list-style-type: none"> <li>• *.asc during normal encryption</li> <li>• .exe during sda process</li> <li>• .pga during pgparchive process</li> </ul> Optional.
pgp_partner_name	The partner name used in encryption and signing. If specified, the business process uses the parameters you specify in the selected partner profile. Required if you specify a value in the pgp_sponsor_name parameter. The values you specify in the GPM override the values you specify in the profile.
pgp_sponsor_name	The sponsor name used in encryption and signing. If specified, the business process uses the parameters you specify in the selected sponsor profile. Required if you specify a value in the pgp_partner_name parameter. The values you specify in the GPM override the values you specify in the profile.
tmpDir	The directory location for temporary scratch files. If not specified, the temporary files are written in the current working directory. If the shell environmental variable TMP is defined, PGP stores temporary files in the named directory. Optional.
clearsig	Generates a signed message that can be read without PGP. The recipient must still use PGP to verify the signature. Unencrypted PGP-signed messages have a signature certificate pre-pended in binary form. The signed message is compressed. Therefore, it is unreadable by humans even though it is not encrypted. Cannot be used with EncryptAndSign on the command line. If you enable clearsig, it is recommended you enable ascii_armor and textmode also. Valid values are On and Off. Default is Off. Optional.

Field	Description
info	<p>How much information is returned. Valid values are:</p> <ul style="list-style-type: none"> <li>• Quiet - Only displays error messages. Not applicable to PGP Command Line. If selected defaults to normal mode.</li> <li>• Normal - Displays warnings and error messages. Default.</li> <li>• Verbose - Displays helpful messages, warnings, and error messages. Use this setting to diagnose problems. Only available for McAfee E-Business Server (version 8.1 or later) and PGP Command Line (version 9.5). If selected with other versions, defaults to normal mode.</li> <li>• Debug - Displays developer-level output in addition to the output produced by the other levels. This level may include the display of internal data, statistics, trace information, and return codes from internal functions. Do not use unless instructed to do so. Not applicable to PGP Command Line. If selected, defaults to normal mode.</li> </ul> <p>Optional.</p>
sda	<p>Applicable only to McAfee E-Business Server (version 8.1 or later) and PGP Command Line (version 9.5). Used only when conv_keymap_name is specified. Creates a self-decrypting executable file, which is conventionally encrypted using a passphrase. The resulting file can be decrypted by double-clicking it and entering the passphrase. Used to send encrypted files to people who do not have E-Business Server or PGP Command Line installed. SDA files can be created with any platform that McAfee E-Business Server (version 8.1 or later) supports, but can be executed only on Windows platforms. To create sda files with PGP Command Line (version 9.5), set the target_platform parameter (described later in this table). The default file extension is .exe.</p> <p><b>Note:</b> The sda file cannot exceed 4 GB after compression. Valid values are On and Off. Default is Off.</p> <p>Optional.</p>
pgparchive	<p>Applicable only to McAfee E-Business Server (version 8.1 or later) and PGP Command Line (version 9.5). Used only when conv_keymap_name is specified. Creates a file that can be decrypted using the archive reader, which can be redistributed freely. Used to send encrypted files to people who do not have E-Business Server or PGP Command Line installed. The default extension is .pga. Valid values are On and Off. Default is Off.</p> <p>Optional.</p>
discard_paths	<p>Applicable only with sda or pgparchive. Strips relative path information from the list of files in a sda or pgparchive. During the decryption of the archive, the files are placed in the current directory instead of in subdirectories of the current directory.</p> <p>Optional.</p>

Field	Description
target_platform	Applicable only with PGP Command Line (version 9.5) and sda. Specifies the platform an sda file can be decrypted on. Valid values are: <ul style="list-style-type: none"> <li>• win32</li> <li>• linux</li> <li>• solaris</li> <li>• aix</li> <li>• hpux</li> <li>• osx</li> </ul> Default is the current platform. Optional.

## Parameters Passed from Service to BP

The following table contains the parameters that are passed from the PGP Package service to the business process:

Parameter	Description
Action (PGP/Action)	Action of this PGP execution. Valid values are: <ul style="list-style-type: none"> <li>• ENCRYPT</li> <li>• ENCRYPT_SIGN</li> <li>• SIGN</li> </ul> Required.
FileName (PGP/FileName)	Name of the file being processed. Required.
Document (PGP/Document)	The processed document is placed in Process Data – not as Primary Document. The attribute is the SCIOBJECTID, which enables a hyperlink for viewing the content of the processed document. Required.
DocumentId (PGP/DocumentId)	Document identifier of the document. Required.
Status (PGP/Status)	Process status. Valid values are Success and Error. Required.
ErrorCode (PGP/ErrorCode)	Value returned from executing PGP commands. Displayed when the Status is Error. Optional.
ErrorDescription (PGP/ ErrorDescription)	This is the error description based on the ErrorCode. Displayed when the Status is Error. Optional.

## Business Process Example - Encrypt Operation (Public Key Encryption)

This following business process uses the PGP Package service to encrypt the primary document in the document area. The profile is based on PGP107. In this example, you use the default Command Line2 adapter configuration, PGPCmdlineService, to execute the encrypt command. You want to use the working directory, remote name and port stated in the BPML. Therefore, these values override the pre-configured values in PGPCmdLineService. The public key ID, which must be in the public keyring file specified in the profile, PGP107, is used for encryption.

```
<process name="PGP_Encrypt ">
  <sequence name="optional">
    <operation name="One">
```



```

    <participant name="PGPPackageService"/>
    <output message="Xout">
      <assign to="." from="*"></assign>
      <assign to="profile_name">PGP107</assign>
      <assign to="compress">on</assign>
      <assign to="workingDir">/server1/tmp</assign>
      <assign to="remoteName">00.000.00.000</assign>
      <assign to="remotePort">12345</assign>
      <assign to="public_user">0x2343</assign>
    </output>
    <input message="Xin">
      <assign to="." from="*"></assign>
    </input>
  </operation>
</sequence>
</process>

```

## Business Process Example - Encrypt Operation (Conventional Encryption)

This following business process uses the PGP Package service to encrypt the primary document in the document area of process data. The profile is based on PGP107. In this example, you use the Command Line2 adapter configuration, MyCLA2, to execute the commands. The remote name, port, and working directory are pre-configured in the service configuration. The value of conv\_keymap\_name, Conv\_abc\_tp, which must be in the profile's conventional key map, is used for conventional encryption:

```

<process name="PGP_Encrypt ">
  <sequence name="optional">
    <operation name="One">
      <participant name=" PGPPackageService "/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>
        <assign to="compress">on</assign>
        <assign to="conv_keymap_name">Conv_abc_tp</assign>
        <assign to="conv_cipher">CAST5</assign>
        <assign to="cmdline2svcname">MyCLA2</assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>

```

## Business Process Example - Encrypt and Sign Operation (Public Key Encryption)

The following business process uses the PGP Package service to encrypt and sign the primary document in the document area. For signing, you need to pass in the secret\_keymap\_name, which must be in the PGP107 profile's secret key map. The public key ID, which must be in the public keyring file specified in the profile, PGP107, is used for encryption. In this example, you choose not to compress the document before signing and encryption.

```

<process name="PGP_Encrypt_Sign">
  <sequence name="optional">
    <operation name="One">
      <participant name=" PGPPackageService "/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>

```

```

        <assign to="compress">off</assign>
        <assign to="workingDir">/server1/tmp</assign>
        <assign to="remoteName">00.000.00.000</assign>
        <assign to="remotePort">12345</assign>
        <assign to="public_user">0x2343</assign>
        <assign to="secret_keymap_name">my_secret</assign>
</output>
    <input message="Xin">
        <assign to="." from="*"></assign>
    </input>
</operation>
</sequence>
</process>

```

## Business Process Example - Encrypt and Sign Operation (Conventional Encryption)

The following business process uses PGP Package Service to encrypt and sign the Primary Document in the document area. For signing, the user needs to pass in the secret\_keymap\_name, which must be present in the PGP107 profile's Secret Key Map. The value of conv\_keymap\_name, Conv\_abc\_tp, which must be present in the Profile's Conventional Key Map, is used for conventional encryption. The user chooses not to compress the document before signing and encryption.

```

<process name="PGP_Encrypt_Sign">
  <sequence name="optional">
    <operation name="One">
      <participant name=" PGPPackageService "/>
      <output message="Xout">
        <assign to="profile_name">PGP107</assign>
        <assign to="compress">off</assign>
        <assign to="workingDir">/localsvr/share/tmp</assign>
        <assign to="remoteName">nn.nnn.nn.nnn</assign>
        <assign to="remotePort">xxxx</assign>
        <assign to="conv_keymap_name">Conv_abc_tp</assign>
        <assign to="conv_cipher">CAST5</assign>
        <assign to="secret_keymap_name">si_secret</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>

```

## Business Process Example - Encrypt Operation (Public Key Encryption) Using a Specific Document ID

The following business process uses the PGP Package service to encrypt a document, with the document ID columbia:1774b9b:feaea8ae12:-6ea8 in the document area.

```

<process name="PGP_Encrypt ">
  <sequence name="optional">
    <operation name="One"> PGPPackageService
      <participant name="PGPPackageService"/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>
        <assign to="compress">on</assign>
        <assign to="workingDir">/server1/tmp</assign>
        <assign to="remoteName">00.000.00.000</assign>
        <assign to="remotePort">12345</assign>
        <assign to="public_user">0x2343</assign>
      </output>
    </operation>
  </sequence>
</process>

```

```

        <assign to="DocumentId">columbia:1774b9b:feaea8ae12:
            -6ea8</assign>
    </output>
    <input message="Xin">
        <assign to="." from="*"></assign>
    </input>
</operation>
</sequence>
</process>

```

## Business Process Example - Sign Operation

The following business process uses the PGP Package service to sign the primary document in the document area.

```

<process name="PGP_Sign ">
  <sequence name="optional">
    <operation name="One">
      <participant name="PGPPackageService"/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>
        <assign to="compress">on</assign>
        <assign to="workingDir">/server1/tmp</assign>
        <assign to="remoteName">00.000.00.000</assign>
        <assign to="remotePort">12345</assign>
        <assign to="secret_keymap_name">my_secret</assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>

```

## Business Process Example - OnFault Handling

The following business process shows the onFault handling for the PGP Package service.

```

<process name="PGP_Sign ">
  <sequence name="optional">
    <operation name="One">
      <participant name="PGPPackageService"/>
      <output message="Xout">
        <assign to="profile_name">PGP107</assign>
        <assign to="compress">on</assign>
        <assign to="workingDir">/localsvr/share/tmp</assign>
        <assign to="remoteName">nn.nnn.nn.nnn</assign>
        <assign to="remotePort">12345</assign>
        <assign to="secret_keymap_name">si_secret</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
    <assign to="Status">The file is signed successfully</assign>
    <onFault>
      <assign to="Status">General Error Occurred</assign>
    </onFault>
    <onFault code="[PGPErrorCode] Signature Check error">
      <assign to="Status">Incorrect signature</assign>
    </onFault>
  </sequence>
</process>

```

## Business Process Example - PGP Partner and PGP Sponsor

The following business process uses the PGP Partner and PGP Sponsor services to encrypt and sign documents.

```
<process name="use_partner_sponsor">
  <operation name="PGP Package Service">
    <participant name="PGPPackageService"/>
      <output message="PGPPackageServiceTypeInputMessage">
        <assign to="pgp_partner_name">partner</assign>
        <assign to="pgp_sponsor_name">sponsor</assign>
        <assign to="profile_name">pgp</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </process>
```

## Advanced Status Messages

The following table contains exit codes from the McAfee E-Business Server and PGP Command Line Freeware. The content of the Description field is displayed in the Advanced Status column, preceded by [PGPErrorCode]:

Status	Description
0	Exit OK, no error
1	Invalid file
2	File not found
3	Unknown file
4	Batch mode error
5	Bad argument
6	Process Interrupted
7	Out of memory error
8	Environment error
20	Signature error
21	Public Key Encryption error
22	Encryption error
23	Compression error
30	Signature Check error
31	Public Key Decryption error
32	Decryption error
33	Decompression error
34	Keyring locked error
101	File parsing error

The following table contains exit codes from PGP Command Line (version 9.5) from PGP Corporation. The content of the Description field is displayed in the Advanced Status column, preceded by [PGPErrorCode]:

Status	Description
0	PGP Command Line exited successfully.
64	Parser error.
71	Bad data was received from the operating system at startup.
128	An internal error occurred.
129	An initialization failure occurred on startup.
130	A user interrupt occurred.
145	Error purging a cache: passphrase, keyring, or both.
146	Error creating keyring files.
147	Error during a speed test operation.
160	Complete failure during a file wipe.
161	Partial fail, partial success during a file wipe (one file wiped, one not, for example).
162	Complete failure during an encode.
163	Partial failure during an encode.
164	Complete failure during a decode.
165	Partial failure during a decode.
210	Error during one of the key list operations.
220	Error during key maintenance.
221	Error when checking signatures.
222	Error when checking user IDs.
230	Error during one of the key edit operations.
240	Error during one of the key server operations.
245	Error with supplied license.
251	License is expired.
255	An unknown error occurred.

The following table contains errors that result from the PGP Package service when it validates information before executing PGP commands on the remote server. The content of the status field will be displayed in the Advanced Status column:

Status	Description
Error in accessing the document with a given DocumentId	The DocumentId value given in the BPML is incorrect.
Fail to get data from Primary Document.: There is no Primary Document	Primary Document is mandatory.
Incorrect Profile Name in BPML Param: 'profile_name'. It is not found in the PGP Server Manager	The profile_name value given in the BPML is incorrect.
Incorrect Key Name (BPML Param: 'secret_keymap_name'). It is not found in the PGP Profile's Secret KeyMap	The secret_keymap_name value given in the BPML is incorrect.
Incorrect Key Name (BPML Param: 'conv_keymap_name'). It is not found in the PGP Profile's Conventional KeyMap	The conv_keymap_name value given in the BPML is incorrect.

## PGP Unpackage Service (Build 5104 or higher)

*Pretty Good Privacy* (PGP) is an open standard data encryption and decryption tool. The PGP Unpackage service, in conjunction with the PGP Server Manager, enables you to decrypt documents and verify their signatures.

The following table provides an overview of the PGP Unpackage service:

System name	PGP Unpackage service
Graphical Process Modeler (GPM) category	All Services
Description	This service is used to decrypt and verify the signature of a document based on the Open PGP standard, using a public key or conventional cryptography.
Business usage	Use this service to decrypt or verify the signature of the document in the document area.
Usage example	A business process is executed to decrypt or verify the signature of the document based on the PGP profile. See <i>PGP Server Manager</i> .
Preconfigured?	Yes
Requires third-party files?	No
Platform availability	<p>All supported Sterling Integrator platforms, with the following restrictions:</p> <p><b>For NAI McAfee eBusiness Server 8.1:</b></p> <ul style="list-style-type: none"> <li>• IBM AIX 4.2 or later</li> <li>• HP-UX 10.20 or later</li> <li>• Linux x86 Red Hat 6.0 or later (2.1.3-15 or later of GLIBC)</li> <li>• SuSE Linux for IBM S/390 and IBM Zseries</li> </ul> <p><b>For NAI McAfee eBusiness Server 8.5:</b></p> <ul style="list-style-type: none"> <li>• Solaris 9 or later</li> <li>• IBM AIX 4.2 or later</li> <li>• HP-UX 10.20 or later</li> </ul> <p><b>For NAI McAfee eBusiness Server 8.5.1:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows NT Server version 4.0 or later (Service Pack 6a or later)</li> <li>• Microsoft Windows 2000 Server or Advanced Server (Service Pack 4 or later)</li> <li>• Microsoft Windows Server 2003</li> <li>• Microsoft Windows XP Professional Version 2002 Service Pack 2</li> </ul> <p><b>For NAI McAfee eBusiness Server 8.6:</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 with Service Pack 4 or later</li> <li>• Red Hat ES 3.0</li> <li>• SunOS 5.9</li> <li>• HP-UX 11.0</li> <li>• AIX 5.1 or later</li> </ul>

Platform availability	<p>All supported Sterling Integrator platforms, with the following restrictions:</p> <p><b>For Massachusetts Institute of Technology (MIT) Command Line Freeware 6.5.8:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows NT version 4.0 or later (Service Pack 3 or later)</li> <li>• Microsoft Windows 2000</li> <li>• Sun Solaris for SPARC version 2.51 or later</li> <li>• IBM AIX 4.2 or later</li> <li>• HP-UX 10.20 or later</li> <li>• Linux x86 RedHat (RPM) 5.0 or later</li> </ul> <p><b>For PGP Corporation PGP® Command Line 9.5:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2000 (SP4)</li> <li>• Microsoft Windows 2003 (SP1)</li> <li>• Microsoft Windows XP (SP2)</li> <li>• Sun Solaris 9 (SPARC only; x86 is not supported)</li> <li>• IBM AIX 5.2</li> <li>• HP-UX 11i</li> <li>• Red Hat Enterprise Linux 3.0 on x86</li> <li>• Mac OS X 10.4 or greater</li> </ul> <p><b>For PGP Corporation PGP® Command Line 9.8:</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 (SP4)</li> <li>• Windows Server 2003 (SP1)</li> <li>• Windows XP (32- and 64-bit)</li> <li>• Windows Vista (32- and 64-bit)</li> <li>• HP-UX 11i and above (PA-RISC and Itanium)</li> <li>• IBM AIX 5.2 and 5.3</li> <li>• RedHat Enterprise Linux 3.0 and above (x86 only and x86_64)</li> <li>• Fedora Core 3 and above (x86_64 only)</li> <li>• Sun Solaris 9 (SPARC only) and Solaris 10 (SPARC, x86, and x86_64)</li> <li>• Apple Mac OS X 10.4.x and 10.5.x (Universal binary)</li> </ul> <p><b>For PGP Corporation PGP® Command Line 10.1:</b></p> <ul style="list-style-type: none"> <li>• Windows 2000 SP4</li> <li>• Windows Server 2003 (32- and 64-bit) SP2</li> <li>• Windows Server 2008</li> <li>• Windows XP (32- and 64-bit) SP3</li> <li>• Windows Vista (32- and 64-bit) SP2</li> <li>• Windows 7 (32- and 64-bit)</li> <li>• HP-UX 11i and above (PA-RISC and Itanium)</li> <li>• IBM AIX 5.3 and 6.1</li> <li>• RedHat Enterprise Linux 5.0 (x86 and x86_64)</li> <li>• Fedora Core 6 (x86_64 only)</li> <li>• Sun Solaris 9 (SPARC) and Solaris 10 (SPARC, x86, and x86_64)</li> <li>• SLES (SUSE Linux Enterprise Server 9 SP4 and 10 SP2 x86)</li> <li>• Apple Mac OS X 10.5.x and 10.6.x (Intel-based systems only)</li> </ul>
Related adapters	<p>The PGP Unpackage service works with the following services:</p> <ul style="list-style-type: none"> <li>• Command Line Adapter 2</li> <li>• PGP Package service</li> </ul>

Application requirements	<p>Before using this service, install one of the following:</p> <ul style="list-style-type: none"> <li>• McAfee E-Business Server (version 8.1)</li> <li>• McAfee E-Business Server (version 8.5)</li> <li>• McAfee E-Business Server (version 8.5.1)</li> <li>• McAfee E-Business Server (version 8.6)</li> <li>• PGP® Command Line Freeware (version 6.5.8)</li> <li>• PGP® Command Line (version 9.5)</li> <li>• PGP® Command Line (version 9.8)</li> <li>• PGP® Command Line (version 10.1)</li> </ul> <p><b>Note:</b> Consider the nature of your PGP usage relative to the PGP vendor's licensing terms when choosing a package.</p>
Initiates business processes?	This service does not initiate business processes. This service cannot be used without a business process.
Invocation	A user who has permission to perform this activity must execute the business process that invokes this service.
Business process context considerations	The configuration parameters and the outgoing documents are picked up by the service in the business process context. In the receiving mode, the service puts the incoming documents into the business process context.
Returned status values	<p>Returned status values:</p> <ul style="list-style-type: none"> <li>• 0 - Success</li> <li>• 1- Error</li> </ul> <p>See <i>Advanced Status Messages</i> for a list of advanced statuses. Exit Codes will be displayed in the Advanced Status column, pre-pended by [PGPErrorCode] .</p>
Restrictions	None
Persistence level	None
Testing considerations	<p>Create the profile in the PGP Server Manager. This profile stores information about the PGP server, including PGP Type, PGP Executable, PGP Path, the location of the public key ring, the secret key ring, and the random number seed. It enables you to create key maps for secret key sets and conventional key sets. A pre-defined Command Line Adapter 2 (PGPCmdlineService) is installed with Sterling Integrator. The Command Line Adapter 2 is used for large file support (streaming). Start the remote Command Line 2 client. For more information about enabling and installing the Command Line Adapter 2, see <i>Command Line Adapter 2 (Build 5104 or higher)</i>.</p>

## Implement the PGP Unpackage Service

To implement the PGP Unpackage service, complete the following tasks:

1. Activate your license for the PGP Unpackage service.
2. Create a PGP profile, using the PGP Server Manager.
3. Create a PGP Unpackage service configuration.
4. Configure the PGP Unpackage service.
5. Use the PGP Unpackage service in a business process.

## Configure the PGP Unpackage Service

Before configuring the PGP Unpackage service, consider the following:

- If the `secret_keymap_name` and `conv_keymap_name` parameters are not present, the PGP Unpackage service will verify the signature of the document only.



- If one of the `keymap_name` parameters is present, it will use the information of the `keymap_name` to decrypt.
- If there is a signature in the document, the verification of the signature will be done automatically.

To configure the PGP Unpackage service, specify the settings for the fields in the GPM. These fields are described in the subsequent table.

Field	Description
<code>Config</code>	Name of the service configuration.
<code>workingDir</code>	The working directory where files for decryption or verification will be read from or written to. You must set this parameter in this field or in the associated Command Line 2 adapter configuration.
<code>remoteName</code>	Remote name or IP address where the remote adapter implementation is running. Optional if the <code>cmdline2svcname</code> field is defined in the Command Line 2 adapter. You must set this parameter in this field or in the associated Command Line 2 adapter configuration.
<code>remotePort</code>	Remote port that the remote adapter implementation is listening on. Optional if the <code>cmdline2svcname</code> field is defined in the Command Line 2 adapter. You must set this parameter in this field or in the associated Command Line 2 adapter configuration.
<code>profile_name</code>	The name of PGP profile. Required.
<code>secret_keymap_name</code>	Key name defined in the secret key ring in the PGP profile. Required for decryption (public key cryptography).
<code>conv_keymap_name</code>	Key name defined in the public key ring in the PGP profile. Required for decryption (conventional cryptography).
<code>DocumentId</code>	The document identifier for the document to be processed. The default document for processing is the primary document. Optional.
<code>cmdline2svcname</code>	If not using the default configuration of the Command Line 2 adapter (PGPCmdlineService), enter the name of the configuration to be used. Optional.

Field	Description
outputfilename	<p>Output file name. For McAfee E-Business Server and PGP Command Line Freeware, outputfilename must have an extension of .asc or .pgp. If a different extension is used, outputfilename will be appended with .asc. For all versions, if outputfilename is not specified, the file name is retrieved from the name of the primary document or the body name of a document and is appended with the following:</p> <ul style="list-style-type: none"> <li>• *.asc during normal encryption</li> <li>• .exe during SDA process</li> <li>• .pga during pgparchive process</li> </ul> <p>Optional.</p>
pgp_partner_name	<p>The partner name used in encryption and signing. If specified, the business processuses the parameters you specify in the selected partner profile. Required if you specify a value in the pgp_sponsor_name parameter. The values you specify in the GPM override the values you specify in the profile.</p>
pgp_sponsor_name	<p>The sponsor name used in encryption and signing. If specified, the business processuses the parameters you specify in the selected sponsor profile. Required if you specify a value in the pgp_partner_name parameter. The values you specify in the GPM override the values you specify in the profile.</p>
tmpDir	<p>The directory location for temporary scratch files. If not specified, the temporary files are written in the current working directory. If the shell environmental variable TMP is defined, PGP stores temporary files in the named directory. Optional.</p>

Field	Description
info	<p>How much information is returned. Valid values are:</p> <ul style="list-style-type: none"> <li>• Quiet - Only displays error messages. Not applicable to PGP Command Line (version 9.5). If selected, defaults to normal mode.</li> <li>• Normal - Displays warnings and error messages. Default.</li> <li>• Verbose - Displays helpful messages, warnings, and error messages. Use this setting to diagnose problems. Only available for McAfee E-Business Server (version 8.1 or later) and PGP Command Line (version 9.5). If selected with other versions, defaults to normal mode.</li> <li>• Debug - Displays developer-level output in addition to the output produced by the other levels. This level may include the display of internal data, statistics, trace information, and return codes from internal functions. Do not use unless instructed to do so. Not applicable to PGP Command Line (version 9.5). If selected, defaults to normal mode.</li> </ul> <p>Optional.</p>

The following table contains the parameters that are passed from the PGP Unpackage service to the business process:

Parameter	Description
Action (PGP/Action)	Action of this PGP execution. Valid values are DECRYPT and VERIFY. Required.
FileName (PGP/FileName)	The name of the file which is being processed. Required.
DocumentPGP/Document()	The processed document is placed in Process Data – not as Primary Document. The attribute is the SCIOBJECTID, which allows the user to click on it for viewing the content of the processed document. Required.
DocumentId (PGP/DocumentId)	The document identifier of the document. Required.
Status (PGP/Status)	The status shows if this process has completed successfully or failed. Valid values are Success and Error. Required.
ErrorCodePGP/ErrorCode()	This is the exit value returned from executing PGP commands. This will be shown when the Status is 'Error'. Optional.
ErrorDescription (PGP/ ErrorDescription)	This is the error description based on the ErrorCode. This will be shown when the Status is 'Error'. Optional.

## Business Process Example - Decrypt Operation (Public Key Decryption)

The following business process uses the PGP Unpackage service to decrypt the primary document in the document area. The profile is based on PGP107. In this case, the default Command Line 2 adapter configuration, PGPCmdlineService, is used to execute the decrypt command. It uses the working directory, remote name and port stated in the business process. Therefore, these values will override any pre-configured values in PGPCmdlineService.

```
<process name="PGP_Decrypt ">
  <sequence name="optional">
    <operation name="One">
      <participant name=" PGPUnPackageService "/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>
        <assign to=" secret_keymap_name"> my_secret </assign>
        <assign to="workingDir">/server1/tmp</assign>
        <assign to="remoteName">00.000.00.000</assign>
        <assign to="remotePort">12345</assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>
```

## Business Process Example - Verify Operation

The following business process uses the PGP Unpackage service to verify the primary document in the document area. The profile is based on PGP107. In this case, the Command Line 2 adapter configuration called MyCLA2 is used to execute the commands. The remote name, port and working directory have been pre-configured in the service configuration. Therefore, they are not required in the business process.

```
<process name="PGP_Verify">
  <sequence name="optional">
    <operation name="One">
      <participant name="PGPUnPackageService "/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>
        <assign to="cmdline2svcname">MyCLA2</assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>
```

## Business Process Example - OnFault Handling

The following business process shows onFault handling with the PGP Unpackage service.

```
<process name="PGP_Decrypt">
  <sequence name="optional">
    <operation name="One">
      <participant name="PGPUnPackageService "/>
      <output message="Xout">
```

```

        <assign to="." from="*"></assign>
        <assign to="profile_name">PGP107</assign>
        <assign to=" secret_keymap_name"> si_secret </assign>
        <assign to="workingDir">/server1/tmp</assign>
        <assign to="remoteName">00.000.00.000</assign>
        <assign to="remotePort">12345</assign>
    </output>
    <input message="Xin">
        <assign to="." from="*"></assign>
    </input>
</operation>
<onFault>
    <assign to="Status">The file is decrypted successfully</assign>
</onFault>
<onFault>
    <assign to="Status">General Error Occurred</assign>
</onFault>
<onFault code="[PGPErrorCode] Decryption error">
    <assign to="Status">Decryption error</assign>
</onFault>
</sequence>
</process>

```

## Business Process Example - PGP Partner and PGP Sponsor

The following business process uses the PGP Partner and PGP Sponsor services to decrypt and verify documents.

```

<process name="use_partner_sponsor">
  <operation name="PGP Unpackage Service">
    <participant name="PGPUnpackageService"/>
    <output message="PGPUnpackageServiceTypeInputMessage">
      <assign to="pgp_partner_name">partner</assign>
      <assign to="pgp_sponsor_name">sponsor</assign>
      <assign to="profile_name">pgp</assign>
      <assign to="." from="*"></assign>
    </output>
    <input message="inmsg">
      <assign to="." from="*"></assign>
    </input>
  </operation>
</process>

```

## Advanced Status Messages

Exit Codes from E-Business Server and PGP Command Line Freeware

The following table contains exit codes from E-Business Server and PGP Command Line Freeware. The content of the description field will be displayed in the Advanced Status column, preceded by [PGPErrorCode]:

Status	Description
0	Exit OK, no error
1	Invalid file
2	File not found
3	Unknown file
4	Batch mode error
5	Bad argument
6	Process Interrupted
7	Out of memory error
8	Environment error

Status	Description
20	Signature error
21	Public Key Encryption error
22	Encryption error
23	Compression error
30	Signature Check error
31	Public Key Decryption error
32	Decryption error
33	Decompression error
34	Keyring locked error
101	File parsing error

## Exit Codes from PGP Command Line - PGP Corporation

The following table contains exit codes from PGP Command Line (version 9.5) from PGP Corporation. The content of the description field will be displayed in the Advanced Status column, preceded by [PGPErrorCode]:

Status	Description
0	PGP Command Line exited successfully.
64	Parser error.
71	Bad data was received from the operating system at startup.
128	An internal error occurred.
129	An initialization failure occurred on startup.
130	A user interrupt occurred.
145	Error purging a cache: passphrase, keyring, or both.
146	Error creating keyring files.
147	Error during a speed test operation.
160	Complete failure during a file wipe.
161	Partial fail, partial success during a file wipe (one file wiped, one not, for example).
162	Complete failure during an encode.
163	Partial failure during an encode.
164	Complete failure during a decode.
165	Partial failure during a decode.
210	Error during one of the key list operations.
220	Error during key maintenance.
221	Error when checking signatures.
222	Error when checking user IDs.
230	Error during one of the key edit operations.
240	Error during one of the key server operations.

Status	Description
245	Error with supplied license.
251	License is expired.
255	An unknown error occurred.

## Errors During Validation

The following table contains errors that result from the PGP Unpackage service when it validates information before executing PGP commands on the remote server. The content of the status field will be displayed in the Advanced Status column:

Status	Description
Error in accessing the document with a given DocumentId	The DocumentId value given in the bpml is incorrect.
Fail to get data from Primary Document	There is no Primary Document. Primary Document is mandatory.
You must enter one of these BPML Params: 'public_user' or 'secret_keymap_name' or 'conv_keymap_name'	Either one of the BPML Parameters must be present for PGP to encrypt, sign or encrypt and sign.
Incorrect Profile Name in BPML Param: 'profile_name'. It is not found in the PGP Server Manager	The profile_name value given in the bpml is incorrect.
Incorrect Key Name (BPML Param: 'secret_keymap_name'). It is not found in the PGP Profile's Secret KeyMap	The secret_keymap_name value given in the bpml is incorrect.
Incorrect Key Name (BPML Param: 'conv_keymap_name'). It is not found in the PGP Profile's Conventional KeyMap	The conv_keymap_name value given in the bpml is incorrect.

---

## Build 5102 or Higher

### EDI Encoder Service

**Note:** If the input document character encoding is specified, it overrides the encoding specified in the map. The output document content type and character encoding are set based on the information contained in the map.

The following table provides an overview of the EDI Encoder service:

System name	EDIEncoderType
Graphical Process Modeler (GPM) categories	<ul style="list-style-type: none"> <li>• All Services</li> <li>• EDI &gt; X12</li> <li>• EDI &gt; EDIFACT</li> <li>• EDI &gt; CII</li> <li>• EDI &gt; SWIFT</li> </ul>

System name	EDIEncoderType
Description	<p>Determines which transaction-level envelope will be used on the document. If translations are specified in an envelope, the service determines which map to use. Additionally, for the CHIPS standard, allows you to specify the Sender ID and/or Application Sender ID along with the Acceptor Lookup Alias, to allow for an envelope lookup for a document that is to be enveloped. For the Fedwire standard, allows you to specify the Sender ID and/or Application Sender ID, Receiver ID and/or Application Receiver ID, along with the Acceptor Lookup Alias, which allows for an envelope lookup for a document that is to be enveloped (outbound).</p> <p><b>Note:</b> In previous releases, the document lifespan default was zero so that when the workflow expired, all associated documents were purged/archived with the workflow. Now the lifespan is configurable for documents (the default is 30 days) and standards that use the EDI Encoder service.</p>
Preconfigured?	A configuration of this service is installed with the product, but is not configured. The only configuration required for the service is to specify parameter values to be used within a business process, but you must also define the envelopes within the application.
Requires third party files?	No
Platform availability	All supported application platforms.
Related services	EDI Envelope Service
Application requirements	No
Initiates business processes?	None
Invocation	Runs by a predefined business process.
Returned status values	<ul style="list-style-type: none"> <li>• Success - The envelope for the document was found and if the envelope specified a map, this information is passed to the EDI Envelope service.</li> <li>• Error - The envelope for the document could not be located.</li> </ul>
Restrictions	This service is used in outbound business processes only.

## Implementing the EDI Encoder Service

To implement the EDI Encoder service, complete the following tasks:

1. Create an EDI Encoder service configuration. For information, see *Managing Services and Adapters*.
2. Configure the EDI Encoder service. For information, see *EDI Encoder Service*.
3. Use the EDI Encoder service in a business process.



## Configuring the EDI Encoder

To configure the EDI Encoder service, you must specify settings for the following fields in the GPM:

Field	Description
Config	Name of the service configuration.
AcceptorLookupAlias	<p>Identifying string used with the sender ID (and/or Application Sender ID for CHIPS) and receiver ID (and/or Application Receiver ID for CHIPS) to look up this envelope. This alias associates a document with the service it requires. This same field is specified in the transaction-level outbound envelope. Also, this identifying string is used with the Sender ID and Receiver ID to look up this envelope for the Fedwire Outbound Envelope. Required.</p> <p><b>Note:</b> To specify this parameter in the CHIPS Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the CHIPS Outbound Envelope <b>Acceptor Lookup Alias</b> parameter.</p>
EDI Standard	Enter the EDI standard to be used (including CHIPS or Fedwire).
Mode	<p>Determines whether documents are enveloped immediately or deferred to be enveloped at a later time. Optional. The mode used here must correspond to the mode in which the EDI Envelope service will be called.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>• Immediate - The envelopes are determined and associated with the document to be used during enveloping. Assumes the EDI Envelope service will be used to envelope the document later in the process.</li> <li>• Deferred - The service marks the document to be enveloped at a later time, usually according to a schedule. The document is stored in the database until enveloping takes place. (Default)</li> </ul> <p><b>Note:</b> If the mode is not specified, the default will write an entry to the CORRELATION_SET table that the document needs to be enveloped. This makes it eligible for deferred enveloping.</p>

Field	Description
ReceiverID	<p>Receiver identification, 2 characters minimum, 15 maximum. Required. Must match the receiver ID in the transaction-level document envelope.</p> <p><b>Note:</b> To specify this parameter in the CHIPS Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the CHIPS Outbound Envelope <b>Receive Participant Number</b> parameter. To specify this parameter in the Fedwire Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the Fedwire Outbound Envelope <b>Receiver ID</b> parameter.</p>
SenderID	<p>Sender identification, 2 characters minimum, 15 maximum. Required. Must match the sender ID in the transaction-level document envelope.</p> <p><b>Note:</b> To specify this parameter in the CHIPS Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the CHIPS Outbound Envelope <b>Send Participant Number</b> parameter. To specify this parameter in the Fedwire Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the Fedwire Outbound Envelope <b>Sender ID</b> parameter.</p>
ReceiverIDQual	<p>Receiver ID qualifier. Optional. Must match the receiver ID qualifier in the transaction-level document envelope.</p>
SenderIDQual	<p>Sender ID qualifier. Optional. Must match the sender ID qualifier in the transaction-level document envelope.</p>
AppSenderID	<p>Coded identifier of the application data sender. Optional.</p> <p><b>Note:</b> To specify this parameter in the CHIPS Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the CHIPS Outbound Envelope <b>Application Sender ID</b> parameter. To specify this parameter in the Fedwire Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the Fedwire Outbound Envelope <b>Application Sender ID</b> parameter.</p>

Field	Description
AppReceiverID	Coded identifier of the customer number or data source number. Optional. <b>Note:</b> To specify this parameter in the CHIPS Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the CHIPS Outbound Envelope <b>Application Receiver ID</b> parameter. To specify this parameter in the Fedwire Outbound Envelope wizard to perform an envelope lookup for a document to be enveloped, type this value in the Fedwire Outbound Envelope <b>Application Receiver ID</b> parameter.

## Using Wildcards in Enveloping

As a way to help reduce the number of envelopes you need to create and use, the EDI Envelope and EDI De-envelope services support use of an asterisk (\*) as a wildcard character in mandatory envelope fields for X12, EDIFACT, CHIPS and Fedwire only. The exception to this rule is when the field is Sender ID, Receiver ID, or a qualifier for one of those fields. For example, in EDIFACT the following fields are conditional, but are considered to be part of the Sender / Receiver ID and therefore must have a "\*" placed in the field if you want to override those values:

- (0008) Interchange Sender Internal Identification
- (0042) Interchange Sender Internal Sub-identification
- (0014) Interchange Recipient Internal Identification
- (0046) Interchange Recipient Internal Sub-identification

By using wildcards, you can set up one set of envelopes that can be used for multiple trading partners. If certain trading partners have specific requirements, you can still have envelopes that pertain just to them, and the EDI Envelope service chooses the envelope that is the best match. In other words, the envelope that has the most matches to specific fields in the data (for example, Receiver ID, Receiver ID Qualifier), is the one selected.

## Document Tracking Levels and Performance

You can boost EDI performance in the application by using the TRACKING\_LEVEL parameter to adjust the tracking level for business processes.

You set the default global settings for the TRACKING\_LEVEL parameter in the enveloping.properties file. However, these global settings can be overridden for certain EDI-related services by using the BPML-only TRACKING\_LEVEL parameter. This enables you to obtain maximum EDI performance in some business processes and maximum search and tracking functionality in others. This parameter can be set for the following services:

Inbound:

- CII Deenvelope service
- EDIFACT Deenvelope service
- EDI Post Processor service

- X12 Deenvelope service
- Generic Deenvelope service

#### Outbound

- EDI Encoder service
- CII Envelope service
- EDIFACT Envelope service
- Envelope Generic service
- X12 Envelope service

This performance boost is done at the expense of Tracking and Search functionality. The tracking level setting affects the following EDI functionality:

- EDI Correlation Search
- EDI Document Tracking
- EDI Reporting

The TRACKING\_LEVEL parameter is not available in the application service configuration or in the GPM: it must be added manually to the BPML. Use the TRACKING\_LEVEL parameter with one of the following settings:

Setting	Description
none	Provides the best EDI performance with the least tracking and search functionality. EDI Correlation Search, EDI Document Tracking and EDI Reporting are nonfunctional.
basic	Provides a good EDI performance while also providing search functionality. EDI Correlation Search is functional. EDI Document Tracking and EDI Reporting are nonfunctional.
full	Default setting. Provides the lowest EDI performance with the highest search and tracking functionality. EDI Correlation Search, EDI Document Tracking and EDI Reporting are fully functional.

**Note:** Document tracking is turned off by default in the system-defined EDI business processes. If you define an EDI business process and turn Document Tracking on, that will override the TRACKING\_LEVEL settings in both the enveloping.properties file and the EDI service parameter.

## FTP Server Adapter

The following table provides an overview of the FTP Server adapter:

System name	FTP Server Adapter
Graphical Process Modeler (GPM) category	None
Description	This adapter receives and processes requests from external trading partners that are submitted using the FTP protocol. This adapter is used with a perimeter server.

Business usage	Use this adapter to put files into, or get files from, a mailbox.
Usage example	A trading partner uses an FTP client to retrieve a business document from a mailbox. The FTP Server adapter receives and processes the trading partner request.
Preconfigured?	A configuration of the FTP Server adapter is installed, but disabled by default. You can enable the preconfigured FTP Server adapter or create a new configuration.
Requires third party files?	Certicom SSL Library provided
Platform availability	All supported platforms
Related services	None
Application requirements	To log in to the FTP server, you must have permission to your virtual root (either explicitly assigned or defaulted). To access a mailbox, you must have permission to that mailbox and all mailboxes between it and your virtual root. If a user exceeds the maximum number of failed login attempts, the FTP Server adapter locks the user out. The lock must be reset before the user can access the server again.
Initiates business processes?	The FTP Server adapter does not directly initiate business processes. However, mailbox activities can trigger routing rules.
Invocation	Not used in business processes
Business process context considerations	None
Returned status values	None

Restrictions	<p>Restrictions:</p> <ul style="list-style-type: none"> <li>• FTP Server is tightly integrated with the application's mailbox system. An FTP client can only access the mailbox that is assigned to its user account.</li> <li>• FTP Server does not support all functions specified in RFC 0959 (Standard FTP Server). Basic functions are supported to integrate with the mailbox system, such as list message and sub-mailbox, send and extract message to/from mailbox.</li> <li>• FTP Server is not integrated with business process invocation when processing a request from a client.</li> <li>• The home directory for FTP is a virtual root mailbox. Mailboxes include both extractable and nonextractable messages. When accessing a mailbox using the FTP Server adapter, only extractable messages are displayed. To change this default behavior, edit the ftpserver.properties file and set listUnextractables=true (default is false).</li> <li>• The timeout value for a control channel connection is controlled by a parameter in the ftpserver.properties file. The default timeout value is 600 seconds. The minimum value is 60 seconds. If the control channel is idle longer than the timeout value, the session is terminated, unless the data channel is open (whether or not data is being transferred).</li> <li>• To access the FTP Server adapter and have full mailbox operations (listing, retrieving, and placing messages), you must have permission to the virtual root (either explicitly assigned or default). To operate fully on mailboxes in the hierarchy directory, you must have permissions on all mailboxes between the target mailbox and the virtual root.</li> <li>• Restricted operation can be granted to users with a parameter named <b>MailboxLoginWithoutVirtualRootPermission</b>. With this permission, you can log in and list files in a mailbox, but cannot retrieve or place files. This restricted permission only applies to the virtual root mailbox and does not impact operation on submailboxes.</li> </ul>
Persistence level	None. This adapter does not have a pre-set persistence level.

Testing considerations	<p>At application startup, attempt to access the FTP server using a supported FTP client with the configured IP address and port. Debug information can be found in the FTP logs. Select Logging Level from the following:</p> <ul style="list-style-type: none"> <li>• Error – Errors only</li> <li>• Communication Trace – Errors, requests from clients, and responses from the Server adapter, including ACL violations</li> <li>• All - for debugging, all activities</li> </ul>
------------------------	---

## Implementing the FTP Server Adapter

To implement the FTP Server adapter, complete the following tasks:

1. Create an FTP Server adapter configuration (or enable the installed configuration and edit parameters as needed).
2. Configure the FTP Server adapter.

## Configuring the FTP Server Adapter

To configure the FTP Server adapter, you must specify settings for the following fields:

Field	Description
Name	Unique and meaningful name for the adapter configuration. Required.
Description	Meaningful description for the adapter configuration. Required.
Select a Group	Not applicable for this adapter. Do not change default value.
FTP Server Listen Port	Port number that the FTP Server should bind to and listen on for connection requests. The default value depends on your system platform and on configuration. Required.
Active Data Port Range	<p>Range of ports the server can allocate for the transfer of data to or from the FTP client in active mode. Optional. Example values are:</p> <ul style="list-style-type: none"> <li>• 1024-2048</li> <li>• 2222</li> <li>• 3000-4000</li> </ul> <p><b>Note:</b> You can enter double ranges separated by commas, as shown in this example: 10500-10599,10700-10799. If left blank, the server selects available system ports.</p>

Field	Description
Passive Data Port Range	<p>Range of ports the server can allocate for the transfer of data to or from the FTP client in passive mode. Optional. Example values are:</p> <ul style="list-style-type: none"> <li>• 1024-2048</li> <li>• 2222</li> <li>• 3000-4000</li> </ul> <p><b>Note:</b> You can enter double ranges separated by commas, as shown in this example: 10500-10599,10700-10799. If left blank, the server will choose available system ports.</p>
Perimeter Server	<p>Select a perimeter server from the list. Default is node1 and local. Required.</p> <p><b>Note:</b> You should use a specific external interface for communications with trading partners. Using a wildcard address can cause problems with FTP sessions. If another process binds the port used for the data channel on an interface, it may receive connections intended for the data channel. Using a specific TCP/IP address or DNS name prevents this from occurring.</p>
Transfer Buffer Size (bytes)	<p>Specifies the size in bytes of the buffer used when transferring a file. Required. Valid values are 0 to 9,999,999,999. Default is 32000.</p>
Minimum Number of Threads	<p>Tuning parameter indicating the range of threads available for handling events to improve performance. Must be less than or equal to the Maximum Number of Threads value. Default is 3. Required.</p> <p><b>Note:</b> Do not change the default value unless instructed otherwise by Sterling Commerce support.</p>
Maximum Number of Threads	<p>Tuning parameter indicating the range of threads available for handling events to improve performance. Must be greater than or equal to the Minimum Number of Threads value. Default is 6. Required.</p> <p><b>Note:</b> Do not change the default value unless instructed otherwise by Sterling Commerce support.</p>
NAT Address	<p>Specifies the NAT IP address the FTP server should send to the user FTP client in passive connection mode. Optional. Overrides the global NAT address specified in the ftpserver.properties file.</p>
Maximum Logins	<p>Maximum number of logins the adapter may have active at any time. If no value is specified, logins are unlimited. Optional. Valid value is any integer to 9999999999.</p>



Field	Description
Maximum Logins per user	Maximum number of logins each user may have active on this adapter at any point of time. If no value is specified, logins are unlimited. Optional. Valid value is any integer to 9999999999.
Document Storage	<p>Indicates whether the body of the request document must be stored on the file system or in the database. Valid values are:</p> <ul style="list-style-type: none"> <li>• System Default – If your system administrator has changed the default value, this ensures the correct location is used.</li> <li>• Database – Body of the request document will be stored in the database.</li> <li>• File System (default) – This is the default value, but it can be changed. Contact your system administrator to see if the default has been changed.</li> </ul> <p>Required.  <b>Note:</b> For more information about document storage types, see <i>Managing Services and Adapters</i>.</p>
Should the adapter be restricted to a certain group of users?	Select Yes or No to indicate whether to restrict access to the FTP server. Required. Default is No. If Yes, select Users and or Groups from the lists on subsequent pages.
Should the restricted users be assigned a specific range of ports?	Select Yes or No to indicate whether to assign a specific port, range, or range of ports to users. Required. Default is No. If Yes, specify <i>User Active Ports</i> , <i>User Passive Ports</i> , <i>Group Active Ports</i> , and or <i>Group Passive Ports</i> on subsequent pages. You can specify any or all of these fields.
Should users start in the directory that matches their user name upon login?	<p>Places the user, upon logging in, into a directory (mailbox) that corresponds to their user ID. Valid values are:</p> <ul style="list-style-type: none"> <li>• Yes – Upon login, the user is automatically placed in a directory that matches their user ID. If such a directory is not available, the user is placed in the virtual root directory. This option allows Connect:Enterprise UNIX customers to run production scripts that require each user to be placed into directories that correspond to their user ID. <b>Caution:</b> Do not select Yes if any user IDs differ only by case (example: jsmith and JSmith). Unlike user IDs, mailbox names are not case-sensitive.</li> <li>• No – User is placed in the virtual root directory.</li> </ul>
Users	Select a list of users who are granted permission to access the server.

Field	Description
Groups	Select a list of groups who are granted permission to access the server.
User Active Ports	Any port number or a range of port numbers to be used as ACTIVE port. Valid values are valid, available port numbers or a range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Optional. Examples of valid values are: <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
User Passive Ports	Any port number or a range of port numbers to be used as PASSIVE port. Valid values are valid, available port numbers or a range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Optional. Examples of valid values are: <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
Group Active Ports	Any port number or a range of port numbers to be used as ACTIVE port. Valid values are valid, available port numbers or a range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Optional. Examples of valid values are: <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
Group Passive Ports	Any port number or a range of port numbers to be used as PASSIVE port. Valid values are valid, available port numbers or range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Optional. Examples of valid values are: <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
Extractable Count	The number of times the message can be extracted. Cannot be specified in conjunction with Extractable or Extractable For. Valid value is any integer. Optional.
Extractable For	Indicates the length of time (in days, hours and minutes) the message can be extracted. Cannot be specified in conjunction with Extractable or Extractable Count. Valid value is in the format <i>dddhhmm</i> . Optional.

Field	Description
Extractable	Whether the message can be extracted. Cannot be specified in conjunction with Extractable Count or Extractable For. Valid values are Yes and No. Default is Yes. Optional.
SSL	Whether Secure Sockets Layer (SSL) is active. Required. Valid values are: <ul style="list-style-type: none"> <li>• None – If SSL is requested by a client it will be rejected (default)</li> <li>• Optional – SSL is used if requested by a client</li> <li>• Must – Clients that do not request SSL are not allowed to authenticate</li> </ul> <b>Note:</b> If Optional or Must is selected, the asset protection key must enable SSL for the appropriate protocol.
Key Certificate Passphrase	Password that protects the server key certificate. Used to encrypt and decrypt messages. Required if SSL option is Must or Optional.
Cipher Strength	Strength of the algorithms used to encrypt data. Required if SSL option is Must or Optional. Valid values are: <ul style="list-style-type: none"> <li>• ALL</li> <li>• WEAK – Often required for international e-commerce, because government regulations prohibit STRONG encryption from being exported</li> <li>• STRONG – Default</li> </ul>
Key Certificate (System Store)	Private key and certificate for server authentication. Used to encrypt and decrypt messages. Required if SSL option is Must or Optional.
CA Certificates	Certificate used to validate the certificate of an FTP client. This is the public key. If no CA certificate is chosen, no client certification is performed. Optional.
Clear Command Channel	Indicates that communication across the command channel is not encrypted after authentication is completed. Optional.

## FTP Server Functions Supported

The following table lists the FTP functions that are supported with the FTP Server adapter:

Category	Commands Supported
Access Control commands	<ul style="list-style-type: none"> <li>• USER – User name</li> <li>• PASS – Password</li> <li>• CWD – Change Working Directory</li> <li>• CDUP – Change to Parent Directory</li> <li>• QUIT – Logout</li> </ul>
Transfer Parameter Commands	<ul style="list-style-type: none"> <li>• PORT – Data port</li> <li>• PASV – Passive mode</li> <li>• TYPE – Representation type (ASCII and Binary )</li> <li>• STRU – File Structure (File )</li> <li>• MODE – Transfer mode (Stream )</li> </ul>
Service Commands	<ul style="list-style-type: none"> <li>• DELE – Delete</li> <li>• RETR – Retrieve</li> <li>• STOR – Store</li> <li>• ABOR – Abort</li> <li>• PWD – Print Working Directory</li> <li>• XPWD – Print Working Directory (legacy format)</li> <li>• LIST – List</li> <li>• NLST – Name List</li> <li>• HELP – Help</li> <li>• NOOP – No Operation</li> <li>• RNFR – Rename From</li> <li>• RNT0 – Rename To</li> <li>• SITE – Site Parameter (CPWD and HELP)</li> <li>• SYST – System</li> <li>• MDTM – Last-modified time of a given file on a remote host</li> <li>• SIZE – Return size of a remote file</li> </ul>
Security Commands	<ul style="list-style-type: none"> <li>• AUTH – Authentication/Security Mechanism</li> <li>• CCC – Clear Command Channel</li> <li>• PBSZ – Protect Buffer Size</li> <li>• PROT – Data Channel Protection Level</li> <li>• REST – Restart</li> </ul>

## FTP Server Functions Not Supported

The following table lists the FTP functions that are not supported with the FTP Server adapter:

Category	Commands Not Supported
Access Control commands	<ul style="list-style-type: none"> <li>• ACCT – Account</li> <li>• SMNT – Structure Mount</li> <li>• REIN – Re-initialize</li> </ul>

Category	Commands Not Supported
Transfer Parameter Commands	<ul style="list-style-type: none"> <li>• TYPE – Representation type (EBCDIC and Local Byte )</li> <li>• STRU – File Structure (Record and Page)</li> <li>• MODE – Transfer mode (Block and Compressed )</li> </ul>
Service Commands	<ul style="list-style-type: none"> <li>• STOU – Store Unique</li> <li>• APPE – Append</li> <li>• ALLO – Allocate</li> <li>• RMD – Remove Directory</li> <li>• MKD – Make Directory</li> <li>• STAT – Status</li> </ul>

## Activity Types for the FTP Server Adapter

This adapter reports the following activities to the Services Controller for activity monitoring:

- PUT – Adds a file to a mailbox
- GET – Retrieves a file from a mailbox
- Session – Records all activity after connection

## User Exits

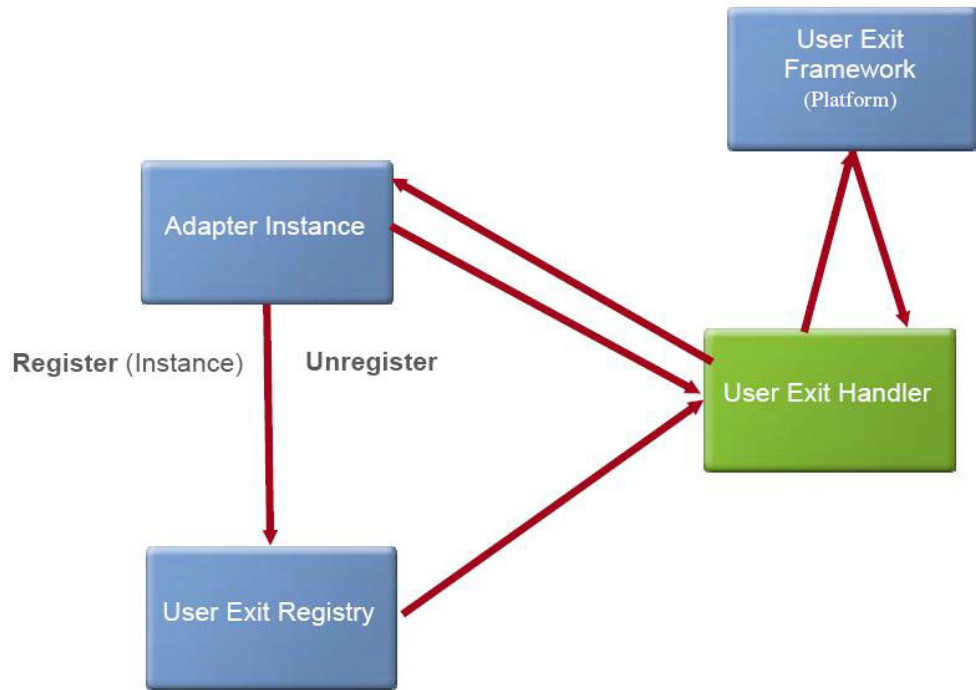
User exits are a set of predefined points that allow you to implement customized functions by adding custom code to perform a desired operation, thereby extending the functionality of the adapter.

The User Exit framework consists of the following components, plus a handler that interacts with all the components to perform the desired task:

- Adapter or service that needs to use the execution framework
- User exit registry that can be queried for all user exits configured for a particular adapter instance. All user exits are registered and maintained in this registry.
- User exit execution framework that allows you to obtain the references to the user exit implementation and to execute the user exit

The handler's reference is maintained by the adapter, which refers to the registry and the execution framework.

The following figure shows the user exit architecture:



The following table provides the generic properties that are defined for a user exit:

Property	Description
Implementations	<p>Contains the list of custom code implementation classes that must be invoked when a user exit is executed.</p> <p>The implementation classes are invoked in the order they were added. If a user exit implementation fails, the next user exit implementation in the chain is not invoked.</p>
return.on.exception	<p>Determines the result if an exception occurs when a user exit is being executed.</p> <p>You should set the value to false only if the user exit is critical and displays a failure.</p>
pool.size (integer value 1 - 10)	<p>These properties are used to manage thread pools for executing the user exits.</p>
maximum.queue.length (integer value 1 – 100)	
wait.time (integer value 1 - 600) in seconds	

## Configuring User Exits

The following user exit points are defined in the FTP Server Adapter:

- `com.sterlingcommerce.woodstock.userexit.services.ftpserver.interfaces.IFtpServerUserExit_OnFileReceiveBeforeCommit`
- `com.sterlingcommerce.woodstock.userexit.services.ftpserver.interfaces.IFtpServerUserExit_OnCwdCommandBeforeExecute`
- `com.sterlingcommerce.woodstock.userexit.services.ftpserver.interfaces.IFtpServerUserExit_OnUnknownSiteSubCommand`

The interfaces are provided through separate jar files present in the `install_dir/install/userexit/jars` (`install_dir\install\userexit\jars` for Windows) directory.

Perform the following tasks to configure user exit points:

1. Write the code to implement the interface for the desired point.
2. Add the custom code classes to a .jar file.
3. Add the path of the .jar file to the `dynamicclasspath.cfg` file in the `install_dir/install/properties` (`install_dir\install\properties` for Windows) directory.
4. Restart Sterling Integrator.
5. Navigate to the `install_dir/properties/userexit` (`install_dir\properties\userexit` for Windows) directory and locate `FtpServerUserExits.xml` file.
6. Edit `FtpServerUserExits.xml` file and add an entry for each implementation as shown. The user exits are executed in the same order as they appear.

```
<bean id="com.sterlingcommerce.woodstock.userexit.services.ftpserver.
interfaces.
IFtpServerUserExit_OnCwdCommandBeforeExecute"
class="com.sterlingcommerce.woodstock.
userexit.services.
ftpserver.FtpServerUserExit">
  <property name="implementations">
    <list>
      <value>implementation1</value>
      <value> implementation2</value>
    </list>
  </property>
  <property name="generalParameters">
    <props>
      <prop key="return.on.exception">false</prop>
      <prop key="pool.size">5</prop>
      <prop key="maximum.queue.length">5</prop>
      <prop key="wait.time">10</prop>
      <prop key="execution.threshold.time">600000</prop>
    </props>
  </property>
</bean>
```

Remove all values to deactivate the user exit points.

7. Restart the FTP Server adapter instance to apply the changes.

**Note:** Restart only the adapter instance if you modify implementation class list and other properties.

## Image Cash Letter Join Service

The Image Cash Letter Join service inserts variable length binary images (Type52 records) into Image Cash Letter documents. This service is typically used after translation to join the binary images previously split out by the Image Cash Letter Split service.

**Note:** This service does not enforce or validate the standard.

The following table provides an overview of the Image Cash Letter Join service:

System name	ImageCashLetterSplit
Graphical Process Modeler (GPM) categories	<ul style="list-style-type: none"> <li>• All Services</li> <li>• EDI</li> </ul>

<b>System name</b>	<b>ImageCashLetterSplit</b>
Description	The default behavior is to read through the PrimaryDocument looking for binary image data placeholder records (inserted by the Image Cash Letter Split service) and, if found, join the corresponding binary image back into the Image Cash Letter document. Alternatively, this service can be used to insert binary images based on truncated Type52 records (only contains fields 1-17).
Preconfigured?	A configuration of this service is created when the product is installed.
Requires third party files?	No
Platform availability	All supported application platforms
Related services	Image Cash Letter Split service
Application requirements	No
Initiates business processes?	None
Invocation	Runs as part of a business process.
Returned status values	<ul style="list-style-type: none"> <li>• Success (this status value is returned if the service successfully joined the binary images into the document)</li> <li>• Error (see below for list of errors) <ol style="list-style-type: none"> <li>1. Not licensed for use</li> <li>2. No Primary Document or zero bytes</li> <li>3. No Placeholder records found</li> <li>4. No Type52 records found</li> <li>5. Missing Type52 record for image</li> <li>6. Missing Type52 record after Type50</li> <li>7. Invalid record length</li> <li>8. Image document not found</li> </ol> </li> </ul>
Restrictions	No

## Implementing the Image Cash Letter Join Service

To implement the Image Cash Letter Join service, you just need to use the Image Cash Letter Join service in a business process.

### Parameters Passed From Business Process to Service

The following table contains the parameters passed from the business process to the Image Cash Letter Join service:

Parameter	Description
join_bufferSize	This is the size of the buffer for reading data. If not specified, the default is 2048.
join_encoding	This specifies the encoding of the input PrimaryDocument. If not specified, the PrimaryDocument encoding is used (if set) or the system default is used.



Parameter	Description
join_inputRecLen	<p>This indicates whether the input PrimaryDocument contains a record length for each record. If not specified, it defaults to true (indicating that the input contains the record length).</p> <p><b>Note:</b> The record length is always written to the output PrimaryDocument.</p>
join_inputRecSepNum	<p>This indicates whether the input PrimaryDocument contains record separators. If not specified, the default is zero (no separators). This behavior can be overridden by changing the value of this parameter (for example, if the file uses CR/LF record separator, set this parameter to <b>split_inputRecSepNum=2</b>).</p>
join_outputRecSeps	<p>This indicates whether each record written to the output PrimaryDocument will be followed by a record separator. If not specified, the default is none (no record separators). If you want each record written with a record separator, you must do so using two-byte hex characters (for example, <b>split_outputRecSeps='0D0A'</b> indicates the separator used is the carriage return/line feed).</p>
join52	<p>This indicates whether the service looks for placeholder records or Type52 records for image replacement. If not specified, it defaults to false, which instructs the service to look for placeholder records previously inserted by the Image Cash Letter Split service. If you want the service to use Type52 records, you must set this parameter to true. Furthermore, the Type52 records must contain fields 1-17 only and this service will fill in field18 (length of image data) and field19 (the image data). The images to be joined using the "join52=true" option must be in the ProcessData tree as follows:</p> <pre data-bbox="967 1451 1127 1734"> &lt;ProcessData&gt; &lt;Images&gt; &lt;Image1/&gt; &lt;ImageN/&gt; &lt;/Images&gt; &lt;/ProcessData&gt; </pre>
errorIfNothingToJoin	<p>This determines whether an error is returned if no placeholder or Type52 records are found in the PrimaryDocument. The default is true (return an error if no placeholder or Type52 records are found), unless otherwise specified.</p>

## Image Cash Letter Split Service

The Image Cash Letter Split service removes variable length binary images (Type52 records) from Image Cash Letter documents. This service is typically used before translation.

**Note:** This service does not enforce or validate the standard.

The following table provides an overview of the Image Cash Letter Split service:

System name	ImageCashLetterSplit
Graphical Process Modeler (GPM) categories	<ul style="list-style-type: none"> <li>All Services</li> <li>EDI</li> </ul>
Description	Removes variable length binary images (Type52 records) from Image Cash Letter documents. This service is typically used before translation and it replaces the Type52 record with a fixed length placeholder record that begins with   <b>CheckImage</b> followed by a number of the image file created in ProcessData (for example,  CheckImage1,  CheckImage2, and so forth). This default behavior can be changed to strip Type52 records and the image data separately by setting the workflow parameter <b>split52=true</b> . In this case, the textual portion of the record is added as an attribute of the image document.
Preconfigured?	A configuration of this service is created when the product is installed.
Requires third party files?	No
Platform availability	All supported application platforms
Related services	Image Cash Letter Join service
Application requirements	No
Initiates business processes?	None
Invocation	Runs as part of a business process.
Returned status values	<ul style="list-style-type: none"> <li>Success (this status value is returned if the service successfully splits the binary images from the document)</li> <li>Error (see below for list of errors) <ol style="list-style-type: none"> <li>Not licensed for use</li> <li>No Primary Document or zero bytes</li> <li>Unexpected record type</li> <li>Invalid record length</li> <li>No Type52 records found</li> </ol> </li> </ul>
Restrictions	No

## Implementing the Image Cash Letter Split Service

To implement the Image Cash Letter Split service, you just need to use the Image Cash Letter Split service in a business process.

## Parameters Passed From Business Process to Service

The following table contains the parameters passed from the business process to the Image Cash Letter Split service:

Parameter	Description
split_bufferSize	This is the size of the buffer for reading data. If not specified, the default is 2048.
split_encoding	This specifies the encoding of the input PrimaryDocument. If not specified, the PrimaryDocument encoding is used (if set) or the system default is used.
split_inputRecSepNum	This indicates whether the input PrimaryDocument contains record separators. If not specified, the default is zero (no separators). This behavior can be overridden by changing the value of this parameter (for example, if the file uses CR/LF record separator, set this parameter to <b>split_inputRecSepNum=2</b> ).
split_outputRecSeps	This indicates whether each record written to the output PrimaryDocument will be followed by a record separator. The default record separator used is hex 0x0A(line feed). If you want to specify a different record separator, you must do so using two-byte hex characters (for example, split_outputRecSeps="0D0A" indicates the separator used is carriage return/line feed).
split_outputRecLen	This indicates whether the record lengths will be written to the output PrimaryDocument for each record. If not specified, it defaults to true (the record lengths are written to the output PrimaryDocument for each record).
split52	This specifies whether the Type52 record is removed from the PrimaryDocument as one entity. If not specified, it defaults to false. If you want the Type 52 record and image data removed separately, you must set this parameter to true (which will add the textual portion of the record as an attribute of the image document).
errorIfNothingToSplit	This determines whether an error is returned if no Type52 records are found in the PrimaryDocument. The default is true (return an error if no Type52 records are found), unless otherwise specified.

## SFTP Client GET Service

The following table provides an overview of the SFTP Client GET service:

System name	SFTP Client GET Service
Graphical Process Modeler (GPM) category	All Services, B2B Protocols > SFTP Client

Description	This service is used to retrieve one or more documents from a specified directory on the trading partner's SFTP server.
Business usage	Use this service to retrieve one or more documents from a trading partner and move them into Sterling Integrator when the SFTP protocol is required as the transport mechanism.
Usage example	A business process is executed to retrieve a specified file or files from the external trading partner. Sterling Integrator uses the SFTP Client GET service, working through the SFTP Client adapter, to retrieve a file or files from a specified directory on the trading partner system.
Preconfigured?	Yes. To implement, use the preconfigured service in a business process.
Requires third party files?	No
Platform availability	All Sterling Integrator supported platforms
Related services	The following services are related. Configured in a business process, they initiate the SFTP Client adapter to perform their operations: <ul style="list-style-type: none"> <li>• SFTP Client Begin Session service</li> <li>• SFTP Client CD service</li> <li>• SFTP Client DELETE service</li> <li>• SFTP Client End Session service</li> <li>• SFTP Client GET service</li> <li>• SFTP Client LIST service</li> <li>• SFTP Client MOVE service</li> <li>• SFTP Client PUT service</li> <li>• SFTP Client PWD service</li> </ul>
Application requirements	An SFTP Server at the external trading partner location
Initiates business processes?	No
Invocation	This service is invoked from a business process.
Business process context considerations	None
Returned status values	0 – Success, 1 – Error
Restrictions	None
Persistence level	System default
Testing considerations	To test this service, run the SFTPClientDemoAllServices business process and verify that it completes successfully. For more information about the SFTPClientDemoAllServices business process, see the <i>SFTP Client adapter</i> documentation. For further information, go to Operations > System > Logs > SFTP Client Adapter and Services

## Input from Business Process to Service

The following table contains the parameters passed from the business process to the SFTP Client GET service:

Field	Description
RemoteFileName	Name of the file to be retrieved from the remote trading partner. Optional. You cannot use this parameter if RemoteFilePattern is specified. <b>Note:</b> Either RemoteFileName or RemoteFilePattern must be specified. Both cannot be left blank.
ResponseTimeout	Maximum number of seconds it can take for the trading partner system to respond before the session times out and terminates. If a number less than 30 is specified, 30 seconds will be used. Optional. Default is the ResponseTimeout value specified in the SFTP Client Begin Session service.
SessionToken	Returned SessionToken from the Begin Session service. Required.
RemoteFilePattern	File filter pattern. Using this field activates multiple-get mode. Optional. You cannot use this parameter if RemoteFileName is specified. <b>Note:</b> Either RemoteFileName or RemoteFilePattern must be specified. Both cannot be left blank.
RetrieveErrorSetSuccess	SFTP Client Get service will succeed in case of any error when RetrieveErrorSetSuccess field is set to YES. Optional. Valid values are YES and NO.

## Output from Service to Business Process

The following table contains the parameters passed from the SFTP Client GET service to the business process:

Parameter	Description
ServiceStartTime	Date/time stamp for when the service started
DocumentId	Provides information about the file retrieved as a result of the GET service.

Parameter	Description
ServerResponse	SFTP server response, which may include a reply code and any text associated with the reply code. Valid values are: <ul style="list-style-type: none"> <li>• 0 - OK</li> <li>• 1 - End of File</li> <li>• 2 - No Such File</li> <li>• 3 - Permission Denied</li> <li>• 4 - General Failure</li> <li>• 5 - Bad Message</li> <li>• 6 - No Connection</li> <li>• 7 - Connection Lost</li> <li>• 8 - Operation Unsupported</li> </ul>
ServiceEndTime	Date/time stamp for when the service ended
Primary Document	File retrieved as a result of the GET service

## Business Process Example

The following business process excerpts illustrate using the SFTP Client GET service:

- Process to get a binary file named FileNameToGet from the server

[[Insert begin session here]]

```
<operation name="SFTP Client GET Service">
  <participant name="SFTPClientGet"/>
  <output message="SFTPClientGetServiceTypeInputMessage">
    <assign to="RemoteFileName" >FileNameToGet</assign>
    <assign to="SessionToken" from="SFTPClientBeginSessionServiceResults/
SessionToken/text()"></assign>
  </output>
  <input message="inmsg">
    <assign to="SFTPClientGetServiceResults" from="*"></assign>
  </input>
</operation>
```

[[Insert end session here]]

- Process using a multiple get command

[[Insert begin session here]]

```
<operation name="SFTP Client Multiple GET Service">
  <participant name="SFTPClientGet"/>
  <output message="SFTPClientGetServiceTypeInputMessage">
    <assign to="RemoteFilePattern">*.txt</assign>
    <assign to="SessionToken"
from="SFTPClientBeginSessionServiceResults/SessionToken/text()"></assign>
  </output>
  <input message="inmsg">
    <assign to="SFTPClientGetServiceResults" from="*"></assign>
  </input>
</operation>
```

[[Insert end session here]]

## Correlations and Document Tracking

The following table details the correlations available from the SFTP Client GET service for document tracking:

Key	Values
ACTION	Get, Put
Direction	Inbound, Outbound
Protocol	SFTP
RemoteHostAddress	remoteAddress
RemoteHostName	remoteHost
Username	username
RemoteFile	filename

## SFTP Client PUT Service

The following table provides an overview of the SFTP Client PUT service:

System name	SFTP Client PUT Service
Graphical Process Modeler (GPM) category	All Services, B2B Protocols > SFTP Client
Description	Used to place a document or documents in a specified directory on the trading partner's SFTP server.
Business usage	Use this service to transfer a document or documents from Sterling Integrator to a trading partner when the SFTP protocol is required as the transport mechanism.
Usage example	A business process is executed that translates a document or documents to send to a trading partner. After the translation, Sterling Integrator uses the SFTP Client PUT service, working through the SFTP Client adapter, to place the document or documents in a specified directory on the trading partner system.
Preconfigured?	Yes. To implement, use the preconfigured service in a business process.
Requires third party files?	No
Platform availability	All Sterling Integrator supported platforms

Related services	<p>The following services are related. Configured in a business process, they initiate the SFTP Client adapter to perform their operations:</p> <ul style="list-style-type: none"> <li>• SFTP Client Begin Session service</li> <li>• SFTP Client CD service</li> <li>• SFTP Client DELETE service</li> <li>• SFTP Client End Session service</li> <li>• SFTP Client GET service</li> <li>• SFTP Client LIST service</li> <li>• SFTP Client MOVE service</li> <li>• SFTP Client PUT service</li> <li>• SFTP Client PWD service</li> </ul> <p>The SFTP Client PUT service must be placed between an SFTP Begin Session service and an SFTP End Session service. It may be used to put a document that is returned from an SFTP Client GET service.</p>
Application requirements	An SFTP Server at the external trading partner location
Initiates business processes?	No
Invocation	This service is invoked from a business process.
Business process context considerations	None
Returned status values	0 – Success, 1 – Error
Restrictions	None
Persistence level	System default
Testing considerations	To test this service, run the SFTPClientDemoAllServices business process and verify that it completes successfully. For more information about the SFTPClientDemoAllServices business process, see the <i>SFTP Client adapter</i> documentation. For debugging information, go to Operations > System > Logs > SFTP Client Adapter and Services

## Input from Business Process to Service

The following table contains the parameters passed from the business process to the SFTP Client PUT service:



Field	Description
DocumentId	Document ID to PUT to the remote server. A single DocumentId can appear directly in the message to the service or any number of DocumentIds can appear under the DocumentList element. Optional. <b>Note:</b> The SFTP Client PUT service will use DocumentList if a list is provided. If no list is specified in DocumentList, the service will use DocumentId. The service will not use both DocumentList and DocumentId. If no values are specified for either DocumentList or DocumentId, the service will PUT the primary document to the remote server.
RemoteFileName	Name of the file used to place the document on the remote trading partner server. If not specified, the name of the document will be used. Optional.
ResponseTimeout	Maximum number of seconds it can take for the trading partner system to respond before the session times out and terminates. If a number less than 30 is specified, 30 seconds will be used. Optional. Default is the ResponseTimeout value specified in the SFTP Client Begin Session service.
SessionToken	Returned SessionToken from the Begin Session service. Required.
Primary Document	File transferred as a result of the PUT service.
DocumentList	List of documents to PUT to the remote server. Each item must be a DocumentId. A list could look like the following example: <pre>&lt;DocumentList&gt;   &lt;DocumentId&gt;12345&lt;/DocumentId&gt;   &lt;DocumentId&gt;67890&lt;/DocumentId&gt; &lt;/DocumentList&gt;</pre>
UseDocBodyName	Specifies whether to use document body name as the remote file name. This parameter is only use in MPUT operation. Optional.  Valid values are: <ul style="list-style-type: none"> <li>• Yes – Use document body name</li> <li>• No – (Default) Use document name</li> </ul>

## Output from Service to Business Process

The following table contains the parameters passed from the SFTP Client PUT service to the business process:

Parameter	Description
ServerResponse	<p>The SFTP server response, which may include a reply code and any text associated with the reply code. Valid values are:</p> <ul style="list-style-type: none"> <li>• 0 - OK</li> <li>• 2 - No Such File</li> <li>• 3 - Permission Denied</li> <li>• 4 - General Failure</li> <li>• 5 - Bad Message</li> <li>• 6 - No Connection</li> <li>• 7 - Connection Lost</li> <li>• 8 - Operation Unsupported</li> </ul>

## Business Process Example

The following business process excerpt uses the SFTP Client Adapter to send the primary document from Sterling Integrator to the remote SFTP server using the SFTP Client PUT service:

[[Insert Begin Session]]

```

<operation name="SFTP PUT SERVICE">
  <participant name="SFTPClientPut"/>
  <output message="PutRequest">
    <assign to="SessionToken"
      from="/ProcessData/SftpBeginSessionServiceResults/SessionToken/text() ">
    </assign>
    <assign to="RemoteFileName">FilenameToPut</assign>
    <assign to="." From="PrimaryDocument"></assign>
  </output>
  <input message="inmsg">
    <assign to="SftpPutServiceResults" from="*"></assign>
  </input>
</operation>

```

[[Insert End Session]]

The following business process excerpt uses the SFTP Client Adapter to send a document received from a GET from Sterling Integrator to the remote SFTP server:

[[Insert Begin Session]]

```

<operation name="Get">
  <participant name="SFTPClientGet"/>
  <output message="GetRequest">
    <assign to="SessionToken"
      from="/ProcessData/SftpBeginSessionResults/SessionToken/text() ">
    </assign>
    <assign to="RemoteFileName">FilenameToGet</assign>
  </output>
  <input message="GetResults">
    <assign to="GetResults" from="DocumentId"/>
  </input>
</operation>
<operation name="Put">
  <participant name="SFTPClientPut"/>
  <output message="PutRequest">
    <assign to="SessionToken"
      from="/ProcessData/SftpBeginSessionResults/SessionToken/text() ">
    </assign>
    <assign to="." From="/ProcessData/GetResults/DocumentId"/>
  <input message="SftpPutResults">

```

```

        <assign to="PutResults" from="*"></assign>
    </input>
</operation>
[[Insert End Session]]

```

The following business process uses the SFTP Client adapter to send all documents received from a GET operation from Sterling Integrator to the remote SFTP server:

```

[[Insert Begin Session]]
<operation name="Get">
<participant name="SFTPClientGet"/>
<output message="GetRequest">
<assign to="SessionToken"
from="/ProcessData/SftpBeginSessionResults/SessionToken/text()">
</assign>
<assign to="RemoteFilePattern">*. *</assign>
</output>
<input message="GetResults">
<assign to="GetResults" from="DocumentList"/>
</input>
</operation>
<operation name="Put">
<participant name="SFTPClientPut"/>
<output message="PutRequest">
<assign to="SessionToken"
from="/ProcessData/SftpBeginSessionResults/SessionToken/text()">
</assign>
<assign to="." From="/ProcessData/GetResults/DocumentList"/>
<input message="SFtpPutResults">
<assign to="PutResults" from="*"></assign>
</input>
</operation>
[[Insert End Session]]

```

## Correlations and Document Tracking

The following table details the correlations available from the SFTP Client PUT service for document tracking:

Key	Values
ACTION	Get, Put
Direction	Inbound, Outbound
Protocol	SFTP
RemoteHostAddress	remoteAddress
RemoteHostName	remoteHost
Username	username
RemoteFile	filename

---

## Build 5101 or Higher

### FTP Server Adapter

The FTP Server adapter receives and processes requests from external trading partners that are submitted using the FTP protocol. This adapter is used with a Perimeter server. The following table provides an overview of the FTP Server adapter:

System name	FTP Server Adapter
-------------	--------------------

Graphical Process Modeler (GPM) category	None
Description	This adapter receives and processes requests from external trading partners that are submitted using the FTP protocol. This adapter is used with a Perimeter server.
Business usage	Use this adapter to get or put files from: <ul style="list-style-type: none"> <li>• Mailbox in this system</li> <li>• Physical file system</li> </ul> No additional permissions are required.
Usage example	A trading partner uses an FTP client to retrieve a business document from a mailbox. The FTP Server adapter receives and processes the trading partner request.
Preconfigured?	A configuration of the FTP Server adapter is installed, but is disabled by default. You can enable the preconfigured FTP Server adapter or create a new configuration.
Requires third party files?	Certicom SSL Library (currently available in the system)
Platform availability	All supported platforms
Related services	None
Application requirements	To log in to the FTP server, you must have permission to your virtual root (either explicitly assigned or defaulted).  To access a mailbox, you must have permission to that mailbox and all mailboxes that may be between it and your virtual root.
Initiates business processes?	The FTP Server adapter: <ul style="list-style-type: none"> <li>• Can initiate business processes if the Payload Repository is a File System. You can configure the adapter to invoke a specific business process each time a message or file is placed in the home directory.</li> <li>• Does not initiate business processes if the Payload Repository is a mailbox. However, mailbox activities can trigger routing rules.</li> </ul>
Invocation	Not used in business processes
Business process context considerations	None
Returned status values	None

Restrictions	<ul style="list-style-type: none"> <li>• FTP Server is tightly integrated with the systems's mailbox system. An FTP client can only access the mailbox that is assigned to its user account.</li> <li>• FTP Server does not support all functions specified in RFC 0959 (Standard FTP Server). It supports basic functions to integrate with the system mailbox system such as list message and sub-mailbox, send and extract message to/from mailbox.</li> <li>• FTP Server is not integrated with business process invocation when processing a request from a client.</li> <li>• The home directory for FTP is a virtual root mailbox in the system. Mailboxes include both extractable and nonextractable messages. When accessing a mailbox using the FTP Server adapter, only extractable messages are displayed. To change this default behavior, edit the ftpserver.properties file and set listUnextractables=true (Default is false).</li> <li>• The timeout value for a control channel connection is controlled by a parameter in the ftpserver.properties file. The default timeout value is 600 seconds. The minimum value is 60 seconds. If the control channel is idle longer than the timeout value, the session is terminated, unless the data channel is open (whether or not data is being transferred).</li> <li>• To access the FTP Server adapter and have full mailbox operations (listing, retrieving, and placing messages), you must have permission to the virtual root (either explicitly assigned or default). To operate fully on mailboxes in the hierarchy directory, you must have permissions on all mailboxes between the target mailbox and the virtual root.</li> <li>• Restricted operation can be granted to users with a parameter named <b>MailboxLoginWithoutVirtualRootPermission</b>. With this permission, you can log in and list files in a mailbox, but cannot retrieve or place files. This restricted permission only applies to the virtual root mailbox and does not impact operation on submailboxes.</li> </ul>
Persistence level	None. This adapter does not have a pre-set persistence level.

Testing considerations	<p>At startup, attempt to access the FTP server using a supported FTP client with the configured IP address and port.</p> <p>Debug information can be found in the FTP logs. Select Logging Level from the following:</p> <ul style="list-style-type: none"> <li>• Error – Errors only</li> <li>• Communication Trace – Errors, requests from clients, and responses from the Server adapter, including ACL violations</li> <li>• All - for debugging, all activities.</li> </ul>
------------------------	---

## Implementing the FTP Server Adapter

To implement the FTP Server adapter, complete the following tasks:

1. Create an FTP Server adapter configuration (or enable the configuration installed with the application and edit parameters as needed).
2. Configure the FTP Server adapter.

## Configuring the FTP Server Adapter

To configure the FTP Server adapter, you must specify settings for the following fields:

UI Field	Description
Name	Unique and meaningful name for the adapter configuration. Required.
Description	Meaningful description for the adapter configuration, for reference purposes. Required.
Select a Group	Not applicable for this adapter. Leave at default.
FTP Server Listen Port	The port number that the FTP Server should bind to and listen on for connection requests. The default value depends on the system platform and on your application configuration. Required.
Active Data Port Range	A range of ports that the server can allocate for the transfer of data to or from the FTP client in active mode. Optional. If left blank, the server will choose available system ports. Example values are: <ul style="list-style-type: none"> <li>• 1024-2048</li> <li>• 2222</li> <li>• 3000-4000</li> <li>• 10500-10599,10700-10799</li> </ul>

UI Field	Description
Passive Data Port Range	<p>A range of ports that the server can allocate for the transfer of data to or from the FTP client in passive mode. Optional. If left blank, the server will choose available system ports. Example values are:</p> <ul style="list-style-type: none"> <li>• 1024-2048</li> <li>• 2222</li> <li>• 3000-4000</li> <li>• 10500-10599,10700-10799</li> </ul>
Perimeter Server	<p>Select a Perimeter server from the list. Default is node1 &amp; local. Required.</p> <p><b>Note:</b> You should use a specific external interface for communications with trading partners. Using a wildcard address can cause problems with FTP sessions. If some other process has bound the port used for the data channel on an interface, it may receive connections intended for the data channel. Using a specific TCP/IP address or DNS name prevents this from occurring.</p>
Transfer Buffer Size (bytes)	<p>Specifies the size in bytes of the buffer used when transferring a file. Required. Valid values are 0 to 9,999,999,999. Default is 32000.</p>
Minimum Number of Threads	<p>A tuning parameter that indicates the range of threads available for handling events to improve performance. Must be less than or equal to the Maximum Number of Threads value. Default is 3. Required.</p> <p><b>Note:</b> Retain the default value unless instructed otherwise by Sterling Commerce support.</p>
Maximum Number of Threads	<p>A tuning parameter that indicates the range of threads available for handling events to improve performance. Must be greater than or equal to the Minimum Number of Threads value. Default is 6. Required.</p> <p><b>Note:</b> Retain the default value unless instructed otherwise by Sterling Commerce support.</p>
Resumption Timeout (hours)	<p>Timeout value for the incomplete document before it is purged. Required. Valid value is any number between 1 and 9,999,999.</p>
NAT Address	<p>Specifies the NAT IP address that the FTP server should send to the user FTP client in the passive connection mode. Optional. Overrides the global NAT address specified in the ftpserver.properties file.</p>
Maximum Logins	<p>Maximum number of logins the adapter may have active at any point of time. If no value is specified, logins are unlimited. Optional. Valid value is any integer to 9999999999.</p>

UI Field	Description
Maximum Logins per User	Maximum number of logins each user may have active on this adapter at any point of time. If no value is specified, logins are unlimited. Optional. Valid value is any integer to 9999999999.
Payload Repository	Whether files or messages will be stored in a mailbox or a physical file system on the server. Required. Valid values are: <ul style="list-style-type: none"> <li>• Mailbox (default) - If you want to restrict user access to specific mailboxes, see the <i>Mailbox Features, Creating Virtual Roots</i> documentation.</li> <li>• File System - If you want to restrict user access to specific file system folders and subfolders, see the <i>Configuring an File System Virtual Root</i>.</li> </ul>
Document Storage	Displayed only if Mailbox is selected for Payload Repository. Indicates whether the body of the requested document must be stored on the file system or if it should be in the database. Required. Valid values are: <ul style="list-style-type: none"> <li>• System Default – If your system administrator has changed the installed default of File System, this ensures that the correct location is used.</li> <li>• Database – Body of the request document will be stored in the database.</li> <li>• File System (default) – This is the default value when the application is installed, but it can be changed. Contact your system administrator to see if the default has been changed.</li> </ul> <p><b>Note:</b> For more information about document storage types, see <i>Managing Services and Adapters</i>.</p>
Add Policy Type	If you want to apply an existing policy to this instance, select the plus sign.
Select policy type	Select one of the adapter policy types: <ul style="list-style-type: none"> <li>• Bandwidth Limiting Policy</li> <li>• Lockout Policy</li> <li>• Data Limit Policy</li> <li>• Command Limiting Policy</li> </ul>
Select Policy	Select from the list. Policy must have already been created.
Select Business Process Base Directory	Parameter is only configurable if File System is selected for Payload Repository. Choose the business process from the list to be invoked each time an inbound file is received. Optional.



UI Field	Description
Base Directory	Parameter is only configurable if File System is selected for Payload Repository. Path to the directory on the physical file system which this server adapter has access to. The file system virtual root defined for any user should be relative to this directory. The home directory for any user will be a combination of this directory and the file system virtual root. Required. The operating system level user who is running the JVM must have access to this directory.
Should the adapter be restricted to a certain group of users?	Select Yes or No to indicate whether to restrict specific users and groups to access the FTP server. Required. Default is No. If Yes, select Users and or Groups from the lists on subsequent pages.
Should the restricted users be assigned a specific range of ports?	Select Yes or No to indicate whether to assign a specific port, range, or ranges of ports to the users. Required. Default is No. If Yes, specify <i>User Active Ports</i> , <i>User Passive Ports</i> , <i>Group Active Ports</i> , and or <i>Group Passive Ports</i> on subsequent pages. You can specify any or all of these fields.
Should users start in the directory that matches their user name upon login?	Valid values are: <ul style="list-style-type: none"> <li>• Yes – Upon login, the user is automatically placed in a directory that matches his or her user ID. If such a directory is not available, the user is placed in the virtual root directory. This option allows Connect:Enterprise UNIX customers to run production scripts that require each user to be placed into directories that correspond to user ID. <b>Caution:</b> Do not select Yes if there is any chance that users of your application might have user IDs that differ only by case (example: jsmith and JSmith). Unlike user IDs, mailbox names in this application are not case-sensitive.</li> <li>• No – The user is placed in the virtual root directory.</li> </ul>
Users	Select a list of users who are granted permission to access the server.
Groups	Select a list of groups who are granted permission to access the server.
<i>User Active Ports</i>	Any port number, range, or ranges of port numbers to be used as ACTIVE port. Optional. Valid values are valid, available port numbers or range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Examples of valid values are: <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>

UI Field	Description
<i>User</i> Passive Ports	<p>Any port number, range, or ranges of port numbers to be used as PASSIVE port. Optional. Valid values are valid, available port numbers or range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Examples of valid values are:</p> <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
<i>Group</i> Active Ports	<p>Any port number, range, or ranges of port numbers to be used as ACTIVE port. Optional. Valid values are valid, available port numbers or range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Examples of valid values are:</p> <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
<i>Group</i> Passive Ports	<p>Any port number, range, or ranges of port numbers to be used as PASSIVE port. Optional. Valid values are valid, available port numbers or range of port numbers. Ranges are separated by hyphens. Multiple entries must be separated by commas. Spaces do not affect the meaning. Examples of valid values are:</p> <ul style="list-style-type: none"> <li>• 3000</li> <li>• 4000-5000, 6000</li> </ul>
Extractable Count	<p>The number of times the message can be extracted. Cannot be specified in conjunction with Extractable or Extractable For. Valid value is any integer. Optional.</p>
Extractable For	<p>Indicates the length of time (in days, hours and minutes) the message can be extracted. Cannot be specified in conjunction with Extractable or Extractable Count. Valid value is in the format <i>dddhhmm</i>. Optional.</p>
Extractable	<p>Whether the message can be extracted. Cannot be specified in conjunction with Extractable Count or Extractable For. Optional. Valid values are:</p> <ul style="list-style-type: none"> <li>• Yes (Default)</li> <li>• No</li> </ul>

UI Field	Description
SSL	Whether Secure Sockets Layer (SSL) is active. Required. Valid values are: <ul style="list-style-type: none"> <li>• None – If SSL is requested by a client it will be rejected. (Default)</li> <li>• Optional – SSL is used if requested by a client.</li> <li>• Must – Clients that do not request SSL are not allowed to authenticate.</li> </ul> <p><b>Note:</b> If Optional or Must is specified, the asset protection key must enable SSL for the appropriate protocol.</p>
Key Certificate Passphrase	Password that protects the server key certificate. Used to encrypt and decrypt messages. Required if SSL option is Must or Optional.
Cipher Strength	Strength of the algorithms used to encrypt data. Required if SSL option is Must or Optional. Valid values are: <ul style="list-style-type: none"> <li>• ALL</li> <li>• WEAK – Often required for international e-commerce, because government regulations prohibit STRONG encryption from being exported.</li> <li>• STRONG – Default.</li> </ul>
Key Certificate (System Store)	Private key and certificate for server authentication. Used to encrypt and decrypt messages. Required if SSL option is Must or Optional.
CA Certificates	Certificate used to validate the certificate of an FTP client. This is the public key. If no CA certificate is chosen, no client certification is performed. Optional.
Clear Command Channel	Indicates that communication across the command channel is not encrypted after authentication is completed. Optional.

## Applying Policies to the FTP Adapter

You can apply adapter policies to the FTP Adapter. You can define Lockout, Bandwidth Limiting, Command Limiting, and Data Limit policies from the Admin Console UI (Deployment > Adapter Utilities > Policies). For more information, see *Adapter Policies*.

## FTP Server Functions Supported

The following table lists the FTP functions that are supported with the FTP Server adapter:

Category	Commands Supported
Access Control commands	<ul style="list-style-type: none"> <li>• CDUP – Change to Parent Directory</li> <li>• CWD – Change Working Directory</li> <li>• PASS – Password</li> <li>• QUIT – Logout</li> <li>• REIN – Reinitialize</li> <li>• USER – User Name</li> </ul>
Transfer Parameter Commands	<ul style="list-style-type: none"> <li>• MODE – Transfer Mode (Streamed)</li> <li>• PASV – Passive Mode</li> <li>• PORT – Data Port</li> <li>• TYPE – Representation Type (ASCII, Binary, EBCDIC, and Local byte)</li> </ul>
Service Commands	<ul style="list-style-type: none"> <li>• ABOR – Abort</li> <li>• ALLO – Allocate</li> <li>• APPE – Append</li> <li>• DELE – Delete</li> <li>• HELP – Help</li> <li>• LIST – List</li> <li>• MDTM – Last modified time of a given file on a remote host</li> <li>• MKD – Make Directory</li> <li>• NLST – Name List</li> <li>• NOOP – No Operation</li> <li>• PWD – Print Working Directory</li> <li>• REST – Restart</li> <li>• RETR – Retrieve</li> <li>• RMD – Remove Directory</li> <li>• RNFR – Rename From</li> <li>• RNTO – Rename To</li> <li>• SITE – Site Parameter (CPWD, HELP, PSWD, and WHO ZONE)</li> <li>• STAT – Status</li> <li>• STOR – Store</li> <li>• STOU – Store Unique</li> <li>• SYST – System</li> <li>• XMKD – Make Directory (Legacy format)</li> <li>• XPWD – Print Working Directory (Legacy format)</li> <li>• XRMD – Remove Directory (Legacy format)</li> </ul>

Category	Commands Supported
Security Commands	<ul style="list-style-type: none"> <li>• AUTH – Authentication/Security Mechanism</li> <li>• CCC – Clear Command Channel</li> <li>• EPRT – Specifies an address and port to which the server should connect</li> <li>• EPSV – Enter extended passive mode</li> <li>• PBSZ – Protect Buffer Size</li> <li>• PROT – Data Channel Protection Level</li> <li>• SIZE – Return the size of a file</li> </ul>

## FTP Server Functions Not Supported

The following table lists the FTP functions that are not supported with the FTP Server adapter:

Category	Commands Not Supported
Access Control commands	<ul style="list-style-type: none"> <li>• ACCT – Account</li> <li>• SMNT – Structure Mount</li> </ul>
Transfer Parameter Commands	<ul style="list-style-type: none"> <li>• MODE – Transfer Mode (Block and Compressed)</li> <li>• STRU – File Structure (Record and Page)</li> </ul>

## Activity Types for the FTP Server Adapter

This adapter reports the following activities to the Services Controller for activity monitoring:

- PUT – Adds a file to a mailbox
- GET – Retrieves a file from a mailbox
- Session – Records all activity after connection

## File System Virtual Root

When you configure an FTP adapter and the Payload Repository is defined as File System, and if you want to restrict user access to specific file system folders and subfolders, then you need to configure the file system virtual root. The file system virtual root is relative to the adapter Base Directory. The virtual root defines the point of access for each user who has permission to use the adapter. The file system virtual root is relative to the Base Directory.

## Configuring a File System Virtual Root

Before you begin, you need to know:

- User ID that need permission to the adapter virtual root
- Path to the Base Directory
- Create a folder under the base directory which will be the virtual root

To create a new File System Virtual Root:

1. Navigate to the **Administration Menu > Deployment > Adapter Utilities > FS Virtual Root**.

2. Next to **Create a new Virtual Root**, click **Go!**
3. Select the **User ID** from the list and click **Next**.
4. Enter the path to the virtual root.  
For example, if the base directory is `/install_dir/install/ftpserver1` then the file system virtual root can be any folder/directory under the `/install_dir/install/ftpserver1` directory.
5. Click **Finish**.

## Editing a File System Virtual Root

To edit a File System Virtual Root:

1. Navigate to the **Administration Menu > Deployment > Adapter Utilities > FS Virtual Root**.
2. Use either Search or List to locate the User ID for which the virtual root needs to be edited.
3. Click **edit** next to the User ID. The User ID is displayed.
4. Click **Next**.
5. Update the Virtual Root and click **Next**.
6. Click **Finish**.

## Deleting a File System Virtual Root

To delete a File System Virtual Root:

1. Navigate to the **Administration Menu > Deployment > Adapter Utilities > FS Virtual Root**.
2. Use either Search or List to locate the Virtual Root.
3. Click **delete** next to the User ID which virtual root needs to be deleted.
4. Click **OK**.
5. Review the virtual root information.
6. Click **Delete**.

## SFTP Server Adapter

The SFTP Server adapter enables external SFTP clients or SCP clients to put files into, or get files from, a mailbox in this application or to a physical file system on the server. The SFTP Server adapter:

- Uses Perimeter services.
- Uses the Mailbox subsystem or the physical file system directory as its repository (virtual roots).
- Uses routing rules for items placed in Mailbox to trigger a business process, or if items are placed in a directory on the file system, you can identify a business process to be invoked each time a new message or file is received.
- Supports SSH2 with SFTP version 3 or lower.
- Supports inbound SSH/SFTP and SSH/SCP protocols.

The following table provides an overview of the SFTP Server adapter:

System name	SFTP Server Adapter
Graphical Process Modeler (GPM) category	None

Description	Receives and processes requests from external trading partners that are submitted through the SFTP protocol or SCP protocol.
Business usage	Use this adapter to enable external SFTP clients or SCP clients to put files into, or get files from, a mailbox in this application or to a physical file system on the server.
Usage example	A trading partner uses an SFTP client to retrieve a business document from a mailbox. The SFTP Server adapter receives and processes the trading partner request.
Preconfigured?	DemoAllSFTPServerAdapter is fully preconfigured and enabled when you perform the demo procedure. See <i>Run SFTPClientDemoAllServices</i> . SFTP Server adapter is partially preconfigured. Because both configurations specify the same port, only one of these adapters can be enabled at a time. DemoAllSFTPServerAdapter is enabled after installation of your application. To enable the SFTP Server adapter, you must first disable DemoAllSFTPServerAdapter or change the port assignment.
Requires third party files?	No
Platform availability	All supported platforms for this application
Related services	Perimeter services
Application requirements	An SFTP or SCP client at the external trading partner location. When this adapter is configured with a non-local-mode perimeter server, the perimeter server must be installed and running. The perimeter server is typically installed in a DMZ environment, separated from the application by a firewall. Refer to the perimeter services documentation for details on installing and running that component.
Initiates business processes?	The SFTP Server adapter can: <ul style="list-style-type: none"> <li>• Can initiate business processes if the Payload Repository is a File System. You can configure the adapter to invoke a specific business process each time a message or file is placed in the home directory.</li> <li>• Does not initiate business processes if the Payload Repository is a mailbox. However, mailbox activities can trigger routing rules.</li> </ul>
Invocation	This adapter is not invoked from a business process.
Business process context considerations	None
Returned status values	Not applicable

Restrictions	<p>Restricted to platforms that support Java SDK version 1.5 and above. Transfer resumption (for mailboxes) is disabled by default. To enable transfer resumption and listing documents that are in the staging area, edit the sftp.properties file (located at &lt;install_dir&gt;/properties/sftp.properties.in) to set listStagedDocuments = True.</p> <p>To support transfer resumption, the SFTP Server adapter keeps partial documents in a temporary document staging area. This allows SFTP clients to resume a transfer (within a specified time frame). If the transfer does not resume within the specified amount of time, the Partial Document Clean Up Service removes documents from the staging area and the transfer is no longer available for resumption.</p> <p>A common behavior among SFTP clients before resuming a transfer is to request a list of the directory contents. In response to list requests, the default behavior is for the SFTP Server adapter to return a listing that includes:</p> <ul style="list-style-type: none"> <li>• Complete documents in the target mailbox.</li> <li>• Partial documents in the staging area. Partial documents are assigned to a particular user. The system only displays partial documents to the user to whom they are assigned.</li> </ul> <p>If two documents with the same name exist in both the mailbox and the document staging area, only the partial document in the staging area is displayed in response to a list request.</p> <p>The home directory for SFTP is a virtual root mailbox in the application or a path and directory specified on a physical file system on the server. The mailbox can include both extractable and nonextractable messages. When the SFTP Server adapter accesses the home directory, only extractable messages are displayed.</p> <p>The SFTP Server adapter does not return nonextractable files as part of a directory listing. Once a message becomes nonextractable, it effectively disappears from the SFTP view of the mailbox.</p>
--------------	---



Permissions	<p>To access the SFTP Server adapter and have full mailbox operations (listing, retrieving, and placing messages), you must have permission to the virtual root (either explicitly assigned or by default). To operate fully on mailboxes in the hierarchy directory, you must have permissions on all mailboxes between the target mailbox and the virtual root and full rights. Rights that can be given on behalf of a user are: write, read, execute, view, and delete. Each right allows specific actions to be performed. By default, a user assigned to a mailbox has all available rights.</p> <p>If a user needs to fully operate on a mailbox at a lower level in the mailbox hierarchy, the user must also have permission and rights on all mailboxes that are between the target mailbox and his virtual root. Rights required for mailbox operations are:</p> <ul style="list-style-type: none"> <li>• Add a message to a mailbox – Write permission for the Mailbox</li> <li>• Extract message from mailbox – Read for the Mailbox</li> <li>• List submailbox – Execute for All mailboxes from virtual root to submailbox</li> <li>• List virtual root mailbox – Execute for the Virtual root mailbox</li> <li>•</li> <li>• List virtual root mailbox without mailbox execute permission – Execute for the MailboxLoginWithoutVirtualRootPermission</li> <li>• Login if ACL active – Execute for Server Permission</li> <li>• Login to the virtual root mailbox – Execute for Virtual root mailbox</li> <li>• Login to the virtual root mailbox without mailbox execute permission – Execute for MailboxLoginWithoutVirtualRootPermission</li> <li>• Move message to mailbox – Write for Destination Mailbox</li> <li>• Remove message from mailbox – Delete Mailbox</li> </ul> <p>Restricted operation can be granted to users with a permission named MailboxLoginWithoutVirtualRootPermission. With this permission, you can log in and list files in a mailbox, but cannot retrieve or place files. This restricted permission only applies to the virtual root mailbox and does not impact operation on submailboxes.</p>
Persistence level	Default

Testing considerations	<p>At application startup, attempt to access the SFTP server using a supported SFTP client with the configured IP address and port. Debug information can be found in the SFTP logs. Select Logging Level from the following:</p> <ul style="list-style-type: none"> <li>• Error – Errors only</li> <li>• Communication Trace – Errors, requests from clients, and responses from the Server adapter, including ACL violations</li> <li>• All – Debugging, all activities</li> </ul>
------------------------	--

## Implementing the SFTP Server Adapter

To implement the SFTP Server adapter, complete the following tasks:

1. Create a configuration of the SFTP Server adapter (or enable the configuration installed with the application and edit parameters as needed).
2. Configure the SFTP Server adapter.

## Configuring the SFTP Server Adapter

To configure the SFTP Server adapter:

1. Select **Deployment > Services > Configuration**.
2. Next to New Service, click **Go!**
3. Select the List View icon, then select the **SFTP Server adapter** from the list. Click **Save**.
4. Click **Next**.
5. Specify field settings:

Field	Description
Name	Name this adapter will have in the application
Description	Description of adapter
Environment	<p>The Environment field is displayed only in a cluster setup. Required.</p> <p>Select the node in which the adapter should be deployed. If you do not select any node, all nodes will be selected by default and the adapter will start on the node that will be started first. The SFTP session must be node-specific. When the traffic starts, if the required node is not the default node, the adapter will be disabled. Restart traffic by editing the adapter configuration and selecting the correct node or container node.</p>
Select a Group	None – Do not include this configuration in a group.
Perimeter Server	List of perimeter servers, including local-mode perimeter servers. Required. Default is Node 1 & Local.

Field	Description
Enabled Protocols	Select the protocols to enable for this adapter. Required. Valid values are: <ul style="list-style-type: none"> <li>• SFTP and SCP (default).</li> <li>• SFTP.</li> <li>• SCP. The SCP option is only available for new configurations of the SFTP Server adapter. If you have a previous version, you can disable it and create a new one to enable SCP or SFTP and SCP.</li> </ul>
Host Identity Key	Private/Public key pair used to identify the application SFTP server to remote clients. Required.
SFTP Server Listen Port	The unique port number that the SFTP server should bind to and listen on for connection requests. Cannot be used by any other adapter. Required.
Minimum Number of Threads	A tuning parameter that indicates the minimum number of threads that the perimeter server will use to improve performance. Optional. Default is 3. <b>Note:</b> Retain the default value unless instructed otherwise by Sterling Commerce Support.
Maximum Number of Threads	A tuning parameter that indicates the maximum number of threads that the perimeter server will use to improve performance. Optional. Default is 6. <b>Note:</b> Retain the default value unless instructed otherwise by Sterling Commerce Support.
Transfer Thread Pool Size	A tuning parameter that indicates the number of permanent transfer threads the server begins with. Once a socket has either been accepted or connected, the socket is registered with a transfer thread. This thread asynchronously performs all the input and output for the socket. If all the permanent threads become fully loaded, additional threads are created to handle additional connections and shut down once they have no sockets to service. Optional. Default is 2.
Channels per Transfer Thread	A tuning parameter that indicates the number of channels available for each transfer thread. Set maximum number of SelectableChannels that can be assigned to the accept, transfer, and connect selectors. Value of 1 effectively makes server behave in thread-per-connection mode. Optional. Default is 400.
Maximum Authentications	The maximum number of failed authentication attempts a user is allowed before the session is ended. Optional. Default is 3.

Field	Description
Session Timeout (seconds)	The number of seconds each session is allowed to last. Required. Valid value is any number between 1 and 9,999,999. Default is 120,000. <b>Note:</b> If the timeout is reached during a transfer, the session will be closed immediately after the transfer completes.
Idle Connection Timeout (minutes)	The number of minutes after which the server adapter closes the TCP connection if the client/connection is idle for that length of time. Optional.
Resumption Timeout (hours)	Timeout value for the incomplete document before it is purged. Required. Valid value is any number between 1 and 9,999,999. Default is 48.
Compression	Specifies whether data is to be compressed, which reduces the amount of data transmitted as the file is copied from one node to another. The file will be automatically decompressed at the destination. Optional. Valid values: <ul style="list-style-type: none"> <li>• None</li> <li>• ZLIB</li> </ul>
PreferredCipher	The cipher the server prefers to use for both client to server and server to client stream encryption. Optional. Default is blowfish-cbc. Valid values are: <ul style="list-style-type: none"> <li>• 3des-cbc</li> <li>• blowfish-cbc</li> <li>• aes256-cbc</li> <li>• aes192-cbc</li> <li>• aes128-cbc</li> <li>• cast128-cbc</li> <li>• twofish256-cbc</li> <li>• twofish192-cbc</li> <li>• twofish128-cbc</li> </ul>
PreferredMAC	The MAC the server prefers to use for stream encryption. Optional. Valid values are: <ul style="list-style-type: none"> <li>• hmac-sha1 (default)</li> <li>• hmac-md5</li> </ul>

Field	Description
Required Authentication	<p>Specifies the type of authentication required for the adapter. Required. Valid values are:</p> <ul style="list-style-type: none"> <li>• Password or Public Key (default)</li> <li>• Password</li> <li>• Public Key</li> <li>• Password and Public Key</li> </ul> <p><b>Note:</b> If an application user account is associated with multiple public keys (SSH Authorized User keys), any of the corresponding private keys can be used to log into the SFTP Server adapter.</p>
Maximum Logins	<p>Maximum number of logins the adapter may have active at any point of time. Use this to limit the total number of users allowed to access a server at any one time. This can be used to manage server performance. If no value is specified, logins are unlimited. Optional. Valid value is any integer to 9999999999.</p>
Maximum Logins Per User	<p>Maximum number of logins each user may have active on this adapter at any point of time. Use this to limit users who want to make many connections at the same time to ensure bandwidth is shared among users. If no value is specified, logins are unlimited. Optional. Valid value is any integer to 9999999999.</p>
Payload Repository	<p>Whether files or messages will be stored in a mailbox or a physical file system on the server. Required. Valid values are:</p> <ul style="list-style-type: none"> <li>• Mailbox (default) - If you want to restrict user access to specific mailboxes, see <i>Mailbox Features, Creating Virtual Roots</i> documentation.</li> <li>• File System - If you want to restrict user access to specific file system folders and subfolders, see the <i>Configuring an File System Virtual Root</i>.</li> </ul>
Document Storage Type	<p>Select whether documents will be stored on the file system, the database, or the system default. Required. Valid values are:</p> <ul style="list-style-type: none"> <li>• File System (default) – Default value when the application is installed, but it can be changed. Contact your system administrator to see if the default has been changed.</li> <li>• Database – Body of the request document will be stored in the database.</li> <li>• System Default – If your system administrator has changed the installed default of File System, this ensures that the correct location is used.</li> </ul>

Field	Description
Add Policy Type	If you want to apply an existing policy to this instance, select the plus sign.
Select policy type	Select one of the adapter policy types: <ul style="list-style-type: none"> <li>• Lockout Policy</li> <li>• Bandwidth Limiting Policy</li> <li>• Command Limiting Policy</li> <li>• Data Limit Policy</li> </ul>
Select Policy	Select from the list. Policy must have already been created.
Should the adapter be restricted to a certain group of users?	Select Yes or No to indicate whether to restrict specific users and groups to access the SFTP server. Required. Default is No. If Yes, select Users and or Groups from the lists on subsequent pages.
Should users start in the directory that matches their user name upon login?	Places the user, upon logging in, into a directory (mailbox in the application) that corresponds to his or her user ID. Valid values are: <ul style="list-style-type: none"> <li>• Yes – Upon login, the user is automatically placed in a directory that matches his or her user ID. If such a directory is not available, the user is placed in the virtual root directory. This option allows Connect:Enterprise UNIX customers to run production scripts that require each user to be placed into directories that correspond to user ID. <b>Caution:</b> Do not select Yes if there is any chance that users of your application might have user IDs that differ only by case (example: jsmith and JSmith). Unlike user IDs, mailbox names in this application are not case-sensitive.</li> <li>• No – The user is placed in the virtual root directory.</li> </ul>
Users	Select a list of users who are granted permission to access the server.
Groups	Select a list of groups who are granted permission to access the server.
Extractable Count	The number of times the message can be extracted. Cannot be specified in conjunction with Extractable or Extractable For. Optional. Valid value is any integer.
Extractable For	A counter indicating the length of time (in days, hours and minutes) the message can be extracted. Cannot be specified in conjunction with Extractable or Extractable Count. Optional. Format is dddhhmm.
Extractable	A yes or no value indicating if this message can be extracted. Cannot be specified in conjunction with Extractable Count or Extractable For. Optional.

- On the Confirm screen, ensure that **Enable service for Business Process** is selected. Click **Finish**.

**Note:** The SFTP Server adapter will stop all active connections and shut down automatically when the database connection goes down. The SFTP Server adapter restarts after the database connection is up and running.

## Correlations and Document Tracking

The following table details the correlations available from the SFTP Server adapter for document tracking:

Key	Values
ACTION	Get, Put
Direction	Inbound, Outbound
Protocol	SFTP or SCP
RemoteHostAddress	remoteAddress
RemoteHostName	remoteHost
Username	username

## Adding Policies to the SFTP Adapter

You can apply adapter policies to the SFTP adapter. You can define Lockout, Bandwidth Limiting, Command Limiting, and Data Limit policies from the Admin Console UI (Deployment > Adapter Utilities > Policies). For more information on creating Adapter Polices, see *Adapter Polices*.

## Using Multiple SSH Keys for a single user

You can associate multiple authorized user (SSH) keys with a single Application user. You can share a single user ID with multiple trading partners who use different (private) SSH keys to authenticate to the SFTP Server adapter.

## Correlations and Document Tracking

The following table details the correlations available from the SFTP Server adapter for document tracking:

Key	Values
ACTION	Get, Put
Direction	Inbound, Outbound
Protocol	SFTP or SCP
RemoteHostAddress	remoteAddress
RemoteHostName	remoteHost
Username	username

## Activity Monitoring for the SFTP Server Adapter

The SFTP Server adapter creates activity monitoring records for the following activities:

- Active sessions (connections to clients)
- In progress PUTs display the data transferred in kbps with a progress indicator
- In progress GETs display the data transferred in kbps

To view the records, select **Business Processes > Current Activities > SFTP Server Adapter**.

## SFTP Server Options That Are Supported

Incoming Packet Types:

- INIT: Initialize the protocol (in).
- VERSION: Specify the version of the protocol that agrees with both client and server (out).
- OPEN: Opens a file for reading and/or writing.
- CLOSE: Closes a file.
- READ: Reads data from a file.
- WRITE: Writes data to a file. Also supports the following as part of WRITE: Append (APPEND), Exclusive (EXCL), Create (CREAT), Truncate (TRUNC).
- OPENDIR: Opens a directory for reading.
- READDIR: Reads files and directories from within a directory.
- REMOVE: Removes a file.
- RENAME: Renames a file (will not support directories).
- STAT: Status of a file (does not follow links).
- LSTAT: Status of a file (follows links).
- FSTAT: Status of an open file.
- REALPATH: Returns the absolute canonical path of a file or directory.

Outgoing Packet Types:

- STATUS: The result of a command.
- HANDLE: A handle to a file.
- DATA: Data from a READ.
- NAME: The name of a file or directory from a READDIR.

## SFTP Server Options That Are Not Supported

Incoming Packet Types:

- SETSTAT: Changes the status of a file.
- FSETSTAT: Changes the status of an open file.
- READLINK: Reads a symbolic link.
- SYMLINK: Creates a symbolic link.
- EXTENDED: Sends an extended command.

Outgoing Packet Types:

- EXTENDED\_REPLY: Replies to an extended command.

## SFTP Server Adapter Starts/Restarts

When restarting the SFTP Server Adapter, allow for the other necessary processes to restart. For example, after a database shutdown, there are associated processes



which need to go down before the SFTP Server shuts down. This is also applicable in the case of a database start up. Pre-requisite processes for the SFTP Server start before the SFTP Server starts up. It takes several minutes for all of pre-requisite services to restart. The amount of time to restart is highly variably by environment.

## File System Virtual Root for SFTP

When you configure an SFTP adapter and the Payload Repository is defined as File System, and if you want to restrict user access to specific file system folders and subfolders, then you need to configure the file system virtual root. The file system virtual root is relative to the adapter Base Directory. The virtual root defines the point of access for each user who has permission to use the adapter. The virtual root is relative to the Base Directory.

## Configuring a File System Virtual Root

Before you begin, you need to know:

- User ID that need permission to the adapter virtual root
- Path to the Base Directory
- Create a folder under the base directory which will be the virtual root

To create a new File System Virtual Root:

1. Navigate to the **Administration Menu > Deployment > Adapter Utilities > FS Virtual Root**.
2. Next to **Create a new Virtual Root**, click **Go!**
3. Select the **User ID** from the list and click **Next**.
4. Enter the path to the virtual root.  
For example, if the base directory is `/install_dir/install/ftpserver1`, then the file system virtual root can be any folder/directory under the `/install_dir/install/ftpserver1` directory.
5. Click **Finish**.

## Editing a File System Virtual Root

To edit a File System Virtual Root:

1. Navigate to the **Administration Menu > Deployment > Adapter Utilities > FS Virtual Root**.
2. Use either Search or List to locate the User ID for which the virtual root needs to be edited.
3. Click **edit** next to the User ID. The User ID is displayed.
4. Click **Next**.
5. Update the Virtual Root and click **Next**.
6. Click **Finish**.

## Deleting a File System Virtual Root

To delete a File System Virtual Root:

1. Navigate to the **Administration Menu > Deployment > Adapter Utilities > FS Virtual Root**.
2. Use either Search or List to locate the Virtual Root.
3. Click **delete** next to the User ID which virtual root needs to be deleted.

4. Click **OK**.
5. Review the virtual root information.
6. Click **Delete**.

---

## 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.*

*19-21, Nihonbashi-Hakozakicho, Chuo-ku*

*Tokyo 103-8510, 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.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2015. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2015.

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

#### **Trademarks**

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)<sup>®</sup> 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.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center<sup>®</sup>, Connect:Direct<sup>®</sup>, Connect:Enterprise<sup>®</sup>, Gentran<sup>®</sup>, Gentran<sup>®</sup>:Basic<sup>®</sup>, Gentran:Control<sup>®</sup>, Gentran:Director<sup>®</sup>, Gentran:Plus<sup>®</sup>, Gentran:Realtime<sup>®</sup>, Gentran:Server<sup>®</sup>, Gentran:Viewpoint<sup>®</sup>, Sterling Commerce<sup>™</sup>, Sterling Information Broker<sup>®</sup>, and Sterling Integrator<sup>®</sup> are trademarks or registered trademarks of Sterling Commerce<sup>®</sup>, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.





Product Number:

Printed in USA