Sterling B2B Integrator

Odette FTP Protocol Support

Version 5.2

Sterling B2B Integrator

Odette FTP Protocol Support

Version 5.2

Note
Before using this information and the product it supports, read the information in "Notices" on page 47.

Contents

Odette FTP Protocol Support

The Odette File Transfer Protocol (OFTP) is a packet-oriented file transfer protocol (RFC 5024) facilitating electronic data interchange of business data between trading partners.

Originally defined by the non-profit organization Odette (Organization for Data Exchange by Tele Transmission in Europe) for the automotive industry sector, it is used across a wide spectrum of industry sectors like banking, retail, manufacturing, and transport to list a few.

The protocol supports both direct peer to peer communication and indirect communication using a Value Added Network and may be used with TCP/IP, ISDN, and X.25 based networks.

Note: X.25 is not supported in IBM® Sterling B2B Integrator.

Features of the Odette FTP adapter include:

- Support of OFTP Version 2.0. For additional information, see *Using the Odette FTP Implementation*.
- Improving support of clustered environments because the OFTP Partner Profile resides in the Sterling B2B Integrator Database.
- The ability to list, search, create, and edit OFTP Partner Profile elements in the Sterling B2B Integrator user interface.
- The ability to list, export, or modify (insert or delete) one or many Odette FTP Partner Profile elements through the OFTPPartnerManager command line tool which uses Partner Profile XML file as an import or export format.

Using OFTP

The Odette FTP system uses the Odette FTP Partner Profile Database, Odette FTP Message Queue, Odette FTP Adapter, Odette FTP Queue Handler Service, and IBM Sterling B2B Integrator Scheduler/Odette FTP Scheduler Service.

The Odette FTP system uses many components. It includes the:

- Odette FTP Partner Profile Database
- Odette FTP Message Queue
- Odette FTP Adapter
- Odette FTP Queue Handler Service
- IBM Sterling B2B Integrator Scheduler/Odette FTP Scheduler Service

Odette FTP Partner Profile Database

The Odette FTP Partner Profile represents the data model describing the communication relationship between a local and remote OFTP partner (peer-to-peer) or one-to-many relationships between partners (VAN scenarios). There are OFTP Partner Profile elements on the physical and logical level. Partners and Physical Partner Contracts define the communication link parameters for TCP/IP or ISDN and Logical Partners and Logical Partner Contracts represent

companies or organizations together, with their departments or sub-organizations, that can be used on OFTP File level (SFID) for routing purposes.

Configuring the Odette FTP Partner Profile should always be the first step of each OFTP implementation.

Odette FTP Message Queue

The Odette FTP Message Queue is the central repository in the database for inbound and outbound files and OFTP receipts EERP and NERP. Each entry in the Odette FTP Message Queue has a "Status" which indicates the processing step of the file or receipt, for example, "SCHEDULED" means that the file or receipt has to be sent to a remote partner.

Note: You should create new entries in the Odette FTP Message Queue with the Odette FTP Queue Handler so that "queuing" files and initiating an OFTP Session are independent processes. Alternatively, in Manual Mode, you can create entries in the Odette FTP Message Queue directly with the Odette FTP Adapter and initiate an OFTP Session in one BusinessProcess step.

Odette FTP Adapter

The Odette FTP Adapter is used to initiate OFTP sessions, for example, to send files to remote partners, accept inbound OFTP sessions, receive files from OFTP Partners, or to be polled for files. The Odette FTP Adapter implements the OFTP State Machines and Communication State Machines for CAPI/SDN and TCP/IP. Each instance of an Odette FTP Adapter handles either ISDN or TCP/IP communication. You can create and use multiple adapter instances for each communication type. If a Physical Partner Contract name is passed to the adapter then all files or receipts in the Odette FTP Message Queue for this Physical Partner Contract with status "SCHEDULED" are searched, an OFTP session is initiated and the related messages are sent to the remote partner. Alternatively, a set of documents can be passed directly to the adapter which allows synchronous queuing and sending. If the Odette FTP Adapter accepts an inbound call, then all received files or receipts are persisted in the Odette FTP Message Queue and (optionally) in a Partner Mailbox.

Note: Before using the Odette FTP Adapter, the Odette FTP Partner Profile must be present, by entering the appropriate OFTP Partner data within in the IBM Sterling B2B Integrator user interface. For additional information, see *Odette FTP Partner Profile*. You can also import using the OFTPPartnerManager.

Odette FTP Queue Handler

The Odette FTP Queue Handler is used to create new entries in the OFTP Message Queue for queuing files, EERPs, or NERPs. A file can be queued by passing a Primary Document or a reference to a Mailbox Message together with additional parameters to the service. If a Primary Document is passed in Mailbox Mode (optional) then a Mailbox Message is also created. Optionally, in OFTP 2.0 a file can be compressed, encrypted, and signed in a CMS package before it is persisted into the Odette FTP Message Queue. Vice versa, when used in DECIPHER Mode, a CMS enveloped file in the Odette FTP Message Queue can be decrypted and written into the process data for further processing (same applies for compressed and/or signed files).

Sterling B2B Integrator Scheduler/Odette FTP Scheduler Service

The Sterling B2B Integrator Scheduler together with the Odette FTP Scheduler Adapter is used to invoke the Odette FTP Adapter for sending files or receipts previously queued in the Odette FTP Message Queue. The Sterling B2B Integrator Scheduler invokes the Odette FTP Scheduler Adapter in business process with a set of Physical Partner Contract names and/or Physical Partner Contract Group names. Then the Odette FTP Scheduler Adapter optionally checks whether there are messages to send for each of the Physical Partner Contracts. If “yes” then the “Initiator Business Process” configured in the Physical Partner Contract is started which invokes the Odette FTP Adapter for this Physical Partner Contract.

Migrating to the Odette FTP Adapter from the OFTP Adapter

The OFTP adapter is being replaced by the Odette FTP adapter.

The following sections show how to migrate from the OFTP adapter to the Odette FTP adapter.

To use the Odette FTP adapter, there are two modes (Queue Handler Mode and Manual Mode). To use the adapter in Queue Handler Mode you must configure the following in Sterling B2B Integrator:

- Odette FTP partner's profiles
- OdetteFTP Service
- OdetteFTPQueueHandler Service
- OdetteFTPScheduler Service
- Business processes (BPs)

For the Manual Mode, the OdetteFTPQueueHandler Service is not required. For more information, refer to documentation about the Odette FTP adapter and the Manual Mode.

Configuring Odette FTP partner's profiles requires the creation of the following in Sterling B2B Integrator:

- Physical Partner profile (for local and remote)
- Physical Partner Contract profile
- Logical Partner profile (for local and remote)
- Logical Partner Contract profile

Users of the OFTP adapter have to configure profiles in a third party software called OFTPplus, but users of the OdetteFTP adapter can configure all OFTP-related configuration in the adapter itself.

This document provides the information on how to map configuration parameters from both OFTPplus and OFTP adapter to the OdetteFTP Adapter's configurations.

Migration of the OFTPplus Partner Profile Configuration to the OdetteFTP Partner Profile Configuration

In the following table, the first column has the configuration paramater of **menusel file**, which contains the partner's configuration used in OFTPplus. The second column has the equivalent configuration parameters of the Odette FTP partner profile configuration.

This table contains the parameters corresponding to TCP/IP and ISDN communication mode. This does not cover X25 and X28, as these are not supported in Odette FTP adapter.

OFTPplus Partner Configuration Parameter	Odette FTP Partner Configuration Parameter
capisdn	Address, in PP (Physical Partner)
capieaz (This field is for future use.Given in Guide)	NA
srvname	A description which needs to be configured in the PP.
nua	(Depends on protocol) A destination address which needs to be configured in PP for the remote profile (i.e., for the IP mode, it's the Hostname).
route	(Depends on protocol) A destination port which needs to be configured in PP for the remote profile (i.e., for the IP mode, it's the IP Port).
userid	OFTP User ID, in PP for the local profile.
oftp_pswd	OFTP User Password, in PP for the local profile.
remid	OFTP User ID, in PP for the remote profile.
rempswd	OFTP User Password, in PP for the remote profile.
speclogic	NA (It is for X28 and X25 communication)
dupdays	Duplicate File Period (it depends on Duplicate File Checking parameter), in PPC (Physical Partner Contract).
duptype	Duplicate File Checking, in PPC.
autoeerp	Send EERP, in LPC (Logical Partner Contract).
waitforeerp	EERP Timeout, in LPC.
logfile	There is log file for logging in SI (OdetteFTP.log).
userfld	SSIDUserField, in PP.
fileuser	OFTP File User Field, in LPC.
hostprof	PP (local or remote profile), in PPC.
recformat	File Format, in LPC.
recl	Records Length, in LPC.
alter_sfid	Odette Name, in LP (Logical Partner with unique Odette name).
ndbtable	NA
fn_w_cntl	NA
commprof	Physical Partner Name, in PP.
api_version	Odette API Level, in PPC.
contact	Contact Person, in LP.
commsType	IP mode or CAPI mode, in PP.
reblock	NA
genfill	NA
filldec	NA
linefeed	Record Delimiter, in LPC.
envfname	NA

OFTPplus Partner Configuration Parameter	Odette FTP Partner Configuration Parameter
buffersz	Exchange Buffer Size, in PPC.
creditwin	Credit Window Size, in PPC.
audit_ext	NA
Profhist	NA
retries	Session Retry Intervals, in PP.
fretries	File Transmission Retries, in LPC.
eerp_script	NA
recv_script	NA
sess_script	NA
run_cmdgen	NA
multlogin	Multiple Login Sessions, in PPC.
send_only	Send Receive Capabilities, in PPC.
recv_only	Send Receive Capabilities, in PPC.
recvname	Default OFTP Virtual Filename, in LPC.
tcpaddr	Hostname, in PP for the local profile.
tcpport	IP Port, in PP for the local profile.
capiport	ISDN Router Address (configured in Odette FTP adapter).
archive	Archive setting, it should be configured in BP.

Migration of the OFTP Adapter Configuration to the OdetteFTP Adapter Configuration

The following table gives details about the equivalent parameters of the OFTP adapter (first column) and the Odette FTP adapter (second column).

OFTP Adapter Parameter	Odette FTP Adapter Parameter
Service Type	Service Type
Description	Description
System Name	System Name
Group Name	Group Name
notification files directory	NA
Partner Profile	It is configured in Sterling B2B Integrator as an Odette FTP partner profile (PP, PPC, LP, LPC).
Run in Trace Mode	NA
Start business process	Inbound Business Process Name
Notification files directory	NA
Pick up notifications	NA
Check for notifications every (seconds)	NA
Integration Mode	NA
Max. time to wait for response (seconds, 0=unlimited)	NA

OFTP Adapter Parameter	Odette FTP Adapter Parameter
Send File Data Path (for oftpsys)	NA
Generate Virtual File Name automatically	The virtual file name can be configured in BP or in LPC.
OFTP Virtual Filename Prefix	NA
OFTP Virtual Filename Time Stamp format	NA
OFTP Virtual Filename Suffix	NA
User	User

Sample Business Processes (BPs)

In the Queue Handler Mode, after you configure OdetteFTP, OdetteFTPQueueHandler, and OdetteFTPScheduler, you must have business processes similar to the ones given below, so that the Odette FTP partner can send and receive files.

Sample Business Process (BPs) to Queue Files

```
<process name = " OFTP_QUEUE_HANDLER">
  <sequence name="Sequence Start">
    <operation name="CreateFILEStructure">
      <participant name="AssignService"/>
      <output message="DataItemOut">
        <assign to="OFTPDataItem/FILE/document" from="PrimaryDocument"></assign>
        <assign to="OFTPDataItem/FILE/properties/LogicalPartnerContract">
OUTBOUNDLPCNAME </assign>
        <assign to="OFTPDataItem/FILE/properties/OFTPVirtualFilename">myfile.dat
        </assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="toProcessData">
        <assign to="." from="*"></assign>
      </input>
    </operation>
    <operation name="OdetteFTP Queue Handler">
      <participant name="Qhandler"/>
      <output message="OdetteFTPQueueHandlerInputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>
```

Sample BP to Initiate Session

```
<process name = "OFTP_INITIATOR">
  <sequence name="Sequence Start">
    <operation name="OdetteFTP">
      <participant name=" odetteftp_ service"/>
      <output message="OdetteFTPInputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
```

```
      </input>
    </operation>
  </sequence>
</process>
```

Sample BP to Send Files

```
<process name=" oftp_sendmessage">
  <sequence name="check">
    <assign to="OFTPPPCName">PPCNAME</assign>
    <assign to="OFTPActionType">Unconditional</assign>
    <operation name="CheckForOFTPMessages">
      <participant name="OFTPScheduler"/>
      <output message="DataSetOut">
        <assign to="." from="*"></assign>
      </output>
      <input message="toProcessData">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>
```

OFTP Version 2.0

In Version 2.0, the protocol additionally supports secure and authenticated communication over the Internet using Transport Layer Security, provides file encryption, signing and compression using Cryptographic Message Syntax and provides signed receipts for the acknowledgment of received files.

With ISDN only, secure authentication and file level encryption are supported.

Additional features in OFTP Version 2.0:

- Session level encryption
- File level encryption
- Secure authentication (for additional information, see *Odette FTP Security*)
- File compression
- Signed EERP
- Signed NERP
- Maximum permitted file size increased to 9PB (petabytes)
- Virtual file description added
- Extended error codes

Note: In V5.2.6 and higher, TLS1.2 is the default security protocol. If needed, you can change this value to TLS1.0 or TLS1.1 by updating the **`OFTP.Global.HelloProtocol`** parameter in `OdetteFTP.properties`. Valid values include the following parameters:

- **`TLS1-TLS1.1`** - for TLS1.0 and TLS1.1
- **`TLS1.1-TLS1.2`** - for TLS1.1 and TLS1.2
- **`TLS1-TLS1.2`** - for TLS1.0, TLS 1.1 and TLS 1.2
- **`TLS1`** - for TLS1.0 only
- **`TLS1.1`** - for TLS1.1 only
- **`TLS1.2`** - for TLS1.2 only

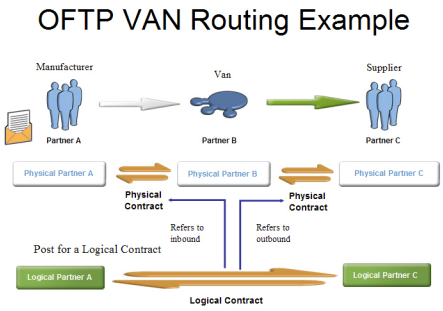
How an OFTP Session Works

The example describes the step of a successful OFTP Session between Partner A (Initiator) and Partner B (Responder).

Procedure

1. Partner A calls a Remote Partner B (ISDN over telephone line or IP connection).
2. Partner B responds with an SSRM command indicating that he is ready to start using the OFTP protocol.
3. Partner A sends a "Start Session" command (SSID) which describes his identity (OFTP User and Password, Exchange Data Buffer proposal, Secure Authentication Y/N, ...).
4. Partner B responds with his SSID (his OFTP User name and Password).
5. If "Secure Authentication" is requested in the SSID, then the Secure Authentication protocol sequence is started to exchange the Authentication Challenge (AUTH) and the Authentication Response (AURP) between the local and remote partner.
6. Partner A sends an "Start File" command (SFID) indicating that they have a file to send. A SFID contains information about Originator and Destination, OFTP Virtual File Name, File Format and options for File Compression, File Encryption and Signed EERP among others. An organization may have more than one originator and destination Logical Partner for each department.
7. Partner B responds with an "Send file positive answer" command (SFPA) indicating that they are willing to accept that file. Note: If B would like to reject the file it would send a negative answer SFNA)
8. Partner A starts to send data in the DATA command with the negotiated "Exchange Buffer Size".
9. After 7 data blocks (Default Credit Window Size), Partner B sends back a CDT command which indicates that Partner B is still listening).
10. At the end of the file, Partner A sends an EFID to indicate that the end of the file is reached.
11. Partner B then sends back an "End of File Positive Answer (EFPA) indicating that the file was successfully received.
12. Partner A has no more files to send. With a Change Direction command it allows Partner B to send his files. Partner A and B are exchanging their roles: now B is Speaker and A is Listener. If Partner B has some files to send the process starts.
13. The process then starts again with sending DATA commands from Partner B.
14. At the end of the file, they change direction again with a Change Direction command.
15. Partner A acknowledges the file by sending an "End-to-End Response" (EERP).
16. Partner B acknowledges the receipt of the EERP by sending the RTR.
17. Partner A has nothing more to send and passes control to Partner B.
18. Partner B also has nothing to send and sends an "End of Session" command (ESID)
19. Partner A receives the ESID and hangs up the line. Store-and-Forward Scenario

    The following diagram describes a sample configuration between two communication partners and one clearing hub.



OFTP and Mailboxes

The Odette FTP system provides an interface to the IBM Sterling B2B Integrator Mailbox system.

About this task

Using the Mailbox system is optional.

The following description of the Mailbox Mode assumes an OFTP communication scenario between OFTP Partner A and B.

Prerequisites:

Procedure

1. Before using the Mailbox Mode, create Mailbox User A (IBM Sterling B2B Integrator users) for yourself, the Local Partner A, and User B for your Remote Partner B.
2. Create a Partner Mailbox for yourself (Mailbox A).
3. Within Mailbox, create a submailbox with name "Inbox." All messages sent from Partner A will be placed into the Inbox of Mailbox A.
4. Create a Partner Mailbox for your Remote Partner B (Mailbox B). As default behaviour all messages received from Partner B will be placed in the root (/) of Partner Mailbox B. Optionally, you may create submailboxes in the Mailbox B of your Remote Partner. The names of the submailboxes have to be configured in the Remote Physical Partner Profile. If submailboxes are used, inbound messages are placed directly into the submailboxes instead of root "/." This option has advantages if you want to receive messages from different remote partners because the messages are placed into separate submailboxes for each remote partner which allows you to define automated Mailbox Rules for each submailbox, for example, to further automate message routing.
5. Create Mailbox Virtual Roots to associate each Mailbox User with its Mailbox Virtual Root Path, for example, User A is associated with the Mailbox Virtual Root "/A." Same for B.
6. To switch on Mailbox Mode, select a Mailbox User A in the Local OFTP Physical Partner Profile and Mailbox User B in the Remote Physical Partner Profile B.

Using Mailbox Mode

When you use mailbox mode, you have two scenarios for both outbound direction and inbound direction.

Outbound Direction (Partner A initiates the OFTP Session)

There are two scenarios for outbound direction:

- For sending files from Partner A to Remote Partner B, a new entry has to be created in the Odette FTP Message Queue first.

  In Mailbox Mode, the Odette FTP Queue Manager Service creates a copy of the outbound message in the Inbox of Partner Mailbox A and an entry in Odette FTP Message Queue (which refers to the Mailbox message ID and contains a reference to the document ID). If Partner A initiates an OFTP session all messages for a given Physical Partner Contract with status "SCHEDULED" are sent to Partner B. Messages received from Partner B in the same OFTP session are placed into the root of Partner Mailbox B (optionally: in submailboxes of B).
- If Partner A wants to poll B's OFTP system for messages and Partner A does not have files to send then A sends an OFTP Change Direction command to B immediately. Then Partner B sends all messages previously scheduled for Partner A in the Inbox of Mailbox A on the remote system back to Partner A within the same OFTP session.

Inbound Direction (Partner B initiates the OFTP session)

There are two cases for inbound direction:

- If Partner A accepts an inbound connection from Remote Partner B and B sends messages to A then these messages are placed in the root of Partner Mailbox B (optionally: in submailboxes of B) together with an entry in the Odette FTP Message Queue which refers to the Mailbox Message ID and Document ID.
- Partner B wants to poll A's OFTP system for messages.

If Partner A accepts an inbound connection from Remote Partner B and Partner B does not have files to send then B sends an OFTP Change Direction command to A immediately. Then Partner A sends all messages previously scheduled for Partner B in the Inbox of Mailbox A in the local system back to Partner B within the same OFTP session.

OFTP Business Scenario and Security Features

This example shows the OFTP business scenario of Partner A sending a file to Partner B using IP communication with the security features of OFTP 2.0.

The following description assumes that you are familiar with the standard protocol flow of OFTP version 1.4.

Intention: Partner A (Originator) wants to send a file to Partner B (Destination) using IP communication with security features of OFTP 2.0.

Physical Partner A is a Manufacturer who wants to order material from his Supplier (Physical Partner B). The procurement department at the Manufacturer is Logical Partner A and the Sales Department of Supplier is Logical Partner B. There is a Logical Partner Contract between the Procurement and Sales department. This Logical Partner Contract has a reference to the Physical Partner Contract between both companies which defines the communication layer.

Precondition: User has configured the OFTP Partner Profile, this includes:

- Logical Partner (LP_A, LP_B)

- Logical Partner contract (LPC, referring to LP_A and LP_B and Physical Partner Contract PPC)
- Physical Partner (PP_A and PP_B, both communication type IP)
- Physical Partner Contract (PPC, between PP_A and PP_B)
- Odette FTP Adapter Instance "OFTP_IP" configured
- Communication Mode "Secure IP"

Description

Originator (A):

1. The user starts a business process calling the OFTP Queue Handler Service and passes:
   - The Logical Partner Contract LPC.
   - OFTP Virtual Filename (optional).
   - Primary Document (the file to send).

   The OFTP Queue Handler:
   - Prepares the file for sending.
   - Signs, compresses and encrypts the file.
   - Prepares the file for sending.
   - Calculates the file size after encryption (required for SFID).
   - Generates Digest (Hash) from the file's transport stream. The digest is stored in database table OFTP_OBJECT_EXT).
   - Persists OFTP Version 2.0 parameters in OFTP Message Queue (table OFTP_OBJECT(_EXT).
2. The OFTP scheduler starts a business process that calls the Odette FTP Adapter instance "OFTP_IP" and passes the name of the Physical Partner Contract "PPC" that should be used for sending the file .

   The Odette FTP Adapter:
   - Establishes an OFTP Session to Partner B.
   - Sends a SSID command to Partner B which requests Secure Authentication (SSIDAUTH=Y, optional, see “Secure Authentication”).
   - Sends a SFID command containing a reference to the file, the file size, the original file size, a virtual file description, security level, Cipher Suite Selection, File compression algorithm, File enveloping format and a request for signed EERP and NERP (SFIDSIGN=Y).

Destination (B):

1. While the file is received by Destination A the Digest is calculated from the byte stream.

   If the file was transferred successfully:
   - The document containing the file is persisted to the database
   - If requested, (here: yes) an EERP is created together with the Digest calculated in step 1. The EERP is signed from B (for non-repudiation purpose)
   - The EERP is created in OFTP Message Queue (table OFTP_OBJECT)
2. B sends a "Change Direction" command (CD) to the Originator A to indicate that it now intends to send data back from B to A.
3. B sends the EERP prepared in OFTP Message Queue (table OFTP_OBJECT).

Originator (A):

1. Partner A receives the EERP from Partner B.
2. "A" checks whether the signature of the EERP is valid. If valid, "A" checks whether:
   - The set of EERP-fields which were signed within the EERP are valid.
   - The fields in the Signature are identical with the fields of the EERP.

If all fields are identical:

- "A" checks whether the Digest in the EERP is identical with the Digest stored in the OFTP_OBJECT_EXT.
- The Digest matches, the file transmission ends with Status "success" otherwise an error status is written to the entry in the OFT_OBJECT table.

Odette FTP Queue Handler

Before a message can be sent with the Odette FTP Adapter, it must be queued into the Odette FTP Message Queue by the Odette FTP Queue Handler.

Optionally, the Odette FTP Queue Handler performs offline file level services for inbound and outbound file processing. Offline file level services include file compression/decompression, file encryption/decryption, and file signing/signature validation as specified in OFTP Version 2.0.

Offline Outbound Processing

Mode “QUEUE” is used to queue schedule a File, EERP or NERP in the Odette FTP Message Queue for sending or getting polled from a remote partner.

About this task

Optionally, in OFTP 2.0 and higher, a file can be compressed, encrypted and signed by the Odette FTP Queue Handler before it is put into the Odette FTP Message Queue. The optional sequence of steps is as follows:

Procedure

1. Insert record length indicators (V-Format files only). To preserve record structure, V format file must have record headers inserted into them prior to signing, compression or encryption (2bytes, network byte order).
2. Sign files
3. Compress files
4. Encrypt files After having queued one or more files in the Odette FTP Message Queue the IBM Sterling B2B Integrator Scheduler is used to initiate OFTP sessions with the Odette FTP Adapter.

Offline Inbound Processing

Files are decrypted and decompressed in the "DECIPHER" mode for the Odette FTP Message Queue.

About this task

In mode "DECIPHER" following steps are performed of for a received file that has been persisted to the Odette FTP Message Queue:

- Offline file level decryption
- Offline file decompression
- All actions have to be performed according to file enveloping format (SFIDENV).
- Encryption and Decryption is performed outside an OFTP session for performance reasons.

Queuing OFTP Messages

Sending OFTP messages in the OFTP Message Queue in IBM Sterling B2B Integrator can be performed asynchronously from a time schedule based sending process.

This is the recommended approach though synchronous queuing and sending is possible (see Odette FTP Adapter, Manual Mode for additional information).

The Odette FTP Queue Handler is used for two different purposes:

- Mode "QUEUE": Queue/schedule a message in the Odette FTP Message Queue for sending or getting polled from a remote partner (this is the default mode)
- Mode "DECIPHER": Perform Offline File Level Decryption, Decompression and Signature verification/de-enveloping for inbound files as specified in OFTP Version 2.0

OFTP Scheduler

OFTP messages in the OFTP Message Queue can schedule asynchronously from a time schedule-based sending process. This is the recommended approach though synchronous queuing and sending is possible.

Overview

The IBM Sterling B2B Integrator Scheduler along with the Odette FTP Scheduler service is used to define when the Odette FTP Adapter should initiate an OFTP Session for either sending previously scheduled messages to a Remote Partner or poll the Remote Partner OFTP system for messages that have been scheduled for the local Partner (or should be forwarded by the local partner).

Upgrading Information

Because the IBM Sterling B2B Integrator Scheduler is now used for scheduling the Odette FTP adapter (instead of using the Odette FTP Scheduling adapter for versions 4.3 and below), it is no longer required to define Time Schedules as part of the Physical Partner Contract Profile. Schedule related PPC fields Initiator Business Process and Business Process User still exist and have the same meaning.

All schedules must be defined in the IBM Sterling B2B Integrator Scheduler (schedule type: business process). The IBM Sterling B2B Integrator Scheduler business process (see template oftpcheckformessages) invokes the Odette FTP Scheduler service and passes parameters to it, which specify what Physical Partner Contract (or PPC Group) messages should be sent or polled.

Setting Up Time Schedules for Initiating OFTP Sessions

You can set up time schedules for initiating OFTP sessions.

About this task

For the general usage of the IBM Sterling B2B Integrator Scheduler see *Creating and Managing Schedules*. For OFTP, keep the following in mind when using IBM Sterling B2B Integrator for OFTP sessions:

Procedure

1. Create a business process that invokes the Odette FTP Adapter and passes all process data parameter to the adapter. (Only the PhysicalPartnerContract parameter is used)
2. Type the name of the business process in the OFTP Physical Partner Contract field Initiator Business Process and type a IBM Sterling B2B Integrator user name in field Business Process User. Optionally, you may enter one or more comma separated Physical Partner Contract Group names in the Group Name List if you want to initiate OFTP sessions for a group of Physical Partner Contracts at the same point of time.
3. Create a Time Schedule. From the Administrator menu, select **Deployment** > **Schedules** > **Schedule a business process**. For initiating an OFTP Session to Remote Partner B every hour (using Physical Partner Contract A_B_Init) and additionally to initiate an OFTP session for PPC Group "PPC_PARTNER_GROUP." In Associate BPs to Documents Service: Select BP and optional name/value pair, type the name of the business process to start (see template "oftpcheckformessages") and define following supported Name-Value-Pairs:

Results

Name	Value
OFTPPPCName	The name of the Physical Partner Contract for which you want to initiate an OFTP session
OFTPPPCGroup	The name of the Physical Partner Contract Group for which you want to initiate OFTP sessions.
OFTPActionType (Used for all PPCs and PPC Groups specified)	Conditional: If messages exist for the PPC or PPC group, initiate OFTP Session. Unconditional: Always initiate OFTP Sessions, even if there are no messages to send. This is used to poll the Remote Partner for messages.

Time Schedules OFTP Session Requirements:

- There must be at least one OFTPPPCName or OFTPPPCGroup Name-Value-Pair.
- Both OFTPPPCName and OFTPPPCGroup Name-Value-Pairs can be repeated.
- OFTPActionType is optional. It may be defined exactly once or not at all.

Note: After successfully testing the scenario you can set the persistence level of business process "oftpcheckformessages" to PERSIST_ON_ERROR to avoid persisting BP data if no OFTP session has to be started because no messages have to be sent. This helps to save system resources if the business process is often called.

OFTP Message Queue

The Odette FTP Message Queue represents the central repository in IBM Sterling B2B Integrator database for all inbound and outbound OFTP messages and receipts.

Each entry in the queue has a status which indicates the current status of the processing step.

Outbound

To send a message with the Odette FTP adapter to a remote partner you have to schedule the message in the Odette FTP Message Queue. The Odette FTP Queue Service can be used to create a new entry for a virtual file or EERP/NERP with initial status SCHEDULED.

Inbound

For each inbound message or receipt the Odette FTP Adapter creates a new entry with initial status RECEIVING.

During processing the Odette FTP Adapter updates the status of each entry in the queue according to the current processing status. All entries in the Queue reach a final state which indicates successful or failed processing. Entries that have reached final states, may be purged by the Odette FTP Scheduler service after a configurable time interval.

The following table contains an extract of the most important fields in the Odette FTP Message Queue (database table OFTP_OBJECT):

Field	Description	Possible Values
TYPE	The message type FILE is used for OFTP virtual files. EERP is a positive end-to-end-acknowledgement. NERP is a negative acknowledgement.	FILE EERP NERP CERTIFICATE

Field	Description	Possible Values
STATUS	The status of the message or receipt that has been scheduled, sent, received or forwarded.	Initial Status: • SCHEDULED • RECEIVING Intermediate Status: • RETRY • WAIT_ON_FORWARDING • FORWARDED_WAIT_ERP • RETRY_FORWARDING • NERP_IGNORED • WRONG_ERP_RECEIVE Outbound direction - Final Success Status: • SENT • SENT_AND_GOT_ERP Outbound direction - Final Error Status: • FAIL • SENT_WAIT_ERP Inbound Direction - Final Success Status: • RECEIVED • RECEIVED_AND_EERP_CREATED • FORWARDED • FORWARDED_AND_GOT_ERP Inbound Direction - Final Error Status: • FORWARD_FAIL • FWD_FAIL_AND_CREATED_NERP • RECEIVE_FAIL
MESSAGE_ID	Mailbox Message ID for the message to send. This field is used for Mailbox Mode, only. For outbound messages the mailbox message is created by the Odette FTP Queue Handler before a new entry in table OFTP_OBJECT is created. For inbound messages the Odette FTP Adapter creates the Mailbox message and a new entry in OFTP_OBJECT when a message is received.	0, if the Mailbox System is not used
DOCUMENT_ID	Document ID of the message to send.	

Field	Description	Possible Values
LPC	Logical Partner Contract as defined in the Odette FTP Partner Profile	
PPC	Physical Partner Contract as defined in the Odette FTP Partner Profile	
SFIDDSN	The OFTP Virtual File Dataset Name as used in the “Start File” SFID command	
SFIDDATE_TIME	Virtual File Date stamp as used in the “Start File” SFID command	
SFIDTIMEC	Virtual File Time stamp as used in the “Start File” SFID command	
SFIDDEST	OFTP Destination as used in the “Start File” SFID command	
SFIDORIG	OFTP Originator as used in the “Start File” SFID command	

Message Status Table

Each status indicates the current condition of an inbound or outbound message.

Status	Description	Successor
	Initial States	
SCHEDULED	Initial Status for outbound direction. The message is ready to send.	None
RECEIVING	Initial Status for inbound direction. A message is being received from a remote partner.	None
	Intermediate States	
SENT_WAIT_ERP	A message is sent successfully to a remote partner and an EERP is requested.	SCHEDULED
RETRY	A message has not been sent successfully and a sent retry is performed.	SCHEDULED or RETRY
WAIT_ON_FORWARDING	A message is received from a remote partner A that needs to be forwarded to a remote partner B.	RECEIVING
FORWARDED_WAIT_ERP	A message has been forwarded to a remote partner successfully and an EERP has been requested.	WAIT_ON_FORWARDING

Status	Description	Successor
RETRY_FORWARDING	A message has not been forwarded successfully to a remote partner and a forward retry is performed.	WAIT_ON_FORWARDING
NERP_IGNORED	Received NERP which cannot be passed back. A NERP has been introduced with Odette API Level 1.4. Scenario: Local system is “in the middle” and we got a message from a remote partner A with the Odette API Level lower than 1.4. We forwarded the message to a remote partner B with Odette API Level equal or higher than 1.4. If the remote partner B sends back a NERP it cannot be passed back to remote partner A because A does not support NERPs.	None
	Final States	
SENT	Final success status for outbound direction if no EERP is required	SCHEDULED
SENT_AND_GOT_ERP	Final success status for outbound direction if and EERP or NERP is received for a sent message.	SENT_WAIT_ERP
FAIL	Final error status for outbound direction if the retry counter is exceeded.	SCHEDULED
RECEIVED	Final success status for inbound direction if no EERP is requested by the remote partner. Used both for type FILE and NERP/EERP.	RECEIVING
RECEIVED_AND_EERP_CREATED	Final success status for inbound direction if an EERP is requested by the remote partner	RECEIVED
FORWARDED	Final success status for inbound direction if the message has been forwarded to the forward partner and no EERP is requested.	WAIT_ON_FORWARDING
FORWARDED_AND_GOT_ERP	Final success status for inbound direction if the message has been forwarded to the forward remote partner and an EERP is requested.	FORWARDED_WAIT_ERP
FORWARD_FAIL	Final error status for inbound direction if a message has not been forwarded successfully to a forward remote partner and no EERP is requested.	WAIT_ON_FORWARDING
FWD_FAIL_AND_CREATED_NERP	Final error status for inbound direction if a message has not been forwarded successfully to a forward remote partner and an EERP is requested.	WAIT_ON_FORWARDING

OFTP Partner Profile Administration

Elements of the Odette FTP Partner Profile can be listed, searched, edited, or new ones created from the **Trading partner** > **OFTP Partner Profile** link.

There are four different types of Partner Profile elements that can be used in the Odette FTP Partner Profile link:

- Odette FTP Physical Partner
- Odette FTP Physical Partner Contract
- Odette FTP Logical Partner
- Odette FTP Local Partner Contract

The Odette Partner link in IBM Sterling B2B Integrator is a convenient and recommended way to create or modify profile elements for the first time. If a large amount of profile elements have to be added (mass import) it is more efficient to use the external command line tool OFTPPartnerManager.

OFTP Partner Manager

All OFTP Partner configuration data resides in the IBM Sterling B2B Integrator database and the OFTP Partner XML file format is used by OFTPPartnerManager for listing, importing, exporting, and deleting OFTP Partner data.

Use the command line tool OFTPPartnerManager (OFTPPartnerManager.sh resp .cmd on Windows) to list, export, insert or delete one or many Odette FTP Partner Profile elements.

It is strongly recommended that you shutdown IBM Sterling B2B Integrator before importing data because the import can change partner data accessed by current OFTP sessions.

For additional information see *Odette FTP Partner Profile*.

OFTP Visibility

The Odette FTP Adapter supports Visibility Events which can be queried in the **Administration** Menu, **Business Process** > **Monitor** > **Advanced Search** and selecting either **DataFlows** or **Communication Sessions**.

Select protocol OFTP together with additional search criteria:

- Visibility Communication Connect/Disconnect Event for OFTP Sessions
- Visibility Communication Authentication
- Visibility Session Update Event
- Visibility Transfer Begin / Transfer Update / Transfer Complete Event for files and receipts (EERP/NERP)
- Visibility Route Discovery (WFID, producer, consumer, document ID)

Tuning Considerations

To improve performance, you can configure OFTP properties to allow your system to run more effectively, depending on your system's configuration. Select one of the following tuning scenarios:

- Adjust one or more of the following properties:

  - **event_input_queue_cap** or **number_visibility_queues** in `visibility.properties.in`
  - **OFTP.Global.PMTimeOut** in `odetteFTP.properties.in`
- Turn off visibility by setting the following property:
  `OFTP.Global.EnableDMIVisibility=false`

OFTP Queue Management

Old entries from the Odette FTP Message Queue can be purged when they reach a configurable time limit and are in a Final Status.

About this task

For a list of values see "OFTP Message Queue" on page 15. These statuses can be purged automatically from the OFTP_OBJECT and OFTP_OBJECT_EXT database tables.

Procedure

1. From the Admin menu, select Deployment > Services > Configuration, and select OFTPScheduler of adapter type Odette FTPScheduler. Click edit.
2. Parameter Number of hours OFTP records are kept in the database (0=unlimited) determines how long entries are kept in the Odette FTP Message Queue. Default is 72 hours. Enter "0" if you do not want to delete any old entries. For example, you want to implement an archiving concept.
3. Save the configuration.
4. Enable the Odette FTP Scheduler adapter.

OFTP Security

The Odette File Transfer Protocol version 2.0 provides a number of new security features including: authentication/authorization, session level encryption, file level encryption, and the signing of files and receipts to help protect the transfer of files.

When using Secure IP as your transport protocol in IBM Sterling B2B Integrator, a new configuration page opens with following configuration parameters:

- System Certificate
- Cipher Strength (Weak, Strong, All)
- CA Certificate

These new configuration parameters are used if an IP-Client (such as a remote partner) tries to establish an IP connection to IBM Sterling B2B Integrator (a local partner). Once an IP connection is established a handshake protocol is used to create a secure connection between the client and server for IBM Sterling B2B Integrator.

The Odette File Transfer protocol version 2.0 supports:

- Secure and authenticated communication over the internet using Transport Layer Security (TLS/SSL)
- File encryption, signing and compression using Cryptographic Message Syntax
- Signed receipts for the acknowledgement of received files

Secure Authentication (Optional for OFTP 2.0 and higher)

After exchanging Start Session commands (SSID) the Initiator may optionally begin an authentication phase in which each trading partner proofs its identity to the other:

1. Initiator sends Security Change Direction (SECD).
2. Responder replies with a Authentication Challenge (AUCH) which contains a Random challenge unique to each session.
3. The signed challenge is sent back to the responder in the Authentication Response (AURP).
4. Responder first verifies authenticity of CMS signature. Then it checks the signing certificate. If successful the responder sends back a SECD.
5. Complementary process of verifying Responder to Initiator.

Note: The Secure Authentication protocol can be enabled or disabled in the OFTP Partner Profile and Physical Partner Contract Secure Authentication box.

Odette FTP Protocol Support (V5.2.4.1 or later)

Steps to complete after installing the iFix jar (V5.2.4.1 or later)

To complete the iFix installation, complete the steps given in the topic after installing the iFix jar.

Procedure

1. Go to `install/properties/buildWARCommonUtils.xml`.
2. Change `<arg value="${installdir}/properties/APPDynamicclasspath.cfg" />` to `<arg value="${installdir}/properties/dynamicclasspath.cfg" />` (`line 400`).
3. Run **`./deployer.sh`** from `<install_dir>/bin`.

Accessing TSL and importing certificates from the TSL list (V5.2.4.1 or later)

Trust-service Status List (TSL) is a signed list of Trusted Services Providers (TSP) and their status on a specified policy. The TSL list contains a list of public keys of certification authorities (CA), authorized by the Odette organization.

In OFTP2 TSL, the digital information that is provided for each TSP is the complete trust chain up to the trusted signer certificate.

The TSL contains a list of all certificate providers or CAs who have requested for inclusion in the Odette TSL list. The Odette organization checks the authenticity of these CAs and their compliance to the agreed terms and criteria. The CAs are added to the TSL list after a successful verification and validation.

To access the TSL and import certificates from the TSL list, configure a business process (BP) and run it. The process of importing involves the following tasks:

1. Checking the time stamp in the .upd file. The .upd file is a text file that contains information about the date and time of the last update of the TSL.
2. Verifying and validating the XML signature of the TSL.

The OdetteFTP TSL service performs the preceding tasks. It verifies the time stamp in the .upd file and the last update time in the local database. If the time stamp in

the .upd file is greater than the last update time in the local database, it verifies and validates the xml signature of the TSL and then imports the TSL into the local database.

Note: For information about the OdetteFTP TSL service, see the *OdetteFTPTSL Service* topic in the *Services and Adapters M to Z* guide.

To update the certificates in the local certificate store regularly, you can schedule the related business process to periodically access the Odette TSL and import new or updated certificates.

Sample Business Process to access the TSL and import certificates

You must have a BP similar to the following BP to access the TSL and import certificates from the TSL:

```
<process name="OdetteTSLFetchOperation">
<sequence>
 <operation name="HTTP Client Begin Session Service">
      <participant name="HTTPClientBegin"/>
      <output message="HTTPClientBeginSessionServiceTypeInputMessage">
        <assign to="HTTPClientAdapter">HTTPTSLLIST</assign>
        <assign to="RemoteHost">www.odette.org (http://www.odette.org)</assign>
        <assign to="RemotePort">80</assign>
    <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="HTTPClientBeginSessionServiceResults" from="*"></assign>
      </input>
 </operation>

   <!-- GET Service -->
    <operation name="Http Client Get Service">
      <participant name="HTTPGet"/>
      <output message="HTTPClientGetServiceTypeInputMessage">
        <assign to="SessionToken" from="HTTPClientBeginSessionServiceResults
     /SessionToken/text()"></assign>
        <assign to="URI">/TSL/TSL_OFTP2.UPD</assign>
        <assign to="ResponseTimeout">120</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*" append="true"/>
      </input>
    </operation>

 <!-- TSL Access.-->
 <operation name="OdetteFTPTSL">
      <participant name="OdetteFTPTSLTest"/>
      <output message="InputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>

 <!-- GET Service -->
    <operation name="Http Client Get Service">
      <participant name="HTTPGet"/>
      <output message="HTTPClientGetServiceTypeInputMessage">
        <assign to="SessionToken" from="HTTPClientBeginSessionServiceResults
     /SessionToken/text()"></assign>
        <assign to="URI">/TSL/TSL_OFTP2.XML</assign>
```

```
        <assign to="ResponseTimeout">120</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*" append="true"/>
      </input>
    </operation>

 <operation name="VerifyMessage">
      <participant name="XMLDSigService"/>
      <output message="verifyRequest">
       <assign to="." from="*"/>
       <assign to="action">verify</assign>
      <!--  <assign to="certificateIdentifier">test_rsa_pub</assign> -->
      </output>
      <input message="verifyResponse">
        <assign to="." from="*"></assign>
      </input>
    </operation>

 <!-- TSL Access.-->
 <operation name="OdetteFTPTSL">
      <participant name="OdetteFTPTSLTest"/>
      <output message="InputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>

    <!-- HTTP Client End Session Service, ends session specified by SessionToken.-->
    <operation name="HTTP Client End Session Service">
      <participant name="HTTPClientEnd"/>
      <output message="HTTPClientEndSessionServiceTypeInputMessage">
        <assign to="SessionToken" from="HTTPClientBeginSessionServiceResults
     /SessionToken/text()"></assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="HTTPClientEndSessionServiceResults" from="*" append="true"/>
      </input>
    </operation>

</sequence>
</process>
```

The following table lists the fields in the TSL information table (database table OFTP_TSL_INFO):

Field	Description	Possible Values
TSL_TSP_TRADE_NAME	Name of the CA certificate provider.	NA
CERT_ID	Contains the reference ID from the master table (CA or trusted related table, or both the tables) of a received certificate.	NA
TSL_UPDATE_TIME	Specifies the time when the TSL xml is updated by Odette organization.	NA

Automatic exchange of CA signed certificates (V5.2.4.1 or later)

You can send and receive CA signed certificates with trading partners.

IBM Sterling B2B Integrator supports automatic exchange of CA signed certificates with trading partners. Exchanging a certificate includes sending a certificate to a trading partner or receiving a certificate from a trading partner. The following sections provide the steps that are involved when you are sending and receiving a certificate.

Sending a certificate

The following tasks are involved when you are sending a certificate to a trading partner:

1. Procure a CA signed certificate. This step is out of the scope of Sterling B2B Integrator.
2. Send the OFTP parameters and CLID information of the certificate to the partner. The CLID information contains information about the subject, issuer, IP address, FQDHN, key usage, and extended key usage.
3. Send the certificate to the partner either through direct mode or through queue mode. Refer to the sample business process, oftp_queuecertificate, in the sample business process section.

   Apart from queueing the certificate, the business process also enters information about the certificate in the CERTIFICATE_MAPPING table. To send the certificate through direct mode, you must use the `oftpout` business process. It is a generic business process available in the system. To send a certificate, you must add the line, `<assign to="OFTPDataSet/DataItem_1/properties/CERTIFICATE">CERTIFICATE</assign>` to the BP.

After you queue the certificate to be sent, the queued certificate is sent to the partner system with SFIDDSN value set to ODETTE_CERTIFICATE_REQUEST or ODETTE_CERTIFICATE_DELIVER.

Attention: If a certificate is being exchanged with the specified partner for the first time, then ODETTE_CERTIFICATE_REQUEST is used to send the certificate. For subsequent exchanges, ODETTE_CERTIFICATE_DELIVER is used.

If the certificate is successfully received by the trading partner, then the receiving partner sends an EERP acknowledgement. If the receiving partner could not process the certificate, then the partner sends an NERP acknowledgement. The OFTP_OBJECT and CERTIFICATE_MAPPING tables are updated with information about the sent certificate.

Receiving a certificate

The following tasks are involved when you are receiving a certificate from a trading partner:

1. Obtain the OFTP parameters of the trading partner and CLID information of the certificate.
2. Create an OFTP profile for the partner.
3. Enter and save the CLID information of the certificate in the system. Use the Odette FTP CLID Info page to enter and save the CLID information.

The following steps are involved when the trading partner sends the certificate:

1. The system verifies the following parameters that are related to the certificate:
   - CLID information
   - Trust chain information
   - Certificate revocation list
   - Expiry date
2. After successful verification, the certificate is imported to the repository that is configured in the CLID information. If the verification for any one of the preceding parameters fails, then the certificate is not imported.
3. After successful import, an EERP acknowledgement is generated and sent to the initiating partner system. For failed imports, an NERP acknowledgement is generated and sent to the initiating partner system.

Sample business process for queueing certificates in the OFTP_OBJECT table

You must have a BP similar to the following BP to queue a certificate in the OFTP_OBJECT table:

```
<process name = "oftp_queuecertificate">
  <sequence name="Sequence Start">
    <operation name="CreateFILEStructure">
      <participant name="AssignService"/>
      <output message="DataItemOut">
        <assign to="OFTPDataItem/CERTIFICATE/document" from="PrimaryDocument"></assign>
        <assign to="OFTPDataItem/CERTIFICATE/properties/LogicalPartnerContract">
        LPC_Outbound</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="toProcessData">
        <assign to="." from="*"></assign>
      </input>
    </operation>

    <operation name="OdetteFTP Queue Handler">
      <participant name="oftp_queuehandler"/>
      <output message="OdetteFTPQueueHandlerInputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>

  </sequence>
</process>
```

The following table lists the fields in the certificate mapping table (database table CERTIFICATE_MAPPING):

Field	Description
OBJECT_ID	User input name for CLID data or an auto generated string for a certificate.
CERT_ID	Reference ID from the master table (TRUSTED_CERT_INFO) of a received certificate. It does not contain any value otherwise.
CERT_SERIAL	Serial number of the certificate.

Field	Description
EVENT_ID	Event ID referenced from the OFTP_OBJECT table.
SUBJECT	Certificate subject name.
ISSUER	Name of the certificate issuer.
FQDHN	Contains the DNS name present in the certificate subject alternative name.
IP_ADDRESS	Contains IP address present in certificate subject alternative name.
CERT_ORIGINATOR	Name of the certificate originator.
CERT_DESTINATION	Destination name of the certificate.
NEXT_CERT_ID	OBJECT_ID of the new certificate. The existing certificate and the new certificate are associated based on the CLID.
CERT_STATUS	Status of the certificate. Valid values: • NONE • SCHEDULED • SENT • RECEIVED • ROLLOVER • REVOKED
KEY_USAGE	Contains integer value that is based on specified key usage. If key usage is not specified, then the field is populated with default value 0.
EXTENDED_KEY_USAGE	Integers that are based on specified extended key usage. If extended key usage is not specified, then the field is populated with default value 0.
CRL_URL	URL for the certificate revocation list (CRL).
CRL_HOST	Host name of the CRL location.

Certificate rollover (V5.2.4.1 or later)

The certificate rollover feature adds extra functionality to Sterling B2B Integrator such as notifications that a certificate is nearing expiration and verification that the Certificate Logical Identification Data (CLID) entries of the certificate that is received from a trading partner match the existing CLID entries.

The certificate rollover feature adds the following functions to Sterling B2B Integrator:

- Notifying an administrator or user that a certificate is nearing expiration.
- Verifying that the Certificate Logical Identification Data (CLID) entries of the certificate received from a trading partner are the same as the CLID entries of the existing certificate.
- Importing the certificate into the local certificate store.
- Associating the new certificate with the existing certificate based on the CLID information of the certificates.

The following is the sequence of events that occur during certificate rollover:

1. The administrator configures and schedules the oftpCheckCertNotification BP.
2. The oftpCheckCertNotification BP checks for certificates with SENT status that are nearing expiration.
3. The BP notifies the administrator through an email that a particular certificate is nearing expiration. The status of the certificate that is nearing expiration is changed to ROLLOVER from SENT in the certificate_mapping table.

   Note: By default, the notification is sent 30 days in advance of the certificate expiry date. An administrator can configure the time period by modifying the param1 value of LightweightJDBCAdapterQuery operation in the oftpCheckCertNotification BP.
4. The administrator requests the concerned certificate issuer or the certificate authority (CA) for new a certificate.

   Note: Requesting for a new certificate is outside the scope of Sterling B2B Integrator.
5. After the new certificate is received, the administrator saves it in the local certificate store and sends the new certificate to the trading partners.

   Note: If the CLID information for the new certificate is different from the existing information, then, the administrator must send the new CLID information to the trading partner, before sending the certificate.

The following is the sequence of events that occur when Sterling B2B Integrator receives a certificate from a trading partner:

1. CLID entries of the certificate, such as, issuer, subject, FQDHN, IP address, key usage, and extended key usage are verified against the CLID entries of the existing certificate.

   Note: If the CLID information of the new certificate is different from the existing information, then the trading partner who is sending the new certificate sends the CLID information first. The new CLID information must be added to the system and associated with the existing certificate using the **Associate CLID** list in the Odette FTP CLID page. When the new certificate is received, it is associated with the new CLID.
2. After the successful verification of the CLID entries (or association in case of new CLID information), the certificate is imported into the local certificate store and associated with the existing certificate. The new certificate is named as `OldName-<New Serial Number>` and associated with the existing certificate.

In the UI, the new certificate name is displayed in parentheses next to the existing certificate name. For example, if the name of the existing certificate is c1 and the name of the new certificate is c2, then the names are displayed as c1(c2) in the UI. This depiction indicates that the certificates are associated with each other. Both the certificates are valid during the roll-over period. The system starts to use the new certificate after the existing certificate expires. However, to use the new certificate immediately after receiving it, you can manually switch over to the new certificate. After the existing certificate expires, the `checkexpiredcertnotification` BP notifies the administrator that the certificate has expired.

Odette FTP queue advanced search (V5.2.4.1 or later)

You can search for queued transfers and view the status of the transfers by criteria, logical partner contract, or logical partner.

You can search for queued transfers and view the status of the transfers by using the Odette FTP Queue Advanced Search page in the Administration Menu, **Business Processess** > **Monitor** > **Advanced Search** > **Odette FTP Queue**.

The search page consists of the following sections:

- Search Criteria
- Search by Logical Partner Contract
- Search by Logical Partner

The Search Criteria section contains generic search parameters, Type, Status, Filename Pattern, and Date Range. You can use the parameters in the Search Criteria section along with the parameters in any of the other two sections to specify the search criteria.

After you search for the queued transfers, use the Odette FTP Queue Search Result page to do the following tasks:

- Reschedule any failed transfer
- Delete a transfer

Attention: Ongoing transfers cannot be deleted.

You can view the transfer details by clicking the event ID link in the Odette FTP Queue Search Result page.

SFNA reason text and reason length (V5.2.4.1 or later)

In Odette FTP, the Start File Negative Acknowledge (SFNA) and the Start File Positive Acknowledge (SFPA) commands are returned in response to a Start File Identification (SFID) request. The SFNA command is returned when the recipient system refuses permission to the sender system that is sending a file.

In Sterling B2B Integrator, the SFNA reason text (SFNAREAST) and the SFNA reason length (SFNAREASL) are included as part of the SFNA command. SFNAREAST provides the reason text for refusing permission to send a file. SFNAREASL provides the length of the SFNA reason text. SFNAREAST and SFNAREASL are supported only for OFTP version 2.0.

When a sender system receives an SFNA command from a recipient system, the corresponding SFNAREAST is displayed in the OFTP Advanced Queue Search page.

If a system initiates an OFTP session through a BP and receives an SFNA command from a recipient system, the corresponding SFNAREAST is displayed in the status report of the BP and the OFTP Advanced Queue Search page.

SFNA retry for each SFNA reason code is set in `OdetteFTP.properties` file. To modify the SFNA retry configuration, set the retry parameters to `true` or `false`, as required, in the `customer_overrrides.properties` file.

Odette FTP Certificate Logical Identification Data user interface (V5.2.4.1 or later)

Sterling B2B Integrator provides the Odette FTP CLID user interface to manage the Certificate Logical Identification Data (CLID) related to a digital certificate. The CLID is shared by a trading partner before exchanging a digital certificate.

A CLID record can include one of the following sets of details:

- Subject, Issuer, Key usage, and Extended key usage.
- Fully Qualified Domain Host Name (FQDHN), Key usage, and Extended key usage. FQDHN is the DNS value present in the Subject Alternative Name or the CN present in the Subject.
- IP address, Key usage, and Extended key usage. IP address is provided in the Subject Alternative Name.

Adding CLID record (V5.2.4.1 or later)

To add a CLID record with the Odette FTP CLID page, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator.
2. Go to **Trading Partner** > **Odette FTP Partner Profile** > **Odette FTP CLID**.
3. On the Odette FTP CLID page, click **Go!**
4. On the Odette FTP CLID page, specify the values for the fields according to the instructions in the following table and click **Next**.

Field	Description
Name	Specify a name for the certificate. The name must be unique for a particular entry of the CLID record. The related certificate is saved with the name specified in the **Name** field.
Use Certificate Property for CLID	Select one of the following options: • Subject and Issuer (default) • FQDHN • IP Address
Subject	If you selected **Subject and issuer** as the certificate property for CLID in the **Use Certificate Property for CLID** field, you must specify the subject details in this field. The details must be comma-separated. For example, CN=TEST1,OU=TEST1 Trust Network,O=The Test Company,C=IN **Remember:** • Subject and issuer details are shared by the related partner. Details for all the attributes might not be shared. • = must not be preceded or succeeded by any space. If there is a space before or after =, the entry is considered invalid. For example, CN=TEST1 is the correct entry. CN = TEST1 is invalid. • Currently, CN, O, OU, C, S or ST, E or EmailAddress, L, attributes are supported. • Each attribute in the **Subject** field must be comma-separated. • Multiple entries are allowed for OU attribute. Enter the multiple entries as shown: OU=TEST1,OU=TEST2.

Field	Description
Issuer	Specify the issuer details in this field. The details must be comma-separated. For example, CN=TEST1, OU=TEST1,Trust Network,O=The Test Company,C=IN. **Remember:** • = must not be preceded or succeeded by any space. If there is a space before or after =, the entry is considered invalid. • Currently, CN, O, OU, C, S or ST, E or EmailAddress, L, attributes are supported. • Each attribute in the **Issuer** field must be comma-separated.
FQDHN	If you selected **FQDHN** as the certificate property for CLID in the **Use Certificate Property for CLID** field, you must specify the DNS value that is provided in the Subject Alternative Name or the CN value that is provided in the Subject attribute of the certificate. Multiple DNS values must be comma-separated. For example, if the Subject Alternative Name in the CLID information contains, DNS Name=www.TEST1.com DNS Name=www.TEST2.com, then you must enter it as `www.TEST1.com,www.TEST2.com`.
IP Address	If you selected **IP Address** as the certificate property for CLID in the **Use Certificate Property for CLID** field, you must specify the IP address that is provided in the Subject Alternative Name attribute of the certificate.
Key Usage	Select the required certificate key usage. The available values are: • DigitalSignature • NonRepudiation • KeyEncipherment • DataEncipherment • KeyAgreement • KeyCertSign • CRLSign • EncipherOnly • DecipherOnly

Field	Description
Extended Key Usage	Select the required certificate extended key usage. The available values are: • AnyExtendedKeyUsage • ServerAuth • ClientAuth • CodeSigning • EmailProtection • IpsecEndSystem • IpsecTunnel • IpsecUser • TimeStamping • OCSPSigning
Import Certificate To Repository	Select the required certificate category. The available values are: • Both • CA • Trusted
Associate CLID	Select the certificate to be associated with the CLID. All certificates in RECEIVED and REVOKED status are listed in the drop-down list.

5. On the Odette FTP CLID confirm page, verify the details and click **Finish**.

Editing CLID record (V5.2.4.1 or later)

To edit a CLID record with the Odette FTP CLID page, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator.
2. Go to **Trading Partner** > **Odette FTP Partner Profile** > **Odette FTP CLID**.
3. On the Odette FTP CLID page, locate and select the CLID record that you want to edit by using either Search or List, and click **Go!**
4. On the Odette FTP CLID edit page, edit the required details and click **Next**.
5. On the Odette FTP CLID confirm page, verify the details and click **Finish**.

   Remember: After you receive the related certificate, the edit option is not available in the UI and you cannot edit the CLID record.

Deleting CLID record (V5.2.4.1 or later)

To delete a CLID record with the Odette FTP CLID page, complete the following steps:

Procedure

1. Log in to Sterling B2B Integrator.
2. Go to **Trading Partner** > **Odette FTP Partner Profile** > **Odette FTP CLID**.
3. On the Odette FTP CLID page, locate and select the CLID record that you want to delete by using either Search or List, and click **Go!**
4. On the Odette FTP CLID page, click **delete** corresponding to the CLID record that you want to delete.

Managing revoked certificates (V5.2.4.1 or later)

The CA creates a Certificate Revocation List (CRL) and publishes it at specified intervals and location. The URL of the location is available in the CRL distribution point attribute of the certificate. In Sterling B2B Integrator, any automatically exchanged certificate must contain information about CRL distribution point.

One of the security enhancements in Odette FTP version 2.0 is the support for Certificate Revocation List (CRL). The CA that issued the certificate can revoke the certificate for some of the following reasons:

- Certificate's private key is compromised.
- Certificate is superseded.
- Certificate is put on hold.
- Certificate's privilege is withdrawn.

You can access the CRL distribution point and retrieve the CRL by scheduling the oftpCRLCheck system BP. The BP does the following tasks:

1. Reads the CRL URL value from the CERTIFICATE_MAPPING table.
2. Accesses the CRL URL and gets the CRL.
3. Checks if any certificates that are currently being used are revoked.

Accordingly, if any certificate is revoked, then the business process updates the status of the revoked certificate in all certificate-related tables. The admin is notified about the revoked certificate through an email.

During the automatic certificate exchange, the certificate that is exchanged is checked for revocation. If the certificate that is received is revoked, then it is not accepted. If the certificate that is sent is revoked, then it is not queued for sending.

If it is determined that a certificate that is used is revoked, you must procure a new certificate from the CA and send it to the partners to replace the revoked certificate. The new certificate might or might not have the same CLID information. If the CLID information is different from the existing one, you must send the new CLID information to the trading partner, before you send the new certificate. When you are sending the new certificate to the partner, set the value of the OFTPVirtualFilename parameter to ODETTE_CERTIFICATE_REPLACE in the related BP. This setting indicates that the new certificate is a replacement certificate.

CMS file exchange and verification (V5.2.4.1 or later)

The OFTP implementation in Sterling B2B Integrator supports sending of Cryptographic Message Syntax (CMS) files to partners. Sterling B2B Integrator also supports verification and validation of a file that is received through OFTP with the file received offline, without using OFTP. For example, by sending it using an email.

To send a file without using OFTP, do the following tasks:

1. Queue the file by using a queue handler.
2. Extract the file from the file system by using a file system adapter (FSA).
3. Send it through an email or use the Simple Mail Transfer Protocol (SMTP) adapter to email the file.

Verification and validation of the files that are received through OFTP and an email include the following steps:

1. Process the file that is received through OFTP. The file that is received through OFTP is processed by the inbound business process. Processing involves deciphering of the CMS file that is received. After processing, the document ID of the file is available in the system.
2. Process the file received through an email. Run a user-defined business process, with the queue handler service in decipher mode and with CMS_FILE and LPC_NAME parameters to decipher the CMS file.

   Note: Set the value of the CMS_FILE parameter to `true` and the value of the LPC_NAME parameter to `inbound LPC name`.
   After the file is processed, the document ID of the offline file can be procured from the process data.
3. Compare the files. Pass the document IDs of both files and a valid hashing algorithm as parameters to the Compare Document service in a user-defined business process. If both files are the same, the business process runs successfully. Otherwise, the business process fails, indicating that the files are different. A business process sample is provided below.

Sample business process for extracting CMS file

```
<process name="oftp_queue_and_extract_CMS_file">
   <sequence name="send">

      <assign to="PhysicalPartnerContract" from="'PARTNER1_PARTNER2'" />
      <assign to="LogicalPartnerContract" from="'PARTNER1_OUT'" />

   <operation name="Timestamp Utility">
            <participant name="TimestampUtilService"/>
            <output message="TimestampUtilServiceTypeInputMessage">
              <assign to="." from="*"></assign>
              <assign to="action">current_time</assign>
              <assign to="format">HHmmss</assign>
            </output>
            <input message="inmsg">
              <assign to="/ProcessData/Time" from="time/text()" append="true"></assign>
            </input>
          </operation>

          <operation name="Timestamp Utility">
            <participant name="TimestampUtilService"/>
            <output message="TimestampUtilServiceTypeInputMessage">
              <assign to="." from="*"></assign>
              <assign to="action">current_time</assign>
              <assign to="format">yyMMdd</assign>
            </output>
            <input message="inmsg">
              <assign to="/ProcessData/Date" from="time/text()" append="true"></assign>
            </input>
          </operation>

          <operation name="Business Process Metadata">
            <participant name="BPMetaDataInfoService"/>
            <output message="BPMetaDataServiceTypeInputMessage">
              <assign to="." from="*"></assign>
            </output>
            <input message="inmsg">
              <assign to="BP_NAME" from="/inmsg/BPDATA/WFD_NAME/text()"></assign>
              <assign to="BP_PID" from="/inmsg/BPDATA/WORKFLOW_ID/text()"></assign>
            </input>
          </operation>

 <operation name="CreateOFTPDataSetStructure">
         <participant name="AssignService" />
```

```
          <output message="DataSetOut">
             <assign to="OFTPDataSet/@PhysicalPartnerContract"
        from="PhysicalPartnerContract/text()"/>
             <assign to="OFTPDataItem/FILE/document" from="PrimaryDocument"/>
             <assign to="OFTPDataItem/FILE/properties/LogicalPartnerContract"
        from="LogicalPartnerContract/text()"/>
             <assign to="OFTPDataItem/FILE/properties/OFTPVirtualFilename" from= "BP_PID/text()"/>
             <assign to="OFTPDataItem/FILE/properties/Date" from="Date/text()"/>
             <assign to="OFTPDataItem/FILE/properties/Time" from="Time/text()"/>
             <assign to="OFTPDataItem/FILE/properties/FileFormat" from="FileFormat/text()"/>
             <!-- Add additional DataItems here, if you want to send multiple
        files in one OFTPDataSet -->
             <assign to="." from="*" />
          </output>

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

         <operation name="OdetteFTP Queue Handler">
              <participant name="OFTPQueueHandler"/>
              <output message="OdetteFTPQueueHandlerInputMessage">
                  <assign to="." from="*"></assign>
              </output>
              <input message="inmsg">
                  <assign to="." from="*"></assign>
              </input>
          </operation>
<assign to="PrimaryDocument" from="//result/PrimaryDocument/@SCIObjectID"></assign>
 <operation name="File System Adapter">
    <participant name="FSA_OFTP"/>
    <output message="FileSystemInputMessage">
      <assign to="Action">FS_EXTRACT</assign>
      <assign to="appendOnExtract">false</assign>
      <assign to="extractionFolder">/home/monicaja/CMS/FilesatSender</assign>
      <assign to="assignedFilename">FileSent.txt</assign>
      <assign to="assignFilename">true</assign>
      <assign to="." from="*"></assign>
    </output>
    <input message="inmsg">
      <assign to="." from="*"></assign>
    </input>
  </operation>

<!-- Add the operation for SMTP adapter for email automatically -->
 </sequence>
</process>
```

Sample business process for deciphering CMS file received through email

```
<process name="oftp_decipher_offline_cms_file">
 <sequence name="decrypt">
  <assign to="mode" from="'DECIPHER'"/>
  <assign to="CMS_FILE" from="'true'"/>
  <assign to="LPC_NAME" from="'PARTNER2_IN'"/>
    <operation name="DecryptFile">
   <participant name="OFTPQueueHandler"/>
   <output message="OFTPOut">
     <assign to="." from="*"/>
   </output>
   <input message="OFTPIn">
     <assign to="." from="*"/>
```

```
   </input>
  </operation>
 </sequence>
</process>
```

Sample business process for comparing the files

```
<process name="oftp_compare_file">
 <sequence name="decrypt">
    <operation name="CompareDocuments">
   <participant name="MyCompareService"/>
   <output message="CompareDocumentsInputMessage">
     <assign to="." from="*">
      </assign>
     <assign to="DocumentID_1" from="'937683144667d51ebnode1'"/>
     <assign to="DocumentID_2" from="'14484314468232115node1'"/>
     <assign to="Algorithm" from="'SHA-1'"/>
   </output>
   <input message="inmsg">
     <assign to="." from="*">
      </assign>
   </input>
  </operation>
 </sequence>
</process>
```

Generating and sending Negative End Response (V5.2.4.1 or later)

A Negative End Response (NERP) is generated because a transmission of the file to the final destination failed or a processing of the file at the final destination failed.

Negative End Response (NERP) is generated because of one of the following reasons:

- Transmission of the file to the final destination failed.
- Processing of the file at the final destination failed.

If transmission of the file fails, then NERP is generated only if the problem is non-temporary. If the node that is transmitting the OFTP message is facing temporary problems, then it tries to retransmit the message after a specified duration.

File processing might fail because of syntax or semantic error, decryption, signature verification, decompression failure, or failure of any service that is used in the business process that is processing the file.

In both the cases, an NERP is sent to the originator of the file with appropriate reason text and reason code. The NERP is stored in the OFTP_OBJECT table and OFTP_OBJECT_EXT table. A user can search for the NERP in the Advanced Queue Search page also.

Remember: Reason text is not supported in OFTP 1.4 implementation. In OFTP 2.0 implementation, you must select the **NERP Reason Text** check box to receive reason text in the NERP.

Logical Partner Contract UI changes

The Logical Partner Contract page is modified to enable users to specify settings that are related to NERP generation. The following table describes the new user interface elements.

User interface element	Description
Generate End Response after File Processing	If **Generate End Response after File Processing** is not selected, then an EERP is generated and sent to the sender after Sterling B2B Integrator receives the file. This is the default OFTP behavior in Sterling B2B Integrator. If **Generate End Response after File Processing** is selected and mode is set to **InLine**, the inbound business process runs after a file is received. Depending on the success or failure of the business process, an NERP or End to End Response (EERP) is generated and sent to the sender. If **File processing** is selected and mode is set to **OffLine**, the file that is received is stored in the system. The status of the file is set to RECEIVED_AND_WAIT_ERP. A user-defined BP must be manually run. The BP picks the files in the RECEIVED_AND_WAIT_ERP status, based on the Physical Partner Contract (PPC) or Logical Partner Contract (LPC) specified in the BP and processes them. Depending on the success or failure of the BP, NERP or EERP is generated and sent to the sender.
File processing mode	**InLine** - When the **InLine** option is selected, the file that is received is processed immediately, though not in the same session. **OffLine** - When the **OffLine** option is selected, the file that is received is processed at a later stage, as required.
NERP Reason Text	If this check box is selected, the reason text is included in the NERP in OFTP version 2.0 implementation.

The UI changes and settings that are related to NERP are applicable only for file processing and not certificate processing. For certificate processing, an NERP is sent to the originator with reason code 99, under the following scenarios:

- The root CA certificate not available in Sterling B2B Integrator.
- The CLID of the certificate does not match with the CLID record present in the system.
- The certificate is listed in the Certificate Revocation List.

OFTPFileProcessingResponse service

A new service, OFTPFileProcessingResponse, supports the NERP implementation in Sterling B2B Integrator. This service is required for generating the end response after file processing is completed. For file processing in inline mode, the service must be added to the inbound BP. For file processing in offline mode, the service must be included in the user-defined BP. Sample BPs for inline and offline modes are provided in the following sections.

OFTP_GenerateEndResponse business process inline mode

```
<process name="OFTP_decipher_GenerateResponse">
<sequence name="decrypt">
<assign to="mode" from="'DECIPHER'" />
<!--
<assign to="MessageId">number</assign>
-->
<!-- Decipher document -->
<operation name="DecryptFile">
<participant name="OFTPQueueHandler" />
<output message="OFTPOut">
<assign to="." from="*"/>
</output>
<input message="OFTPIn">
<assign to="." from="*"/>
</input>
</operation>


 <operation name="GenerateEndResponse">
      <participant name="oftpFileProcessResponse"/>
      <output message="InputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>

 <onFault>
  <sequence>
   <assign to="FILEPROCESS_FAIL">True</assign>
  <operation name="GenerateEndResponse">
      <participant name="oftpFileProcessResponse"/>
      <output message="InputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
  </onFault>

</sequence>
</process>
```

OFTP_GenerateEndResponse business process offline mode

```
<process name="oftpofflinenew">
  <rule name="moreDocuments">
    <condition>currentDocIndex &lt;= totalDocCount</condition>
  </rule>

 <sequence name="Sequence Start">
  <sequence>
    <operation name="select document ids from OFTP_OBJECT table">
      <participant name="LightweightJDBCAdapterQuery"/>
      <output message="LightweightJDBCAdapterTypeInputMessage">
        <assign to="pool">mysqlPool</assign>
        <assign to="query_type">SELECT</assign>
        <assign to="result_name">DocumentID_Results</assign>
        <assign to="row_name">DOCUMENT</assign>
        <assign to="sql">SELECT DOCUMENT_ID FROM OFTP_OBJECT WHERE
     LPC = 'LPC_M1_M2_IN' AND STATUS IN( 'RECEIVED_AND_WAIT_ERP') </assign>
        <assign to="." from="*"></assign>
      </output>
```

```
    <input message="inmsg">
 <assign to="." from="*"></assign>
    </input>
  </operation>

<operation name="XML Encoder">
  <participant name="XMLEncoder"/>
   <output message="XMLEncoderTypeInputMessage">
    <assign to="." from="*"></assign>
    <assign to="exhaust_input">YES</assign>
    <assign to="mode">xml_to_process_data</assign>
    <assign to="output_to_process_data">YES</assign>
   </output>
   <input message="inmsg">
    <assign to="." from="*"></assign>
   </input>
 </operation>

<assign to="totalDocCount" from="count
  (//ProcessData/DocumentID_Results/DOCUMENT/DOCUMENT_ID)"></assign>
<assign to="currentDocIndex">1</assign>

 <choice name="offlineProcessingLoop">
  <select>
   <case ref="moreDocuments" activity="doOfflineProcess"/>
  </select>

 <sequence name="doOfflineProcess">
 <assign to="mode" from="'DECIPHER'"></assign>
       <assign to="FileProcessing">True</assign>
 <assign to="Response_DOC_ID" from="//ProcessData/DocumentID_Results/
   DOCUMENT[position()=//currentDocIndex/text()]/DOCUMENT_ID/text()"></assign>

    <operation name="DecryptFile">
           <participant name="OFTPQueueHandler"/>
           <output message="OFTPOut">
             <assign to="." from="*"></assign>
           </output>
           <input message="OFTPIn">
             <assign to="." from="*"></assign>
           </input>
         </operation>

    <operation name="GenerateEndResponse">
           <participant name="oftpFileProcessResponse"/>
           <output message="InputMessage">
             <assign to="." from="*"></assign>
           </output>
           <input message="inmsg">
             <assign to="." from="*"></assign>
           </input>
         </operation>

    <onFault>
           <sequence>
             <assign to="FILEPROCESS_FAIL">True</assign>
             <operation name="GenerateEndResponse">
               <participant name="oftpFileProcessResponse"/>
               <output message="InputMessage">
                 <assign to="." from="*"></assign>
               </output>
               <input message="inmsg">
                 <assign to="." from="*"></assign>
               </input>
             </operation>

           </sequence>
```

```
          </onFault>

      <assign to="currentDocIndex" from="currentDocIndex + 1"></assign>
      <repeat ref="offlineProcessingLoop"/>
         </sequence>
       </choice>
     </sequence>

  </sequence>
</process>
```

OFTP file transfer resume (V5.2.4.1 or later)

The OFTP implementation in Sterling B2B Integrator supports the resuming of file transfers for failed transmissions.

To enable the resume function, select the **Restart option** check box in the Odette FTP Physical Partner Contract page. A failed file transfer is resumed only if both the partners have enabled the resume function. The number of times the system resumes file transmission depends on the value that is set in the **File Transmission Retries** field in the Odette FTP Logical Partner Contract page.

On transfer of every 1-MB data, the SFIDREST column in the OFTP_OBJECT table of the sending and receiving systems is updated with the sent and received bytes. The transfer progress is displayed in the Odette FTP Queue Advanced Search page.

Note: To modify the amount of data that is saved in the SFIDREST column, set the value of the `max_stream_chunk_size_bytes` parameter in the `jdbc.properties` file to the required value. For example, to save 2-MB data, set `max_stream_chunk_size_bytes` to `2048000`.

When file transmission fails, the transferred bytes and the received bytes are stored in the SFIDREST column of the sending and receiving systems. In the sending system, the status for a failed entry is RETRY_PENDING, and in the receiving system, the status is RECEIVE_FAIL.

When transmission is resumed, the sending system updates the status of the failed entry from `RETRY_PENDING` to `RETRY`, and sends the count of the transferred bytes to the receiving system in an SFID command. In response, the receiving system sends the count of the received bytes in an SFPA command. File transfer restarts under one of the following scenarios:

- Byte count of the sending and the receiving systems are equal.
- Byte count of the receiving system is less than the byte count of the sending system.

If the byte count of the receiving system is more than the byte count of the sending system, then the session is terminated because of data integrity reasons.

After a successful file transfer, the status of the related entries in the OFTP_OBJECT table is changed appropriately.

Note: In a file transmission scenario, if the EFPA command that the receiving system sends after successfully receiving a file does not reach the sending system, then the status of the file is set as follows:

- RETRY_PENDING - If file transmission retry is configured
- FAIL - if file transmission retry is not configured

If file transmission retry is configured, then the sending system tries to resend the file when the network, OFTP adapter, or server are functioning. If duplicate check is configured on the receiving system, then the receiving system rejects the file and sends an SFNA. Consequently, the status of the file in the sending system is changed to FAIL. However, the sending system receives the EERP or NERP.

Alert email generation for failed file transfers (V5.2.4.1 or later)

The OFTP generates alert emails for failed file transmissions and timeouts.

The OFTP implementation in Sterling B2B Integrator supports generation of alert emails for failed file transmissions with the following status:

- SEND_AND_GOT_NERP
- RECEIVED_AND_NERP_CREATED
- FAIL
- RECEIVE_FAIL

Alert emails are also sent for the following timeouts:

- File schedule timeout
- EERP timeout
- NERP timeout

Based on the configuration, alert emails are generated for every failed transfer or according to a specified schedule, which is configured in OFTP scheduler.

Email generation for every failed transfer

The Odette FTP Logical Partner profile page is updated to support alert email generation for failed transfers in general and to generate alert mails for every failed transfer in specific. The following table lists the new fields:

Table 1. Odette FTP Logical Partner modifications to support generation of alert mails

Field	Description
Contact Mail ID	Specify the email ID to which the alert email must be sent.
Mail Server Host	Specify the email server host name.
Mail Server Port	Specify the email server port number.
Generate Alert Mails for each Failure	Select the check box if you want alert emails to be generated for each failed transfer. **Note:** The check box must be selected to generate alert emails for every failed transfer.

Note: The **Contact Mail ID, Mail Server Host** and **Mail Server Port** fields are also used when the email generation is scheduled.

Email generation based on scheduling

To schedule the alert email generation, configure the OFTP scheduler. The OFTPScheduler: OFTP Mail Generation Parameters page is added to the OFTP Services Configuration page. The following table describes the fields in the OFTPScheduler: OFTP Mail Generation Parameters page:

Table 2. OFTPScheduler: OFTP Mail Generation Parameters

Field	Description
Number of mins after which it will check for Failures and generate Mails.(0=No Schedule)	Specify the number of minutes the scheduler must wait before it checks for failures and generates alert emails.
Select Logical Partner for which Alert Should be generated	Select the logical partner for which alert email must be delivered and click the arrow to add it to the selected list. The contact email ID, email server host, and email server port are picked from the selected logical partner's profile.

A system BP with the default OFTP_SMTP_Adapter is used to send emails. If the email parameters are not configured in the Odette FTP Logical Partner profile page, then the parameters are picked from the `sandbox.cfg` properties file.

Support for SFIDDESC and SFIDDESCL parameters in the SFID command (V5.2.4.1 or later)

The SFIDDESC parameter contains the virtual file name description and SFIDDESCL parameter provides information about the description length. The owner organization and the trading partner must agree on the contents and meaning of data in the SFIDDESC parameter.

Based on the enhancements in OFTP v 2.0 and above, IBM Sterling B2B Integrator supports SFIDDESC - Start File Identification Description and SFIDDESCL - Start File Identification Description Length parameters in the Start File Identification (SFID) command.

Changes in the user interface

As part of the support for SFIDDESC parameter, the **Virtual Filename Description** field is added on the Odette FTP Logical Partner Contract, LPC - Part II page. The following table provides a description of the **Virtual Filename Description** field.

Field	Description
Virtual Filename Description	Optional. Provides a description of the virtual file, based on the bilateral agreement between the trading partners. A description is used for clarity when the trading partners exchange files of different formats, such as, CAD, e-invoice, and so on. You can provide the description in the XML DataSet or in the user interface. If the description is provided in the XML DataSet and the user interface, then the description provided in the XML DataSet overrides the description provided in the user interface. **Attention:** Virtual filename description, Virtual filename description length and other details related to a transfer can be viewed by clicking the event ID link in the Odette FTP Queue Search Result page. The search result page is located in the **Administration Menu**, **Business Processess** > **Monitor** > **Advanced Search** > **Odette FTP Queue**. Virtual filename description length is calculated dynamically for each transaction.

Changes in the business process

The **SFIDDESC** (Virtual Filename Description) parameter can be set in the direct mode and queue mode BPs.

- Changes in the queue mode BP:

```
<assign to="OFTPDataItem/FILE/properties/FileDescription">virtual file
description from BP</assign>
```

```
<assign to="OFTPDataSet/DataItem_1/properties/FileDescription"
from="FileDescription/text()"/>
```

- Changes in the direct mode BP:

```
<assign to="OFTPDataItem/FILE/properties/FileDescription">virtual file
description from BP</assign>
```

Sample business process for queueing a file in the OFTP_OBJECT table

You must have a BP similar to the following BP to queue a file with the **SFIDDESC** (Virtual Filename Description) set, in the OFTP_OBJECT table:

```
<process name = "OFTPQueuehandler_FileDescriptionTest">
  <sequence name="Sequence Start">
    <operation name="CreateFILEStructure">
      <participant name="AssignService"/>
      <output message="DataItemOut">
        <assign to="OFTPDataItem/FILE/document" from="PrimaryDocument"></assign>
        <assign to="OFTPDataItem/FILE/properties/LogicalPartnerContract">LPC_AB_Outbound</assign>
        <assign to="OFTPDataItem/FILE/properties/OFTPVirtualFilename">myvirtualfile.dat</assign>
  <assign to="OFTPDataItem/FILE/properties/FileDescription">
     virtual file description from BP</assign>
        <assign to="." from="*"></assign>
      </output>
```

```
      <input message="toProcessData">
        <assign to="." from="*"></assign>
      </input>
    </operation>

    <operation name="OdetteFTP Queue Handler">
      <participant name="qhand_a"/>
      <output message="OdetteFTPQueueHandlerInputMessage">
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>

  </sequence>
</process>
```

Sample business process for directly sending a file

You must have a BP similar to the following BP to directly send a file with the **SFIDDESC** (Virtual Filename Description) set:

```
<process name="oftpout">
   <sequence name="send">
      <!--
        Either pass following six parameters from an initiating process and
    remove the assign statements _or_ enter the names of your Physical
    and Logical Partner Contracts as defined in the PartnerProfile file
         for a first test. The Odette virtual file name and Date/Time stamp
    together should be unique for each file.

  Adding new parameter to set virtual filename description.
      -->
      <assign to="PhysicalPartnerContract" from="'PPC1'" />
      <assign to="LogicalPartnerContract" from="'LPC1'" />
      <assign to="filename">dataitem1.dat</assign>
      <assign to="FileFormat">U</assign>
      <assign to="Date">060825</assign>
      <assign to="Time">153055</assign>

      <operation name="CreateOFTPDataSetStructure">
         <participant name="AssignService" />

         <output message="DataSetOut">
            <assign to="OFTPDataSet/@PhysicalPartnerContract"
     from="PhysicalPartnerContract/text()"/>
            <assign to="OFTPDataSet/DataItem_1/document" from="PrimaryDocument"/>
            <assign to="OFTPDataSet/DataItem_1/properties/LogicalPartnerContract"
     from="LogicalPartnerContract/text()"/>
            <assign to="OFTPDataSet/DataItem_1/properties/OFTPVirtualFilename"
     from="filename/text()"/>
            <assign to="OFTPDataSet/DataItem_1/properties/Date" from="Date/text()"/>
            <assign to="OFTPDataSet/DataItem_1/properties/Time" from="Time/text()"/>
            <assign to="OFTPDataSet/DataItem_1/properties/FileFormat" from="FileFormat/text()"/>
  <assign to="OFTPDataSet/DataItem_1/properties/FileDescription" from="FileDescription/text()"/>
            <!-- Add additional DataItems here, if you want to
      send multiple files in one OFTPDataSet -->
            <assign to="." from="*" />
         </output>

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

      <!-- Start OFTP send process -->
```

```
      <operation name="SendFile">
         <participant name="OFTPSendFile" />

         <output message="OFTPOut">
            <assign to="." from="*"/>
         </output>

         <input message="OFTPIn">
            <assign to="." from="*"/>
         </input>
      </operation>
   </sequence>
</process>
```

Support for separate private key and certificate support for file encryption, file signing, and EERP signing (V5.2.4.1 or later)

The OFTP implementation in Sterling B2B Integrator supports the configuration of separate private key and certificate for file encryption, file signing, and End to End Response (EERP) signing.

Three new list boxes are added on the Odette FTP Logical Partner page to select the private keys to be used for EERP signing, file signing, and file encryption. Also, three new screens are added to configure the certificates.

The following table describes the new fields added to the New Odette FTP Logical Partner and Edit Odette FTP Logical Partner pages.

Table 3. New fields in Odette FTP Logical Partner page

Field	Description
File Decryption Key Certificate	Optional. You can specify the private key to be used for decrypting a file that is received.
File Signing Key Certificate	Optional. You can specify the private key to be used for signing a file.
EERP Signing Key Certificate	Optional. You can specify the private key to be used for signing an EERP or NERP.

The following table describes the File Encryption User Certificate page.

Table 4. File Encryption User Certificate

Field	Description
Filter Data	Field to filter the certificates listed in the Select Certificate list. Type the required text in the field and click the filter icon.
Select Certificate	Optional. Select the certificate to be used for encrypting a file. The certificate for file encryption is shared by the trading partner.

The following table describes the File Signing User Certificate page.

Table 5. File Signing User Certificate

Field	Description
Filter Data	Field to filter the certificates listed in the Select Certificate list. Type the required text in the field and click the filter icon.
Select Certificate	Optional. Select the certificate to be used to verify the digital signature of a received file.

The following table describes the EERP Signing User Certificate page.

Table 6. EERP Signing User Certificate

Field	Description
Filter Data	Field to filter the certificates listed in the Select Certificate list. Type the required text in the field and click the filter icon.
Select Certificate	Optional. Select the certificate to be used to verify the digital signature of an EERP or NERP.

Attention: If file service private key and file service certificate are already configured, then the private key and certificate are retained in the new fields and pages. To configure separate private key and certificates, edit the existing profile and select the required private keys and certificates for file encryption, file signing, and EERP signing

Enhancing performance of OFTP in Sterling B2B Integrator (V5.2.4.1 or later)

To enhance OFTP performance, consider the steps and settings in this section.

Complete the following tasks to enhance OFTP performance:

- Specify values for the following parameters in the `OdetteFTP.properties` file that is located at, `install/properties/OdetteFTP.properties`:
  - **`OFTP.Global.MinThreadsUserMon`**
  - **`OFTP.Global.MinThreadsEntity`**
  - **`OFTP.Global.MinThreadsComm`**
  - **`OFTP.Global.MaxThreadsUserMon`**
  - **`OFTP.Global.MaxThreadsEntity`**
  - **`OFTP.Global.MaxThreadsComm`**
- Set appropriate values for the **Credit Window Size** and **Exchange Buffer Size** fields while configuring a physical partner contract. Higher values in these fields enhance the performance of OFTP. Ensure that the values of these fields and the number of parallel sessions configured do not exhaust the system memory.

  For example, if a system with the following configuration receives 10 MB data in 1000 sessions each, then the system might throw an out of memory error:
  - 1 GB RAM
  - **Credit Window Size** is set to 100
  - **Exchange Buffer size** is set to 90000 bytes in the OFTP trading partner profile

  The error occurs because the system is forced to process data beyond the available memory of 1 GB.

- Set appropriate value for the session timeout parameter, **OFTP.GlobalPMTimeOut** when you are sending big files in multiple concurrent sessions.
- Set the **OFTP.Global.EnableDMIVisibility** parameter to **false** to achieve high performance when the file load transfer is high. By default, the property is set to **true** and is used to enable DMI visibility.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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, MD-NC119
Armonk, NY 10504-1785
US

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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 actual people or business enterprises 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 shown in the next column.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at 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®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Product Number:

Printed in USA