Sterling Integrator®

OdetteFTP Partner Profile

Version 5.0

Sterling Commerce
An IBM Company

Contents

OdetteFTP Partner Profile

The Odette FTP Partner Profile defines all partner specific configuration parameters required to build a model of the OFTP communication link(s) between your organization and your OFTP partner(s). The elements of the Odette FTP Partner Profile are:

- Physical Partner
- Physical Partner Contract
- Logical Partner
- Logical Partner Contract

Physical Partner

A Physical Partner describes general communication link parameters like the OFTP User ID and OFTP Password, which are used to establish an OFTP session (OFTP command "Start Session", SSID).

Beside general OFTP parameters, a Physical Partner describes communication specific parameters for communication over either an ISDN telephone line ("CAPI Mode") or over TCP/IP network ("IP-Mode"). In CAPI Mode, you have to specify your ISDN telephone number ("Address") beside other ISDN specific parameters. In IP Mode you have to specify your IP-Address or Server Name ("Hostname") and the IP Port beside other IP specific parameters.

Note: If you want to setup communication for both ISDN and IP you have to create two different Physical Partners Profiles for it.

The Physical Partner describes communication parameters about you ("Local Physical Partner") or your OFTP Partner ("Remote Physical Partner"). Which role a Physical Partner is playing in the communication scenario is not configured in the Physical Partner itself but is determined by a contract between two Physical Partners, the Physical Partner Contract.

Physical Partner Contract

A Physical Partner Contract defines the OFTP communication link between a local Physical Partner and a remote Physical Partner identified by the Physical Partner Names. It contains OFTP communication parameters that have to be defined in a bilateral agreement between you and your OFTP partner or that are automatically negotiated between you and your partner during establishing an OFTP session like the Odette API Level, for example, the OFTP Exchange Buffer size.

Note: Both Local and Remote Physical Partners must have the same communication type (IP or CAPI).

Note: Local and Remote Physical Partner must not be identical. If you want to create a loopback scenario where local and remote partner reside on the same system for testing purposes you need to create two different Physical Partner Contracts with crossed Local and Remote Physical Partner names.

Logical Partner

A Logical Partner is the logical end-point of the communication. Think of it as a department within your organization or within the organization of your OFTP partner. Beside other parameters the Logical Partner contains the Odette Code ("Odette Name") which uniquely identifies your OFTP communication partner.

Logical Partner Contract

The Logical Partner Contract is the top-level entry point which references the following Partner Profile elements:

✦ Originator Logical Partner
✦ Destination Logical Partner
✦ Inbound Physical Partner Contract
✦ Outbound Physical Partner Contract

The Originator and Destination Logical Partners define the logical end-points of the communication scenario.

There are different types of communication scenarios:

✦ If your organization wants to send messages, you must specify an Outbound Physical Partner Contract only.

✦ If your organization wants to receive messages from a remote partner, you must specify an Inbound Physical Partner Contract only.

✦ If your organization receives data from an OFTP remote partner but you are not the end-point of the communication, you must forward the message to a seconed remote partner. In this case, for your Logical Partner Contract you have to specify both an Inbound and an Outbound Physical Partner Contract. If your organization wants both to send messages to a remote partner and receive messages from the same remote partner, you must use two Logical Partner Contracts. For sending, use an outbound Physical Partner Contract and for receiving, use the second Logical Partner Contract where Originator and Destination Logical Partner exchange their roles.

Managing Odette FTP Partner Profile in Sterling Integrator

Use an Application Maintenance Window to make changes to the Partner Profile. Verify that no business processes are active which call the OdetteFTP adapter.

Note: All changes in the configuration of the Odette Partner Profile database become active immediately after saving the changes with the Odette Partner Profile User Interface or mass importing/updating/deleting Partner Profiles from the command line tool OFTPPartnerManager.sh/.cmd.

It is strongly recommended that you test an OFTP Partner Configuration in a test environment before using it on a production system.

You can list, search, create and edit elements of the Odette FTP Partner Profile in Sterling Integrator. To access them, from Administration menu, select Trading Partner > Odette FTP Partner Profile.

There are four difference types of Odette FTP Partner Profile elements that can be managed:

✦ Odette FTP Physical Partner

✦ Odette FTP Physical Partner Contract

✦ Odette FTP Logical Partner

✦ Odette FTP Logical Partner Contract

Managing Partner Profile in Sterling Integrator User Interface

Creating a Partner Profile

To create a Physical Partner entry as part of the partner profile:

1. From the Administration menu select, Trading Partner > Odette FTP Partner Profile.

2. The Odette FTP Physical Partner page appears. In Create Odette FTP Physical Partner, click Go!.

3. Complete the fields and click **Next**.

Editing, Searching, or Listing a Partner Profile

You can edit a partner profile using the Search or List function on the profile screen.

1. From the Administration menu select, Trading Partner > Odette FTP Partner Profile, then select the element type of the Odette Partner Profile you want to change. You can change one of these four elements:

   ◆ Physical Partner

   ◆ Physical Partner Contract

   ◆ Logical Partner

   ◆ Logical Partner Contract

To search:

✦ In the Search area, type the name of the Physical or Logical Partner or Contract you want to edit and click **Go!**.

To list by letter:

✦ In the List area, type the first letter of the name of the Physical or Logical Partner or Contract you want to edit and click **Go!**.

2. After you Search or List the profile you want to access, a list of profile names appear.

3. In the Select column, click the **edit** link for the partner profile you want to edit.

4. The profile settings appear. Change the setting you want to edit.

5. Click **Next** to navigate to the next screen.

6. Click **Save** to complete your changes.

Physical Partner

To edit a Physical Partner:

1. From the Administration menu select, Trading Partner > Odette FTP Partner Profile > Odette FTP Physical Partner.

2. Locate a Physical Partner by using the search or list function.

3. In the Select list, click the edit link.

4. Edit the fields and click **Next**.

This table describes the fields for a physical partner:

Field Name	Description
Physical Partner Name	Unique name for the Physical Partner. Required.
Description	Textual description of the Physical Partner. Required.
OFTP User ID	The OFTP ID used in the SSID command. Must be defined in the bilateral agreement with your partner. Required.
OFTP User Password	The OFTP password used in the SSID command. Must be defined in the bilateral agreement with your partner. Required. **Note:** In the User Interface the password is encrypted automatically when the profile is saved.
Mailbox User	User name in the Application Mailbox system. Optional. The value of this field determines whether the "Mailbox Mode" is used or not. None: Select this if you do not want to use the Sterling Integrator Mailbox System. If [None] is selected, these fields are disabled: Submailbox, Extractability Type, and Extractability Value. Select a Sterling Integrator User which is tied to a Mailbox in a Mailbox Virtual Root to use the Mailbox Mode (Mailbox Mode is recommended). **Note:** Sterling Integrator Mailbox System requires a separate license.

Field Name	Description
SubMailbox	For Mailbox Mode only. Optional.
	Default messages received from your Remote Partner B on your local system (Local Partner A) are saved in the virtual root of Partner Mailbox B (created on the local System A).
	To make message routing simpler, you can specify a submailbox name in the Remote Physical Partner of system A so that inbound messages from Partner B are placed in a submailbox <name> of local Partner Mailbox B.
Extractability Type	Required for Mailbox Mode, only
	The Mailbox Extractability Type defines whether/how messages may be extracted from Partner Mailboxes.
	There are three types:
	◆ Extractable (Yes/No). Either extraction of messages is forbidden (No) or allowed (Yes) without limitation.
	◆ Extractable Count. Extraction of messages is allowed <Count> times.
	◆ Extractable Until (yyMMddHHmmss). Extraction of messages is allowed until a specified data/time stamp.
Extractability Value	Specifies the value for the Extractability type selected in field "Extractability Type". Default = Yes.
	Valid values are:
	Leave blank if the message cannot be extracted.Required for Mailbox Mode, only.
	Depending on the selection in Mailbox Extractability Type you have to specify an Extractability Value as follows:
	◆ Type = Extractable (Yes/No)
	Value:
	No = Extraction of messages is forbidden
	Yes = Extraction of messages is allowed without limitation.
	◆ Type = Extractable Count
	Specify number <count>=Extraction of messages is allowed <Count> times.
	◆ Type = Extractable Until (yyMMddHHmmss)
	Specify Date/Time in format (yyMMddHHmmss) = Extraction of messages is allowed until given data/time stamp.
Session Retry Intervals	Comma separated list of numbers that indicate when a session will retry if there was a failure.
	Valid values are:
	Optional.
SSIDUserField	Defined in your bilateral agreement. Optional.
Authorization Private Key	Available for Odette API Level 2.0 and higher. Required, if you enable "Secure Authentication" (checkbox "Secure Authentication in Physical Partner Contract). See *Secure Authentication* for additional information."

Field Name	Description
Authentication Certificates	Available for Odette API Level 2.0 and higher.
	Required, if you enable "Secure Authentication" (checkbox "Secure Authentication in Physical Partner Contract).
	See section: "Secure Authentication"
	Select one or more Authentication Certificates.

Physical Partner CAPI Parameters

This table describes the physical partner CAPI parameters for the physical profile:

Field Name	Description
CAPI Mode	Select CAPI Mode if you want a communication link over an ISDN telephone line. You need an ISDN router hardware with Remote CAPI ("Brick").
	In the subsequent configuration pages you need to configure IP communication specific parameters.
Address	The telephone number that either you or your partner calls. Required.
Sub Address	Additional address part. Optional.
Alternative Addresses	Comma separated list of alternative addresses (telephone numbers). List of alternative addresses (in case of a remote physical partner). Optional.
B3_ChannelConf	Comma separated list of B3 channel configuration parameters containing six integer values. Optional.
	The order is:
	◆ LIC - Lowest incoming channel. Default is 0.
	◆ HIC - Highest incoming channel. Default is 0.
	◆ LTC - Lowest two-way channel. Default is 1.
	◆ HTC - Highest two-way channel. Default is 1.
	◆ LOC - Lowest outgoing channel. Default is 0.
	◆ HOC - Highest outgoing channel. Default is 0.
BWindowSize	Transmit and receive window size for B -Channel. Default is 7. Optional.
CallUserData	X.25 parameters, entered as HEX String. Default is 0. Optional.
Facilities	X.25 parameters, entered as HEX String. Default is 0. Optional.
LocalNUA	Local X.121 address used to call. Optional.
RemoteNUA	Remote X.121 address used to call. Optional.
Modulo	Send and Receive sequence number counter in X.25 packet. Valid values are:
	◆ 8 - normal operation (default)
	◆ 128 - extended operation

Physical Partner IP Parameters

Field Name	Description
IP Mode	Select IP Mode if you want a communication link over a TCP/IP socket connection using Sterling Integrator Perimeter Service. In the subsequent configuration pages you need to configure IP communication specific parameters.
Hostname	Name or IP address of the remote host. Required.
IP Filter List	Positive list of IP v4 or IPv6 addresses.
IP Port	Additional address information. Required. Valid values: ◆ Secure Server Port: 6619 (odette-ftps) ◆ Insecure Server Port: 3305 (odette-ftp) (Default)
SSL Enabled	Default is "Disabled". Available for OFTP Version 2.0 and higher. If "SSL enabled" is selected then OFTP "Session Level Encryption" (TLS/SSL) is enabled and the following fields must be configured: ◆ Cipher Strength ◆ SSL Private Key and ◆ SSL Certificates
Cipher Strength	Default is Strong. When SSL is selected, valid values are: ◆ All ◆ Weak ◆ Strong
SSL Private Key	OFTP 2.0 and higher. Select SSL Private key, if SSL is enabled. See *Implement SSL* for additional information.
SSL Certificates List	OFTP 2.0 and higher. Select one or more SSL Certificates, if SSL is enabled. see Sterling Integrator documentation "Implement SSL" for details about SSL.

Physical Partner Contract Parameters

This table describes the physical partner contract parameters:

Field Name	Description
Physical Partner Contract Name	Unique name for the Physical Partner Contract. Required.
Description	Description of the Physical Partner Contract. Required.

Field Name	Description
Local Physical Partner	Reference to the local physical partner (reference by name). Required. Local and Remote Physical Partner must have the same communication type.
Remote Physical Partner	Reference to the remote physical partner (reference by name). Required. Local and Remote Physical Partner must have the same communication type.
Odette API Level	OFTP version. Required. Valid values are: ◆ 1.2 ◆ 1.3 ◆ 1.4 ◆ 2.0 **Note:** To use secure authentication or file compression, encryption, and signing, you must select 2.0.
SessionLogLevel	Default: System Default Log Level for Odette FTP Adapter. The SessionLogLevel allows to define a higher log level for this Physical Partner Contract than the default System Log Level of the Odette FTP Adapter. Usage: Testing. Debugging valid values are: ERROR, WARN, INFO, COMMTRACE, DEBUG, ALL
Accept SFID for non-existing Logical Partner Contract	Checkbox specifying whether Start Field Identifiers (SFIDs) are accepted for nonexistent LPC. Valid values are: ◆ Select to accept SFIDs for nonexistent LPC (default) ◆ Deselect if you do not accept SFIDs for nonexistent LPC Optional.
Credit Window Size	The Credit Window Size defines the number of consecutive Data Exchange Buffers sent by the OFTP Speaker before it must wait for a Credit (CDT) command from the Listener. The credit value is only applied to Data flow in the Data Transfer phase. The Speaker's available credit is initialized to Credit Window Size configured. After negotiation with the partner, the smallest size is selected in the answer of the Responder, otherwise an OFTP protocol error will abort the OFTP session. Negotiation of the "credit-window-size" parameter. Local Window Size m -- SSID ------------> <------------ SSID -- Remote Window Size n (n less or equal m) **Note:** The negotiated value will be "n". Maximum is 999. Default is 7. Optional.

Field Name	Description
Duplicate File Checking	Checking for duplicate files can be performed in the following check modes: ◆ No - Do not check for duplicate files. (default) ◆ SFIDDSN+ADDR - Duplicate file checking is done using fields SFIDDSN, SFIDORIG, SFIDDEST ◆ SFIDDSN+ADDR+DATE - Duplicate file checking is done using fields SFIDDSN, SFIDORIG, SFIDDEST, SFIDDATE and SFIDTIME
Duplicate File Period	Required, if Duplicate File Checking is selected (not value "No"). Defines the period of time in days (from now back into the past) which is used for searching duplicate files. Earlier duplicate files are ignored. Optional. Default is 7 days.
Secure Authentication	The Secure Authentication Protocol is available in OFTP Version 2.0 and higher and is either enabled or disabled in the OFTP SSID command depending on the Secure Authentication configuration. Valid values are: ◆ Yes ◆ No See *Secure Authentication* for additional information.
Exchange Buffer Size	Data buffer size used to transmit files. Default is 128. Optional. Minimum: 128, Maximum: 99999. The length, in octets (bytes), of the largest Exchange Data Buffer that can be accepted by the location. After negotiation with partner the smallest size will be selected.
Group Name List	Comma separated list of Physical Partner Contract Group Names. Optional. PPC Groups allows the Sterling Integrator Scheduler / Odette FTP Scheduler Service to start an "Initiator Business Process" for each Physical Partner Contract in a PPC Group automatically. Each "Initiator Business Process" starts the Odette FPT Adapter, which searches for messages to send for the given Physical Partner Contract name. For details how to configure the Sterling Integrator Scheduler for OFTP please see *OdetteFTP Scheduler and Sterling Integrator Scheduler* in *OFTP Overview*.
Send Receive Capabilities	The type of transmission possible from the local physical partner. Valid values are: ◆ Send (can only send files) ◆ Receive (can only receive file) ◆ Send/Receive (can send and receive files - (default) Optional.
Compression Capabilities	Enable OFTP data compression mode for all file Types. Optional. Valid values are: ◆ Deselect if compression will not be used ◆ Select if compression will be used

Field Name	Description
Multiple Login Sessions	Defines the number of permitted parallel inbound connections in the local system from the remote partner of this Physical Partner Contract. Default is 0 (unlimited). Default is 0.
Initiator Business Process	Business process to initiate OFTP sessions for a specific Physical Partner Contract triggered by the Sterling Integrator Scheduler. Required, if you use the Sterling Integrator Scheduler / Odette FTP Scheduler to initiate OFTP sessions (recommended). Not required in "Manual Mode". Business process to initiate OFTP sessions triggered by the specified schedules. Required.
Business Process User	A user has to be selected, if "Initiator Business Process" is selected. Application user starting this business process. Optional. Default is [Not Applicable]

Note: Each physical partner can be used in physical partner contracts either as **local** or as **remote** physical partner. But it can not be both in two different physical partner contracts. For example, one contract uses partner A as a remote partner and another contract uses partner A as a local partner. If this occurs, you must duplicate the physical partner definition and rename it (that is, A_local and A_remote). If a physical partner B acts as a Forwarder (partner in the middle) between the physical partners A and C the two physical partner contracts needed both contain B as local physical partner.

Logical Partner Parameters

This table describes the logical partner parameters:

Field Name	Description
Logical Partner Name	Unique name for the Logical Partner. Required.
Description	Description of the Logical Partner. Required.
Contact Person	Name of a contact person. Optional.
Odette Name	OFTP identification. Required.
File Service Private Key	File Services are available in OFTP Version 2.0 and higher.
	Select a File Service Private Key if you want to use e.g. OFTP file encryption, Signing using Cryptographic Message Systax (CMS).
	See OFTP 2.0 specification for details about "File Services".
	Optional.
File Service Certificate List	Select one or more File Service Certificates if you want to use e.g. OFTP file encryption, Signing using Cryptographic Message Systax (CMS). See OFTP 2.0 specification for details about "File Services".
	Optional.
	Select a CA- or Trusted- certificate.

Logical Partner Contract Parameters

This table describes the logical partner contract parameters:

Field Name	Description
Logical Partner Contract Name	Unique name for the Logical Partner Contract. Required.
Description	Description of the Logical Partner Contract. Required.
Destination Logical Partner	References the destination logical partner (referenced by name). Required.
Originator Logical Partner	Specifies the originator logical partner (referenced by name). Required.
Inbound Physical Partner Contract	If you want to send messages to your remote partner or poll the remote partner for files in the Mailbox Inbox (Initiator role) then specify a Outbound Physical Partner Contract. This means that you initiate the OFTP session with your remote OFTP partner, you may (optionally) send files in phase 1 and - after a OFTP Change Direction command - optionally receive files from your partner in phase 2 in the same session (if the remote partner has files to send for you).
	If you want to receive messages from your remote partner (Responder role) and the remote partner should call you then specify an Inbound Physical Partner Contract. This implies that your Remote Partner initiates the OFTP Session, e.g. for polling files in the Mailbox Inbox. After receiving files from your remote partner you may optionally send back files to the remote partner after the OFTP Change Direction command in the same OFTP session.
	If you want to forward a message to Partner C (using outbound PPC) which you - Partner B - received from Remote Partner A (using Inbound PPC) then you have to specify both Inbound and Outbound Physical Partner Contracts.
Outbound Physical Partner Contract	Reference to the sending PhysicalPartnerContracts (referenced by name). Either InboundPhysicalPartnerContract or OutboundPhysicalPartnerContract is required.
Inbound Business Process	Select a business process that will be initiated when a message or EERP/NERP is received for this Logical Partner Contract. If [Not Applicable] is selected then the business process configured in the adapter instance configuration is used. Optional.
Business Process User	Select a Sterling Integrator user used to execute the Inbound Business Process. Optional. Default is "admin". Required, if Inbound Business Process is selected.
Char Encoding	The selected character code will be used as property of the Primary Document or Mailbox Messages created for an inbound file.
OFTP File User Field	Defined in the bilateral agreement with your partner. Optional.

Field Name	Description
Default OFTP Virtual Filename	String specifying the default virtual filename. It is used in following cases: ♦ If the message has been scheduled with the Odette FTP Queue Manager and no file name has been provided in the XML DataSet. Note: It is recommended to provide virtual file names when scheduling files. ♦ In Manual Mode, when the Odette FTP Adapter is called directly with a XML DataItem and no virtual file name has been provided. Note: It is recommended to provide a file name when calling Odette FTP Adapter in Manual Mode. The Default OFTP Filename is overwritten by the File names provided in the XML DataItem Sets.Required.
Receive Virtual Filename Pattern	Defines a character pattern in Regular Expression format which is used to validate the Virtual File Name Pattern for inbound messages as follows. The following cases can occur: ♦ If an inbound message arrives the Odette FTP Adapter first searches for a matching Logical Partner Contract (without using the fine name pattern). ♦ If no LPC is found then the message is accepted if field "Accept SFID for non-existing Logical Partner Contract" is enabled (otherwise it is rejected). ♦ If exactly one LPC is found the message is accepted, if the Receive Virtual Filename Pattern matches the inbound message virtual file name - otherwise it is rejected. If "Receive Virtual Filename Pattern" is left empty or has a wildcard value "*", the message is always accepted. ♦ If more than one LPC is found then the Receive Virtual File Name Pattern is used to identify exactly one LPC from the list of LPCs. ♦ If there are zero or more than one LPC matching (after performing file name pattern matching) then the message is rejected. In all other cases (exactly one LPC matches) the message is accepted. **Note:** If the pattern field is used, it is the responsibility of the user to make sure that the file name pattern uniquely identifies one LPC, for example, by using "<prefix>*". Especially, if more than one LPC file pattern is defined as wildcard "*" then the file pattern criteria will always leave the LPC decision ambiguous and the message will be rejected.
File Format	File format of the transmission file, for Outbound only. Optional. Valid values are: ♦ Unstructured Binary file (default) ♦ Fixed format binary file ♦ Variable format binary file ♦ Text

Field Name	Description
Record Delimiter	Depending on File Format: One or two record delimiters (decimal numbers of Character code, e.g. 13,10 for <CR> <LF> (Windows) or 10 for <LF> (UNIX).
	File Format " Unstructured Binary file" ("U") / "Text" ("T"):
	Data is not split up in records. Delimiters are not used.In the OFTP Partner Profile database both Record Delimiters are set to (-1,-1).
	File Format "Variable format binary file" ("V"):
	Data is split up in records separated by one or optionally two record delimiters. Specify one or two delimiters as decimal values. Specify -1,-1 to use Operating system dependent default delimiter (13,10 for Windows and 10 for UNIX)
	File Format "Fixed Format binary file":
	Data is split up in records of length <Record Length>
	For Format "F" there are following special cases:

Records Length	Specifies number of retries for file transmissions. This field is used for outbound only.
File Transmission Retries	Reserved for future use.
Monitor EERP Reception	For a send message it is checked, whether a EERP arrives within a given time period in minutes (EERP Timeout). If the EERP arrives later than specified in EERP Timeout, a Visibility event is created.
	Disabled: Do not monitor EERPs.
EERP Timeout	If the EERP Timeout limit in minutes is exceeded a Visibility event is created.
	Note: Replaces field WaitForEERP in Sterling Integrator 4.3 and older.
Monitor Send Queue	Enabled: For a message with status "SCHEDULED" it is checked, whether a time limit (File Schedule Timeout) has been exceeded. If yes, a Visibility Event is created. The Feature can be used to make sure that a message is sent within a given time frame.
	Disabled: Do not care how long a message stays in Status "SCHEDULED".
File Schedule Timeout	Time limit in minutes how long a message is allowed to stay in Status "SCHEDULED".
File Compression	File Compression File Service is available in OFTP Version 2.0 and higher. Optional.
	See OFTP 2.0 specification for details about File Services.
File Encryption	File Encryption File Service is available in OFTP Version 2.0 and higher. Optional.
	Enable File Encryption to enforce Integrity of file content.
	See OFTP 2.0 specification for details about File Services.

Field Name	Description
File Signing	File Signing File Service is available in OFTP Version 2.0 and higher. Optional.
	Signing of files allows non-repudiation of origin.
	See OFTP 2.0 specification for details about File Services.
Send EERP	When to send an EERP. Required. Valid values are:
	Always (default)
	Never
	Pass through (EERP/NERP forwarding)
Signed EERP Request	EERP Signing is available in OFTP Version 2.0 and higher. Optional.
	Signing of receipts allows Non-repudiation of receipts. The Originator of the virtual file may request a signed EERP in the SFID. The signature of the EERP is in CMS format.
	See OFTP 2.0 specification for details about File Services.
EERP/NERP Signature Check	EERP Signature check is available in OFTP Version 2.0 and higher. Optional.
	While signing of receipts allows Non-repudiation of receipts parameter "EERP/NERP Signature Check" specifies whether the partner who receives an EERP/NERP wants to check the signature contained in the EERP/NERP.
	See OFTP 2.0 specification for details about how the EERP/NERP Signature is checked against local certificates.
Cipher Suite	OFTP Version 2.0 specifies the mandatory list of Cipher Suites and the required key lengths:
	◆ AES_256_CBS_RSA_PKCS1_15 SHA-1 (sym., 256bit key)
	◆ 3DES_EDE_CBS_3KEY_RSA_PKCS1_15 SHA-1 (3 different 64 bit keys)
	Where CBS = Cyclic Block Chaining Mode, EDE = Encryption Decryption Encryption
	Both cipher suites use asymmetric RSA_PKCS1_15 with RSA Padding defined in PKCS#1 and SHA-1 for Hashing.

Managing Partner Profile with PartnerManager

The PartnerManager is a robust tool that performs different operations on one or more Odette FTP Partner Profile elements, such as doing mass imports or exports.

Use the command line tool PartnerManager to:

✦ Import a PartnerProfile.xml file into the Sterling Integrator database (Odette FTP Partner Profile) or perform a consistency check of a new PartnerProfile.xml file.

✦ Export from the Sterling Integrator database (Odette FTP Partner Profile) one or more partner profile elements into a PartnerProfile.xml file.

✦ Delete one or more partner profile elements in the Sterling Integrator database (Odette FTP Partner Profile). Alternatively, to get an initialized state, all entries can be deleted.

✦ List one or more partner profile records from the Sterling Integrator database (Odette FTP Partner Profile) in a short overview containing only the names of the partner profile elements.

The PartnerProfile XML file used in import or export has the structure as described in *PartnerProfile XML Setup*.

Caution: Use caution when executing PartnerManager (performing Sterling Integrator database write operations) while your Sterling Integrator instance is still running. Especially when Odette FTP Adapters are enabled and executing OFTP sessions. It is recommended that you close Sterling Integrator or verify that no OFTP sessions will take place, for example, by disabling all Odette FTP Adapters).

Usage and command line syntax

The PartnerManager gets invoked by executing in Sterling Integrator's bin directory the script (Windows cmd) OFTPPartnerManager.sh (Windows: OFTPPartnerManager.cmd).

When executing without any parameters, a usage screen appears that shows the operations that can be performed:

```
Usage: PartnerManager <command>
  where:

    <command> ::= [<importCommmand>] <PartnerProfileName> [-cleandb]
                || -delete all | <selection>
                || -export <exportSelection> [<exportfilename>]
                || -list   all | <selection>

      <importCommmand>   ::= -insert || -update || -replace || -flatinsert
                             || -simulate

      <selection>        ::= <elementList>
      <exportSelection>  ::= allflat | alltree | <selection>
      <elementList>      ::= <element>=<name||"*"> [<elementList>]
      <element>          ::= PhysicalPartner || pp
                             || PhysicalPartnerContract || ppc
                             || LogicalPartner || lp
                             || LogicalPartnerContract  || lpc
```

The key <name> in <elementList> specifies a particular name of a one of the selectable elements pp, ppc, lp or lpc.

PartnerManager's tree view on the elements of the Partner Profile

This section describes the procedure how the PartnerManager performs its operations on the different types of elements of the Odette FTP Partner Profile. For additional information, see *Odette FTP Partner Profile Overview*. Elements are treated as **nodes** that are connected as **trees**, if possible. For this model, it does not make a difference whether the Partner Profile is in the Sterling Integrator database or in an XML file.

For notation of a tree in the subsequent chapters a tree t (one node with its direct children) will be written as

`t (node_1, .. , node_n)` or **`t_name (node_1, .. , node_n)`**

```
where:
```
- `t is one of {pp, ppc, lp, lpc}`
- `t_name is one t combined with a name (e.g. pp_local or lpc_3)`
- `the nodes node1, .. , node_n can be simple trees, too.`

There are only four different kinds of trees that can occur in a Partner Profile:

1. The simplest tree has only one root node and no children. These are the Physical Partners (pp) or Logical Partners (lp) in an isolated view.
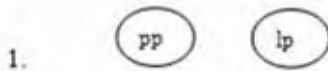
2. PhysicalPartnerContract (ppc) with its local (pp_local) and remote (pp_remote) Physical Partners:
   pp_local ⇓ ppc ◊ pp_remote
   or described in notation above as *ppc (pp_local, pp_remote)*
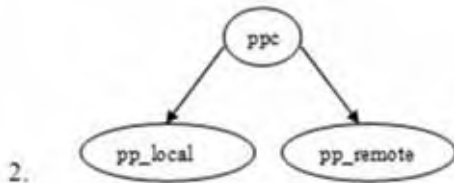
3. Logical Partner Contract (lpc) with:

   ◆ One Physical Partner Contract as a subtree (see above) (either inbound or outbound)

   ◆ Two Logical Partners (lp): one Originator (lp_orig) and one Destination (lp_dest)

   This results in the following tree: *lpc_3 (lp_orig, lp_dest, ppc(pp_local, pp_remote))*
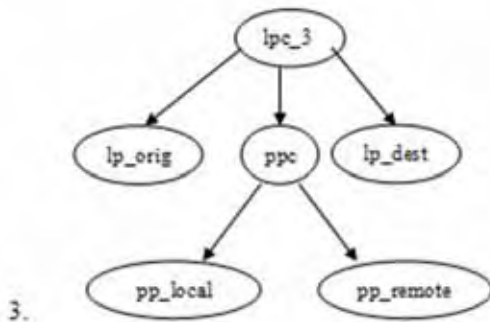
4. Logical Partner Contract (lpc) with:

◆ Two – inbound and outbound – Physical Partner Contracts: ppc_inb, ppc_outb where each of the ppc's have their own Physical Partners pp_X_local, pp_X_remote (X = inb or outb)

◆ Two Logical Partners: one Originator (lp_orig) and one Destination (lp_dest)

This creates in the following tree:

lpc_4 (lp_orig, lp_dest,

ppc_inb(pp_inb_local, pp_inb_remote),

ppc_outb(pp_outbb_local, pp_outb_remote))

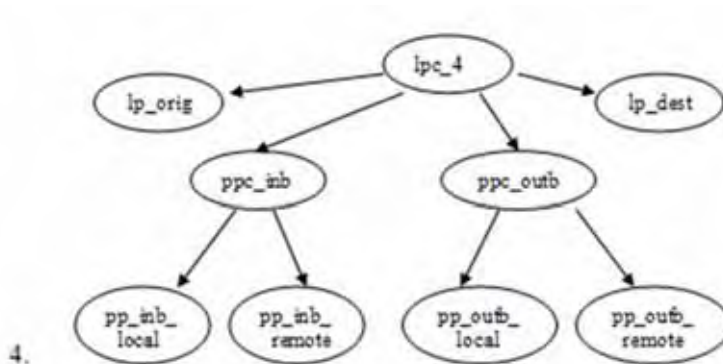These four types are "complete" because all references inside the trees are resolved. However, under certain conditions it is possible to have incomplete trees (see import Operation). For example, a Physical Partner Contract with only one local Physical Partner but no remote PhysicalPhysical Partner is incomplete because of one unresolved reference.

Trees where the root node is a Logical Partner Contract have **maximal size** because they can not be extended any more. These are the trees of type 3 and 4.

The import and export operations in PartnerManager are executed on one or more trees as described above.

The following sections will describe the different commands in detail.

PartnerManager - Import Operation

PartnerManager *[<importcommand>] <PartnerProfileName> [-cleandb] [passphrase <oldPwd>]*

There are five different modes that can be used when importing a PartnerProfile.xml into Sterling Integrator, as shown in the command line syntax for the *importcommand*.

✦ **insert**: all elements of the PartnerProfile.xml file will be imported organized as trees with maximum size and only as new elements into the Sterling Integrator database. If one of the elements from a tree exist in the database, the import of the whole tree will be canceled and the program will continue with the next trees.

✦ **update**: only those elements of the PartnerProfile.xml file that are not in the Sterling Integrator database will be imported. As in insert - mode, the elements are organized as trees with a maximum size. With this mode, only new elements, not part of the Sterling Integrator database, get imported without touching the remaining ones.

✦ **replace**: same as insert except that existing elements are completely replaced by their new counterparts that are going to be imported.

✦ **flatinsert**: same as insert – mode except that import is performed without using trees; however, this mode should be used carefully because it can lead to inconsistent trees in the Sterling Integrator database.

✦ **simulate**: this mode only parses the PartnerProfile.xml file and checks for consistency of its elements but without importing them into Sterling Integrator. This mode should be used first when a new PartnerProfile.xml file was created and the user wants to check it only.

The parameter *<PartnerProfileName>* must be specified and locates the PartnerProfile.xml file to be read from.

If the optional parameter –cleandb is specified before import the whole Odette FTP Partner Profile in the Sterling Integrator database is emptied.

Caution: This parameter should be used with care. If not used correctly, all data in the Odette FTP Partner Profile is lost!

Notes:

✦ If the optional parameter passphrase <oldPwd> is specified, all OFTPUserPasswords of PhysicalPartners in the file to be imported will be decrypted with the passphrase <oldPwd> and then again encrypted with the passphrase of the actual Sterling Integrator system. This parameter must only be used if the passphrases of the two Sterling Integrator systems are different.

✦ To help identify whether an element being imported is part of the database, a unique name is used as a compare key. This implies that there are no two elements (such as, Physical Partners) with the same name.

✦ During import from every Physical Partner to be imported, the OFTP User Password field is selected. If it is not in encrypted format the import right now asks for the corresponding OFTP User Password. It will then be encrypted before the OFTP User Password field is imported into the Sterling Integrator database. Please note that the import file itself will not be changed. If you do not want to be asked for the OFTP User Password during import, you must verify that it is already set. This will be done by the OFTP Password Encryption tool, see *OFTP Password Encryption tool* for additional information.

✦ During import, imported trees can be incomplete under the restriction that all missing references are already part of the database. For example, it is possible to import only a new PhysicalPartnerContract where its referenced Physical Partners already exist in Sterling Integrator database (Odette FTP Partner Profile). If during import an error occurred, an error is written in OdetteFTP.log and the complete tree that could not be inserted is written into a new export file named as the original added with the extension ".exp". This is designed to allow you direct access to only the rejected Partner Profile data and after correction can import this file separately in a second step without the need to import the whole original file again.

PartnerManager - export Operation

PartnerManager *–export <exportSelection> [<exportfilename>] [passphrase <newPwd>]*

According to the command line syntax for the *-export* command in 2.2.1 there are three different exportSelections possible that can be used when exporting elements or trees from Odette FTP Partner Profile in Sterling Integrator database into a xml file:

allflat: all **elements** of the Sterling Integrator database will be exported in the sequence

1. Physical Partners

2. Physical Partner Contracts

---

3. Logical Partners

4. Logical Partner Contracts

Because the sequence is opposite to the order a tree is built from root no trees bigger than a simple node - tree will be grouped in the exportfile.

alltree: all **trees** of the Sterling Integrator database will be exported in the sequence.

1. Logical Partner Contracts: these trees with maximal size (type 3 or 4) get exported as trees first.

2. Logical Partners, not being part of any Logical Partner Contract, will get exported next.

3. Physical Partner Contracts, not being part of any Logical Partner Contract, will get exported next as trees.

4. Physical Partners, still not exported before will get exported as remaining stuff.

<selection>: the specified list performs the export of **trees** in exactly this order as it was specified. However an element is never exported twice although it might occur as root or as child in one or more trees.

If *<exportfilename>* is specified the export data is written to that file. If not specified the export data is written to the default filename PartnerProfileManager.xml in current directory.

PartnerManager - delete Operation

PartnerManager *–delete all | <selection>*

If the optional parameter passphrase <newPwd> is specified, all OFTPUserPasswords of PhysicalPartners being exported will be decrypted with the passphrase of the Sterling Integrator system and then again encrypted with the passphrase <newPwd>. The created exportfile can no longer be imported into the Sterling Integrator system because its OFTPUserPasswords are now encrypted with the passphrase of the second Sterling Integrator system. This parameter must only be used if the passphrases of the two Sterling Integrator systems are different.

According to the command line syntax for the *delete command* in 2.2.1 with this operation, one or all trees of one or more element types can be deleted from the Odette FTP Partner Profile in Sterling Integrator database. For example, the command –delete lpc="*" would try to delete all Logical Partner Contracts with their corresponding Physical Partners.

The deletion of a particular element **e** from the deletelist **L** (all elements enumerated in <elementlist>) takes place only if it can be deleted. It can be deleted if one of the following occurs:

✦ There is no tree in Odette FTP Partner Profile that has t as its child directly or indirectly

✦ If there is a tree t2 in Odette FTP Partner Profile that has t as its child t2 it must belong to the deletelist L.

As an example take the maximal tree type number 3 *lpc_3 (lp_orig, lp_dest, ppc(pp_local, pp_remote))* from chapter 2.2.1.

Trying to delete only lp_orig in comment *-delete lp=lp_orig* would violate rule 1 because lp_orig is a child from tree lpc_3. The first selection criteria *lp=lp_orig* in command *–delete lp=lp_orig,lpc=lpc_3* violates rule 1 too, but it grants rule 2. lpc_3 itself can not be referenced by another element, therefore it grants rule 1.

The command *–delete all* involves emptying the complete Odette FTP Partner Profile without any conditions.

Note: Be careful when using this command because it can not be undone! At best make sure that you always have a backup of the Odette FTP Partner Profile database configuration (using PartnerManager's export command) before deleting parts of the partner configuration.

PartnerManager - list Operation

PartnerManager *–list all | <selection>*

According to the command line syntax for the *-list command* in 2.2.1 with this operation, an overview by names of a particular element or all elements of one or more type in the Odette FTP Partner Profile will be listed. For example the command –list lp="*", lpc="*" will print out all Logical Partners and then all Logical Partner Contracts with their names to stdout.

Partner Profile XML Setup

The Partner Profile XML file is a configuration file in XML format which is used by the OFTPPartnerManager command line tool for mass importing, exporting or deleting OFTP Partner Pofiles into/from Odette FTP Profile Database.

The Partner Profile consists of the following:

✦ One General Parameters section which currently contains only the mandatory field: PartnerProfileVersion.

✦ Physical Partners and Physical Partner Contracts that are specified in one or more PhysicalPartnerSpec targets. A PhysicalPartnerContract consists of the local and the remote physical partner that are used to establish the OFTP communication link between those two physical partners, in addition to other data.

✦ Logical Partners and Logical Partner Contracts that are specified in one or more LogicalPartnerSpec targets. A LogicalPartnerContract contains (in addition to other data):

- ◆ The OriginatorLogicalPartner
- ◆ The DestinationLogicalPartner
- ◆ PhysicalPartnerContract (inbound and/or outbound)

The LogicalPartnerContract is the entry point for all ongoing OFTP communication. It references all corresponding logical partner information and the PhysicalPartnerContracts.

Partner Profile General Parameters

This table describes the general parameter for the Partner Profile:

Field	Description
PartnerProfileVersion	Specifies the version of the partner profile. PartnerProfileVersion is used to identify changes in the Partner Profile, such as added, removed, or changed fields or XML structures. The services and adapters check to ensure they can read the partner profile. Version 3.0. Required.

Physical Partner

This table describes the fields for a physical partner.

XML structure element: <PhysicalPartner name="unique name" type="CommType">

CommType can either be IP or ISDN (see below).:

Field Name	Description
Description	Textual description of the Physical Partner. Optional.
OFTPUserID	The OFTP ID used in the SSID command. Must be defined in the bilateral agreement with your partner. Required.
OFTPUserPassword	The OFTP password used in the SSID command. Must be defined in the bilateral agreement with your partner. Required.
	Note: For security reasons, the OFTPUserPassword content must be encrypted in the partner profile. For details see PartnerManager import or OFTP Password Encryption.
MailboxUser	User name in the Application Mailbox system. Optional. The value of this field determines whether the "Mailbox Mode" is used or not.
	None: Select this if you do not want to use the Sterling Integrator Mailbox System at all. Select a Sterling Integrator User which is tied to a Mailbox in a Mailbox Virtual Root to use the Mailbox Mode. (Mailbox Mode is recommended. Note: Sterling Integrator Mailbox System requires a separate license)
SubMailbox	Required for Mailbox Mode, only:
	As a default messages received from your Remote Partner B on your local system (Local Partner A) are saved in the virtual root of Partner Mailbox B which is created on the local System A. For making message routing simpler, you can specify a submailbox name in the Remote Physical Partner of system A so that inbound messages from Partner B are placed in a submailbox <name> of local Partner Mailbox B.

Field Name	Description
ExtractabilityType	Required for Mailbox Mode, only
	The Mailbox Extractability Type defines whether/how messages may be extracted from Partner Mailboxes.
	There are three types:
	◆ Extractable (Yes/No). Either extraction of messages is forbidden (No) or allowed (Yes) without limitation.
	◆ Extractable Count. Extraction of messages is allowed <Count> times.
	◆ Extractable Until (yyMMddHHmmss). Extraction of messages is allowed until a specified data/time stamp.
	◆ One of the next three lines can be chosen:
	<Extractability type="Extractable">yes or no</Extractability>
	<Extractability type="ExtractableCount">count</Extractability>
	<Extractabilitytype="ExtractableUntil">yyMMddHHmmss</Extractability>
	Depending on the selection in Mailbox Extractability Type you have to specify an Extractability Value as follows:
	◆ Type = Extractable (Yes/No)
	Value:
	No = Extraction of messages is forbidden
	Yes = Extraction of messages is allowed without limitation.
	◆ Extractable Count
	Specify number <count>=Extraction of messages is allowed <Count> times.
	◆ Extractable Unitl (yyMMddHHmmssyyMMddHHmmss)
	Specify Date/Time in format (yyMMddHHmmss) = Extraction of messages is allowed until given data/time stamp.
SessionRetryIntervals	Comma or blank separated list of numbers (in seconds) that indicate when a session will retry if there was a failure.
	Optional.
SSIDUserField	Defined in your bilateral agreement. Optional.
AuthenticationCertificates	Available for Odette API Level 2.0 and higher.
	Required, if you use "Secure Authentication" (field "Secure Authentication in Physical Partner Contract).
	For additional information, see *Partner Profile XML Setup* on page 18.

Physical Partner CAPI Parameters

This table describes the physical partner CAPI parameters for the physical profile:

Field Name	Description
CAPIMode	Select CAPI Mode if you want a communication link over an ISDN telephone line. You need an ISDN router hardware with Remote CAPI ("Brick").
	In the subsequent configuration pages you need to configure CAPI communication specific parameters.
Address	The telephone number that either you or your partner calls. Required.
SubAddress	Additional address part. Optional.
AlternativeAddresses	Comma or blank separated list of alternative addresses (telephone numbers). List of alternative addresses (in case of a remote physical partner). Optional.
B3_ChannelConf	Comma or blank separated list of B3 channel configuration parameters containing exactly six integer values (optional). The order is:
	◆ LIC - Lowest incoming channel. Default is 0.
	◆ HIC - Highest incoming channel. Default is 0.
	◆ LTC - Lowest two-way channel. Default is 1.
	◆ HTC - Highest two-way channel. Default is 1.
	◆ LOC - Lowest outgoing channel. Default is 0.
	◆ HOC - Highest outgoing channel. Default is 0.
BWindowSize	Transmit and receive window size for B -Channel. Default is 7. Optional.
CallUserData	X.25 parameters, entered as HEX String. Default is 0. Optional.
Facilities	X.25 parameters, entered as HEX String. Default is 0. Optional.
LocalNUA	Local X.121 address used to call. Optional.
RemoteNUA	Remote X.121 address used to call. Optional.
Modulo	Send and Receive sequence number counter in X.25 packet. Valid values are:
	◆ 8 - normal operation (default)
	◆ 128 - extended operation

Physical Partner IP Parameters

Field Name	Description
IPMode	Select IP Mode if you want a communication link over a TCP/IP socket connection using Sterling Integrator Perimeter Service.
	In the subsequent configuration pages you need to configure IP communication specific parameters.
Hostname	Name or IP address of the remote host. Required.
IPFilterList	Positive list of IP addresses (can be IPv4 or IPv6 address format).
IPPort	Additional address information. Required.
	Valid values:
	◆ Secure Server Port: 6619 (odette-ftps)
	◆ Insecure Server Port: 3305 (odette-ftp) (Default)
SSL	Available for OFTP Version 2.0 and higher. Default is SSL_NONE which means SSL is disabled.
	If the value is SSL_MUST, then OFTP "Session Level Encryption" (TLS/SSL) is enabled and the following fields must be configured:
	◆ Cipher Strength
	◆ SSL Private Key and/or
	◆ SSL Certificates
CipherStrength	Available for OFTP Version 2.0 and higher. Default is Strong. When SSL is selected, valid values are:
	◆ All
	◆ Weak
	◆ Strong
SSLCertificates	SSL Certificates.
	OFTP 2.0 and higher.
	Specify one or more SSL Certificates, if SSL is enabled.
	For additional information, see *Partner Profile XML Setup* on page 18.

Physical Partner Contract

This table descriptions the fields for a physical partner contract.

XML structure element: <PhysicalPartnerContract name="unique name" >j

Field Name	Description
Description	Description of the Physical Partner Contract. Optional.

Field Name	Description
LocalPhysicalPartner	Reference to the local physical partner (reference by name). Required. Local and Remote Physical Partner must have the same communication type.
RemotePhysicalPartner	Reference to the remote physical partner (reference by name). Required. Local and Remote Physical Partner must have the same communication type.
OdetteFTPAPILevel	OFTP version. Required. Valid values are: ◆ 1.2 ◆ 1.3 ◆ 1.4 ◆ 2.0 **Note:** To use secure authentication or file compression, encryption, and signing, you must select 2.0.
AcceptSFIDsForNonLPC	Boolean value specifying whether Start Field Identifiers (SFIDs) are accepted for nonexistent LPC. Optional.
CreditWindowSize	The Credit Window Size defines the number of consecutive Data Exchange Buffers sent by the OFTP Speaker before it must wait for a Credit (CDT) command from the Listener. The credit value is only applied to Data flow in the Data Transfer phase. The Speaker's available credit is initialized to Credit Window Size configured. After negotiation with the partner, the smallest size is selected in the answer of the Responder, otherwise an OFTP protocol error will abort the OFTP session. Negotiation of the "credit-window-size" parameter. Local Window Size m -- SSID ------------> <------------ SSID -- Remote Window Size n (n less or equal m) **Note:** The negotiated value will be "n". Maximum is 999. Default is 7. Optional.
DuplicateFileChecking	Checking for duplicate files can be performed in the following check modes: ◆ No - Do not check for duplicate files. (default) ◆ SFIDDSN+ADDR - Duplicate file checking is done using fields SFIDDSN, SFIDORIG, SFIDDEST ◆ SFIDDSN+ADDR+DATE - Duplicate file checking is done using fields SFIDDSN, SFIDORIG, SFIDDEST, SFIDDATE and SFIDTIME
DuplicateFilePeriod	Required, if Duplicate File Checking is selected (not value "No"). Defines the period of time in days (from now back into the past) which is used for searching duplicate files. Earlier duplicate files are ignored. Optional. Default is 7 days.

Field Name	Description
SecureAuthentication	The Secure Authentication Protocol is available in OFTP Version 2.0 and higher and is either enabled or disabled in the OFTP SSID command depending on the Secure Authentication configuration.
	Valid values are:
	◆ Yes
	◆ No
	See *Secure Authentication* for additional information.
ExchangeBufferSize	Data buffer size used to transmit files. Default is 128. Minimum: 128, Maximum: 99999. The length, in octets (bytes), of the largest Exchange Data Buffer that can be accepted by the location. After negotiation with partner the smallest size will be selected. Optional.
SessionLogLevel	Default: System Default Log Level for Odette FTP Adapter. The SessionLogLevel allows to define a higher log level for this Physical Partner Contract than the default System Log Level of the Odette FTP Adapter. Usage: Testing. Debugging valid values are: ERROR, WARN, INFO, COMMTRACE, DEBUG, ALL
GroupNameList	Comma separated list of Physical Partner Contract Group Names. Optional.
	PPC Groups allows the Sterling Integrator Scheduler / Odette FTP Scheduler Service to start an "Initiator Business Process" for each Physical Partner Contract in a PPC Group automatically. Each "Initiator Business Process" starts the Odette FTP Adapter, which searches for messages to send for the given Physical Partner Contract name.
	For details how to configure the Sterling Integrator Scheduler for OFTP please see *OdetteFTP Scheduler and Sterling Integrator Scheduler* in *OFTP Overview*.
SendReceiveCapabilities	The type of transmission possible from the local physical partner. Valid values are:
	◆ S: Can only send files)
	◆ R: Can only receive file)
	◆ B: Send/Receive (can send and receive files - (default)
	Optional.
CompressionCapabilities	Support OFTP data compression mode for file types U=Unstructured data, T=Text files, V=Variable record length and F=Fixed record length. Optional. Valid values are:
	◆ No if compression will not be used
	◆ Yes if compression will be used
MultipleLoginSessions	Defines the number of permitted parallel inbound connections in the local system from the remote partner of this Physical Partner Contract. Default is 0 (unlimited).

Field Name	Description
InitiatorBusinessProcess	Business process to initiate OFTP sessions for a specific Physical Partner Contract triggered by the Sterling Integrator Scheduler. Required, if you use the Sterling Integrator Scheduler / Odette FTP Scheduler to initiate OFTP sessions (recommended). Not required in "Manual Mode". Business process to initiate OFTP sessions triggered by the specified schedules. Required.
BusinessProcessUser	A user has to be selected, if "Initiator Business Process" is selected. Optional. Default is admin.

Note: Each physical partner can be used in physical partner contracts either as **local** or as **remote** physical partner. But it can not be both in two different physical partner contracts. For example, one contract uses partner A as a remote partner and another contract uses partner A as a local partner. If this occurs, you must duplicate the physical partner definition and rename it (that is, A_local and A_remote). If a physical partner B acts as a Forwarder (partner in the middle) between the physical partners A and C the two physical partner contracts needed both contain B as local physical partner.

Logical Partner

This table describes the fields of a logical partner.

XML structure element: <LogicalPartner name="unique name" >

Field Name	Description
Description	Description of the Logical Partner. Optional.
ContactPerson	Name of a contact person. Optional.
OdetteName	OFTP identification. Required.
FileServicePrivateCertificate	File Services are available in OFTP Version 2.0 and higher. Use a File Service Certificate if you want to use e.g. OFTP file encryption, Signing using Cryptographic Message Systax (CMS). See OFTP 2.0 specification for details about "File Services". For specification see more details in chapter "Specifying Certificates in Partner Profile XML Setup". Optional.

Logical Partner Contract

This table describes the fields for a logical partner contract.

XML structure element: <LogicalPartnerContract name="unique name" >

Field Name	Description
Description	Description of the Logical Partner Contract. Optional.
DestinationLogicalPartner	References the destination logical partner (referenced by name). Required.
OriginatorLogicalPartner	Specifies the originator logical partner (referenced by name). Required.

Field Name	Description
InboundPhysicalPartnerContract	If you want to send messages to your remote partner or poll the remote partner for files in the Mailbox Inbox (Initiator role) then specify a Outbound Physical Partner Contract. This means that you initiate the OFTP session with your remote OFTP partner, you may (optionally) send files in phase 1 and - after a OFTP Change Direction command - optionally receive files from your partner in pahse 2 in the same session (if the remote partner has files to send for you).
	If you want to receive messages from your remote partner (Responder role) and the remote partner should call you then specify an Inbound Physical Partner Contract. This implies that your Remote Partner initiates the OFTP Session, e.g. for polling files in the Mailbox Inbox. After receiving files from your remote partner you may optionally send back files to the remote partner after the OFTP Change Direction command in the same OFTP session.
	If you want to forward a message to Partner C (using outbound PPC) which you - Partner B - received from Remote Partner A (using Inbound PPC) then you have to specify both Inbound and Outbound Physical Partner Contracts.
OutboundPhysicalPartnerContract	Reference to the sending PhysicalPartnerContracts (referenced by name). Either InboundPhysicalPartnerContract or OutboundPhysicalPartnerContract is required.
InboundBusinessProcess	Select a business process that will be initiated when a message or EERP/NERP is received for this Logical Partner Contract. If [Not Applicable] is selected then the business process configured in the adapter instance configuration is used. Optional.
BusinessProcessUser	Select a Sterling Integrator user used to execute the Inbound Business Process. Optional. Default is "admin". Required, if Inbound Business Process is selected.
CharEncoding	The specified character code will be used as property of the Sterling Integrator Document created for an inbound file.The charset must be registered in the IANA Charset Registry (see java-doc for java.nio.charset.Charset). Optional; Default: ISO-8859-1
OFTPFileUserField	Defined in the bilateral agreement with your partner. Optional.
DefaultOFTPVirtualFilename	String specifying the default virtual filename. It is used in following cases:
	◆ If the message has been scheduled with the Odette FTP Queue Manager and no file name has been provided in the XML DataSet. Note: It is recommended to provide virtual file names when scheduling files.
	◆ In Manual Mode, when the Odette FTP Adapter is called directly with a XML DataItem and no virtual file name has been provided. Note: It is recommended to provide a file name when calling Odette FTP Adapter in Manual Mode.
	The Default OFTP Filename is overwritten by the File names provided in the XML DataItem Sets.Required.

Field Name	Description
ReceiveVirtualFilenamePattern	Defines a character pattern in Regular Expression format which is used to validate the Virtual File Name Pattern for inbound messages as follows. The following cases can occur: ◆ If an inbound message arrives the Odette FTP Adapter first searches for a matching Logical Partner Contract (without using the fine name pattern). ◆ If no LPC is found then the message is accepted if field "Accept SFID for non-existing Logical Partner Contract" is enabled (otherwise it is rejected). ◆ If exactly one LPC is found the message is accepted, if the Receive Virtual Filename Pattern matches the inbound message virtual file name - otherwise it is rejected. If "Receive Virtual Filename Pattern" is left empty or has a wildcard value "*", the message is always accepted. ◆ If more than one LPC is found then the Receive Virtual File Name Pattern is used to identify exactly one LPC from the list of LPCs. ◆ If there are zero or more than one LPC matching (after performing file name pattern matching) then the message is rejected. In all other cases (exactly one LPC matches) the message is accepted. **Note:** If the pattern field is used, it is the responsibility of the user to make sure that the file name pattern uniquely identifies one LPC, for example, by using "<prefix>*". Especially, if more than one LPC file pattern is defined as wildcard "*" then the file pattern criteria will always leave the LPC decision ambiguous and the message will be rejected.
FileFormat	File format of the transmission file. Optional. Valid values are: ◆ U - Unstructured Binary file (default) ◆ F - Fixed format binary file ◆ V - Variable format binary file ◆ T - Text

Field Name	Description
RecordDelimiter	Contingent on File Format. Includes one or two record delimiters (decimal numbers of Character code, for example, 13,10 for <CR><LF> (Windows) or 10 for <LF> (UNIX). File Format for Unstructured Binary file ("U") / "Text" ("T"): ◆ Data is not spit up in records. ◆ Delimiters are not used. ◆ In the OFTP Partner Profile database both Record Delimiters are set to (-1,-1). File Format for Variable format binary file ("V"): ◆ Data is split up in records separated by one or optionally two record delimiters. ◆ Specify one or two delimiters as decimal values. ◆ Specify -1,-1 to use Operating system dependent default delimiter (13,10 for Windows and 10 for UNIX) File Format "Fixed Format binary file": ◆ Data is split up in records of length <Record For Format "F" there are following special cases:

Format	Rec Len	Del 1	Del 2	Sending Party	Receiving Party
F	<rec. len>	-2	-2	Split data in rec. len blocks	appends OS specific delims (1310 or 10)
F	<rec. len>	<d1>	-1	removed d1 from stream	appends <d1> to output data stream
F	<rec. len>	<d1>	<d2>	removed d1/d2 from stream	appends <d1> and <d2> to out. data stream
F	<rec. len>	-1	-1	Split data in rec. len blocks	Do NOT append any delims to out. Stream (newdefault)

Field Name	Description
RecordsLength	Data record length used for fixed record length File Format "F".
FileTransmissionRetries	Number of retries for file transmissions.
EERPTimeout	If the EERP Timeout limit in minutes is exceeded a Visibility event is created. Default 240. value 0 = no limit value -1 = disable Optional. **Note:** Replaces field WaitForEERP in Sterling Integrator 4.3 and older.
FileScheduleTimeout	Time limit in minutes how long a message is allowed to stay in Status "SCHEDULED". Default 240. value 0 = no limit value -1 = disable Optional.

Field Name	Description
FileCompression	Boolean. File Compression File Service is available in OFTP Version 2.0 and higher. Optional.
	See OFTP 2.0 specification for details about File Services.
FileEncryption	Boolean. File Encryption File Service is available in OFTP Version 2.0 and higher. Optional.
	Enable File Encryption to enforce Integrity of file content.
	See OFTP 2.0 specification for details about File Services.
FileSigning	Boolean. File Signing File Service is available in OFTP Version 2.0 and higher. Optional.
	Signing of files allows non-repudiation of origin.
	See OFTP 2.0 specification for details about File Services.
SendEERP	When to send an EERP. Required. Valid values are:
	A - Always (default)
	N - Never
	P - Pass through (EERP/NERP forwarding)
SignedEERPRequest	Boolean. EERP Signing is available in OFTP Version 2.0 and higher. Optional.
	Signing of receipts allows Non-repudiation of receipts. The Originator of the virtual file may request a signed EERP in the SFID. The signature of the EERP is in CMS format.
	See OFTP 2.0 specification for details about File Services.
EERP/NERPSignatureCheck	Boolean. EERP Signature check is available in OFTP Version 2.0 and higher. Optional.
	While signing of receipts allows Non-repudiation of receipts parameter "EERP/NERP Signature Check" specifies whether the partner who receives an EERP/NERP wants to check the signature contained in the EERP/NERP.
	See OFTP 2.0 specification for details about how the EERP/NERP Signature is checked against local certificates.
CipherSuite	OFTP Version 2.0 specifies the mandatory list of Cipher Suites and the required key lengths. Valid values (numeric) are:
	◆ 0 - Use no Security Service
	◆ 1 - 3DES_EDE_CBS_3KEY_RSA_PKCS1_15 SHA-1 (3 different 64 bit keys)
	◆ 2 - AES_256_CBS_RSA_PKCS1_15 SHA-1 (sym., 256bit key)
	Where CBS = Cyclic Block Chaining Mode, EDE = Encryption Decryption Encryption
	Both cipher suites use asymmetric RSA_PKCS1_15 with RSA Padding defined in PKCS#1 and SHA-1 for Hashing.

Using Certificates in Partner Profile XML Setup

The Sterling Integrator user interface allows you to select Certificates and Private Keys from lists in the application; however, if you are using manual Partner Profile XML setup, you must reference them using this setup information.

There are 3 places where one or more certificates can be used:

Location	Certificate Name
PhysicalPartner	AuthenticationCertificate
PhysicalPartner/TCP-IP	SSLCertificate
LogicalPartner	FileServiceCertificate

Each certificate can be a:

✦ CA Certificate (can occur more than once in one location)

✦ Trusted Certificate (can occur more than once in one location)

✦ System Certificate (in OdetteFTP terminology also called PrivateKey, can occur only once in one location)

Specification of a System Certificate

```
<Certificate name> type="PrivateKey"
   Subject <Distinguished Name String>    (required)
   Issuer  <Distinguished Name String>    (required)
   Serial<BigNumber String>   (optional)
```

Note: The components within one distinguished name have to be separated by a comma, optionally following a blank.

For additional information see Digital Certificates.

Code Sample (for additional information, see *Manual Partner Profile Sample* on page 31).

```
<AuthenticationCertificate type="PrivateKey">
   <Subject>CN=SOAServicesTestCertificate, O=SOAServicesTestIdentity1,
C=US</Subject>
   <Issuer> CN=SOAServicesTestCertificate, O=SOAServicesTestIdentity2, C=US</Issuer>
   <Serial>01234567890987654321</Serial>
</AuthenticationCertificate>
```

Specification of a CA- or Trusted Certificate:

```
{  <Certificate name> type="CA or Trusted"
   Subject <Distinguished Name String>    (required)
   Issuer  <Distinguished Name String>    (required)
   Serial<BigNumber String>   (optional)}+  (the whole structure can repeat)
```

Note: The components within one distinguished name have to be separated by a comma, optionally following a blank.

Code Sample (for additional information, see *Manual Partner Profile Sample* on page 31).

```
<SSLCertificate type="Trusted">
    <Subject>CN=OFTP_TLS_A1, OU=RL, O=STERLING, L=DUESSELDORF, ST=NRW, C=DE</Subject>
    <Issuer>C=GE, O=Sterling, OU=RL, CN=RLCA</Issuer>
</SSLCertificate>
```

Manual Partner Profile Sample

This is a sample template of the Partner Profile with its complete content:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--
 This file as template contains all physical and logical partner profile
     information used by the Odette FTP adapter

  -->
- <PartnerProfiles>
- <GeneralParameters>
  <PartnerProfileVersion>3.00</PartnerProfileVersion>
  </GeneralParameters>
- <!--
 PhysicalPartnerSpec and LogicalPartnerSpec can occur more oftenly with
       the restriction that references between different subgroups (e.g.
       PhysicalContract to PhysicalPartner) can only be made backwards but not
       forwards (e.g. a certain PhysicalPartner has already to be
       defined when it will be referenced by PhysicalPartnerContract

  -->
- <!--
 WARNING: this file acts as a template only and has to be fit by the user!
                The user has to review and fill in or substitute with his/her
                actual values needed by the required fields


  -->
- <PhysicalPartnerSpec>
- <!--
 This group should define physical partners and contracts where
        the physical contracts may only follow their corresponding partners.

  -->
- <!--  1. some example Physical Partner entries
  -->
- <PhysicalPartner name="PP_LocalCapi1" type="ISDN">
  <Description>Sample local PhysicalPartner using ISDN</Description>
  <OFTPUserId>LocalCapi1</OFTPUserId>
  <OFTPUserPassword />
  <SSIDUserField>add.Info</SSIDUserField>
  <SessionRetryIntervals>60,300,900</SessionRetryIntervals>
  <MailboxUser>mboxPP_LocalCapi1</MailboxUser>
  <SubMailbox>subMboxPP_Remote1</SubMailbox>
- <!--
```

```
 Extractability: there are three different modes to choose:
   <Extractability type="Extractable">yes or no</Extractability>
   <Extractability type="ExtractableCount">number</Extractability>
   <Extractability type="ExtractableUntil">YYMMTTHHmmss</Extractability>

  -->
  <Extractability type="Extractable">yes</Extractability>
- <!--  Certificates and Private Keys, before import their validity is checked
  -->
- <AuthenticationCertificate type="CA Certificate">
  <Subject>CN=NAGA, OU=DEV, O=CSG, ST=TX, C=US</Subject>
  <Issuer>CN=NAGA, OU=DEV, O=CSG, ST=TX, C=US</Issuer>
  </AuthenticationCertificate>
- <AuthenticationCertificate type="PrivateKey">
  <Subject>CN=SOAServicesTestCertificate, O=SOAServicesTestIdentity, C=US</Subject>
  <Issuer>CN=SOAServicesTestCertificate, O=SOAServicesTestIdentity, C=US</Issuer>
  <Serial>01234567890987654321</Serial>
  </AuthenticationCertificate>
- <Capi_Parameters>
- <!--  mandatory subgroup for a PhysicalPartner with type "ISDN"
  -->
  <Address>ISDNnumber</Address>
  <SubAddress />
  <AlternativeAddresses>altISDNnumber1,..,altISDNnumbern</AlternativeAddresses>
  <LocalNUA />
- <!--  local X.121 address
  -->
  <RemoteNUA />
- <!--  remote X.121 address
  -->
  <B3_ChannelConf>0, 0, 1, 1, 0, 0</B3_ChannelConf>
- <!--
 this array contains exactly 6 items; the order of the items is:
        LIC, HIC, LTC, HTC, LOC and HOC; further details see documentation

  -->
  <Modulo>8</Modulo>
  <BWindowSize>7</BWindowSize>
  <CallUserData>0102abcdef</CallUserData>
  <Facilities>FFEE</Facilities>
  </Capi_Parameters>
  </PhysicalPartner>
- <PhysicalPartner name="PP_RemoteCapi1" type="ISDN">
  <Description>Sample remote PhysicalPartner using CAPI</Description>
  <OFTPUserId>RemoteCapi1</OFTPUserId>
  <OFTPUserPassword />
- <!--
 other fields left out,
        they have to be completed according PP_LocalCapi1

  -->
- <Capi_Parameters>
- <!--  mandatory subgroup for a PhysicalPartner with type "ISDN"
  -->
  <Address>ISDNnumber</Address>
- <!--
```

```
 other fields left out,
         they have to be completed according PP_LocalCapi1


  -->
  </Capi_Parameters>
  </PhysicalPartner>
- <PhysicalPartner name="PP_LocalIP1" type="IP">
  <Description>Sample local PhysicalPartner using IP</Description>
  <OFTPUserId>LocalIP1</OFTPUserId>
  <OFTPUserPassword />
  <SSIDUserField>add.Info</SSIDUserField>
  <SessionRetryIntervals>60,300,900</SessionRetryIntervals>
  <MailboxUser>mboxPP_LocalIP1</MailboxUser>
  <SubMailbox>subMboxPP_Remote1</SubMailbox>
- <!--
 Extractability: there are three different modes to choose:
    <Extractability type="Extractable">yes or no</Extractability>
    <Extractability type="ExtractableCount">number</Extractability>
    <Extractability type="ExtractableUntil">YYMMTTHHmmss</Extractability>


  -->
  <Extractability type="ExtractableCount">3</Extractability>
- <!--  Certificates and Private Keys, before import their validity is checked
  -->
- <AuthenticationCertificate type="Trusted Certificate">
  <Subject>CN=NAGA1, OU=DEV, O=CSG, ST=TX, C=US</Subject>
  <Issuer>CN=NAGA1, OU=DEV, O=CSG, ST=TX, C=US</Issuer>
  </AuthenticationCertificate>
- <AuthenticationCertificate type="Trusted Certificate">
  <Subject>CN=NAGA2, OU=DEV, O=CSG, ST=TX, C=US</Subject>
  <Issuer>CN=NAGA2, OU=DEV, O=CSG, ST=TX, C=US</Issuer>
  </AuthenticationCertificate>
- <TCP-IP_Parameters>
- <!--  mandatory subgroup for a PhysicalPartner with type "IP"
  -->
  <Hostname>hostname or IP address</Hostname>
  <IPPort>13617</IPPort>
  <IPFilter>16.127.128.129 99.86.13.255/26 FEDC:BA74::12:1:1234/120 fe80::1::2
0:0:1980::1:192.168.13.212/64 2002:FE10:2849:DD0A::0/63
2002:FE10:2849:DD0A:B321:AC34:0E21:3/63</IPFilter>
- <!--  session level encryption: SSL stuff including certificates
  -->
  <SSL>SSL_MUST</SSL>
  <CipherStrength>Weak</CipherStrength>
- <SSLCertificate type="PrivateKey">
- <!--  SystemCertificate OpsKey
  -->
  <Subject>CN=Ops, O=Sterling, C=US</Subject>
  <Issuer>CN=Ops, O=Sterling, C=US</Issuer>
  </SSLCertificate>
- <SSLCertificate type="Trusted">
- <!--  TRUSTED_CERT_INFO rmikey
  -->
  <Subject>CN=ken meeks,OU=sterling,O=sterling,L=dublin,ST=ohio,C=us</Subject>
  <Issuer>CN=ken meeks,OU=sterling,O=sterling,L=dublin,ST=ohio,C=us</Issuer>
  </SSLCertificate>
```

```
   </TCP-IP_Parameters>
   </PhysicalPartner>
- <PhysicalPartner name="PP_RemoteIP1" type="IP">
   <Description>Sample remote PhysicalPartner using IP</Description>
   <OFTPUserId>RemoteIP1</OFTPUserId>
   <OFTPUserPassword />
- <!--
 other fields left out,
         they have to be completed according PP_LocalIP1

   -->
- <TCP-IP_Parameters>
- <!--  mandatory subgroup for a PhysicalPartner with type "IP"
   -->
   <Hostname>hostname or IP address</Hostname>
   <IPPort>3305</IPPort>
   <IPFilter>10.123.456.789</IPFilter>
   <SSL>SSL_NONE</SSL>
   </TCP-IP_Parameters>
   </PhysicalPartner>
- <!--  1. some example Physical Partner Contract entries
   -->
- <PhysicalPartnerContract name="PPC_IP1">
   <Description>Sample PhysicalPartnerContract using IP</Description>
   <LocalPhysicalPartner>PP_LocalIP1</LocalPhysicalPartner>
   <RemotePhysicalPartner>PP_RemoteIP1</RemotePhysicalPartner>
   <OdetteFTPAPILevel>1</OdetteFTPAPILevel>
- <!--  valid values: 1 (1.2), 2 (1.3), 4 (1.4)
   -->
   <AcceptSFIDsForNonLPC>Yes</AcceptSFIDsForNonLPC>
   <CreditWindowSize>7</CreditWindowSize>
   <DuplicateFileChecking>No</DuplicateFileChecking>
   <DuplicateFilePeriod>3</DuplicateFilePeriod>
   <ExchangeBufferSize>1024</ExchangeBufferSize>
   <GroupNameList>IP1,IP2</GroupNameList>
   <SessionLogLevel>DEBUG</SessionLogLevel>
   <SendReceiveCapabilities>B</SendReceiveCapabilities>
   <CompressionCapabilities>No</CompressionCapabilities>
   <MultipleLoginSessions>1</MultipleLoginSessions>
   <SecureAuthentication>Yes</SecureAuthentication>
   <InitiatorBusinessProcess>BusinessProcessName</InitiatorBusinessProcess>
   <BusinessProcessUser>admin</BusinessProcessUser>
   </PhysicalPartnerContract>
   </PhysicalPartnerSpec>
- <LogicalPartnerSpec>
- <!--
 This group should define logical partners and contracts where
         the logical contracts may only follow their corresponding partners.

   -->
- <!--  some Logical Partner entries
   -->
- <LogicalPartner name="LP_Local1">
   <Description>Sample local LogicalPartner</Description>
   <OdetteName>ODETTENAME_LP_Local1</OdetteName>
   <ContactPerson>Name of LP_Local1</ContactPerson>
```

```
-  <!--   Certificates and Private Keys, before import their validity is checked
   -->
-  <FileServiceCertificate type="CA Certificate">
   <Subject>CN=NAGA1, OU=DEV, O=CSG, ST=TX, C=US</Subject>
   <Issuer>CN=NAGA1, OU=DEV, O=CSG, ST=TX, C=US</Issuer>
   </FileServiceCertificate>
-  <FileServiceCertificate type="PrivateKey">
-  <!--   SystemCertificate OpsKey
   -->
   <Subject>CN=Ops, O=Sterling, C=US</Subject>
   <Issuer>CN=Ops, O=Sterling, C=US</Issuer>
   </FileServiceCertificate>
-  <FileServiceCertificate type="CA Certificate">
-  <!--   again a CA CERT
   -->
   <Subject>CN=NAGA2, OU=DEV, O=CSG, ST=TX, C=US</Subject>
   <Issuer>CN=NAGA2, OU=DEV, O=CSG, ST=TX, C=US</Issuer>
   </FileServiceCertificate>
   </LogicalPartner>
-  <LogicalPartner name="LP_Remote1">
   <Description>Sample remote LogicalPartner</Description>
   <OdetteName>ODETTENAME_LP_Remote1</OdetteName>
   <ContactPerson>Name of LP_Remote1</ContactPerson>
   </LogicalPartner>
-  <!--   some Logical Partner Contract entries
   -->
-  <LogicalPartnerContract name="LPC1">
   <Description>Sample LogicalPartnerContract</Description>
   <OriginatorLogicalPartner>LP_Local1</OriginatorLogicalPartner>
   <DestinationLogicalPartner>LP_Remote1</DestinationLogicalPartner>
   <InboundPhysicalPartnerContract />
   <OutboundPhysicalPartnerContract>PPC_IP1</OutboundPhysicalPartnerContract>
   <InboundBusinessProcess>inboundBP</InboundBusinessProcess>
   <InboundBusinessProcessUser>admin</InboundBusinessProcessUser>
   <DefaultOFTPVirtualFilename>BilateralOFTPFilename</DefaultOFTPVirtualFilename>
   <ReceiveVirtualFilenamePattern>RegularPattern*</ReceiveVirtualFilenamePattern>
   <SendEERP>A</SendEERP>
   <OFTPFileUserField>yourchoice</OFTPFileUserField>
   <CharEncoding>UTF-8</CharEncoding>
   <FileFormat>V</FileFormat>
-  <!--   valid values: (U)nformatted, (T)ext, (F)ixed, (V)ariable
   -->
-  <!--   RecordLength: only to use if  FileFormat = F or V
   -->
   <RecordLength>120</RecordLength>
   <RecordDelimiter>13,10</RecordDelimiter>
   <EERPTimeout>240</EERPTimeout>
   <FileScheduleTimeout>-1</FileScheduleTimeout>
   <FileCompression>0</FileCompression>
-  <!--   valid values: 0 or 1
   -->
   <FileEncryption>Yes</FileEncryption>
   <FileSigning>Yes</FileSigning>
   <SignedEERPRequest>Yes</SignedEERPRequest>
   <CipherSuite>1</CipherSuite>
-  <!--   valid values: 0, 1, 2
```

```
  -->
  <EERPSignatureCheck>Strict</EERPSignatureCheck>
- <!--  valid values: None or Strict
  -->
  <NERPSignatureCheck>None</NERPSignatureCheck>
- <!--  valid values: None or Strict
  -->
  </LogicalPartnerContract>
  </LogicalPartnerSpec>
  </PartnerProfiles>
```

```
  -->
  <EERPSignatureCheck>Strict</EERPSignatureCheck>
```

OFTP Password Encryption for PartnerProfile.xml

Note: Normally it is no longer required to perform this extra step because during import using the PartnerManager, the OFTP Password Encryption is already performed; however, it might be desired to perform the OFTP Password Encryption before the import is invoked. The import only asks for the OFTP User Passwords that are not set.

In the PartnerProfile.xml file, every physical partner includes two mandatory fields:

✦ OFTPUserID

✦ OFTPUserPassword

For security reasons, the OdetteFTP adapter only accepts the OFTPUserPassword in encrypted format.

To encrypt OFTPUserPasswords, Application includes a script in the ***install_dir*/bin** directory named:

```
encryptOFTPPasswords.sh filename (for Unix)
encryptOFTPPasswords.cmd filename (for Windows)
```

Where *filename* denotes a valid path to the PartnerProfile.xml file.

The script encrypts every unencrypted OFTPUserPassword field of a particular OFTPUserID. If a specified PartnerProfile.xml file is invoked by the script prior to using the partnerProfile.xml file, each OFTPUserPassword field is empty. All successive calls to the same PartnerProfile.xml file are only valid if new physical partners and empty OFTPUserPassword fields are added to this file. In this case, you are prompted to enter the passwords of the newly added physical partner structures.

Note: An OFTPUserPassword field is only encrypted if the content is empty; otherwise the content is not changed and is treated as encrypted.

For example, part of the partnerProfile.xml file looks like the following:

```
<PhysicalPartnerSpec>
    <PhysicalPartner name="PP_Local1" type="ISDN">
    <OFTPUserId>LocalUserId</OFTPUserId>
    <OFTPUserPassword></OFTPUserPassword>yeah?

    <SendEERP>A</SendEERP>
            ...
    </PhysicalPartner>
    ...
</PhysicalPartnerSpec>
...
```

When calling encryptOFTPPasswords.sh <path>/PartnerProfile.xml, the following message is displayed:

```
In PhysicalPartner PP_Local1 please enter for OFTPUserID LocalUserId the
OFTPUserPassword:
```

Enter and confirm a password for the OFTPUserPassword to store in encrypted format. The program will continue and prompt for all other unencrypted passwords.

From the example above, the corresponding line looks like the following:

```
<OFTPUserPassword>rO0ABXQABkRFU2Vk… jGFOyD0CMG7w==</OFTPUserPassword>
```

Note: The password cannot exceed eight characters. Do not change any of the encrypted characters or the password cannot be decrypted properly later.

Copy the PartnerProfile.xml file to the OdetteFTP adapter Partner Profile directory configured in OdetteFTP.properties (the default is *install_dir*/install/properties).

Making Password Changes

Passwords stay the same after mass import/export/delete/update with OFTPPArtner Manager.

It is not required, if you change the password in the Partner UI.

In the PartnerProfile XML file from one or more Physical Partners, you can change your OFTP User Password:

1. Copy the PartnerProfile file and open it in an text editor.

2. Empty the Physical Partners whose passwords you want to change in the OFTP Password fields.

3. Save the file.

4. Run the password encryption script. For additional information, see *OFTP Password Encryption for PartnerProfile.xml*.

Note: To add new partners to your OFTP partner profile, test the modified partner profile in a non-production environment successfully before moving it into a production system.

If you do not have a non-production system, check the OdetteFTP log files for errors during partner profile.

Note: Check Odette FTP log file after running a simple send/receive test.