Configuring Java CAPS Environment Components for Application Adapters

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820–4386–10
June 2008

080916@20795

Contents

Configuring Java CAPS Environment Components for Application Adapters

The adapter environment configuration properties contain parameters that define how the adapter connects to and interacts with other Java CAPS components within the environment. The environment properties are accessed from the NetBeans IDE Services window. The following sections provide instructions on how to configure Java CAPS component environment properties and lists the environment properties for the various application adapters.

What You Need to Know

This topic provides information you should know to start configuring the environment properties. "Using the Environment Properties Editor" on page 5.

What You Need to Do

These topics provide configuration information used to set the application adapter environment properties.

- "Configuring Oracle Applications Adapter Environment Properties" on page 7.
- "Configuring the PeopleSoft HTTP Client Adapter Environment Properties" on page 11.
- "Configuring SAP BAPI Adapter Environment Properties" on page 19.
- "Configuring the Siebel EAI Adapter Environment Properties" on page 26.
- "Configuring the SWIFT Alliance Gateway Adapter Environment Properties" on page 32.
- "Configuring Websphere MQ Adapter Environment Properties" on page 35.

Using the Environment Properties Editor

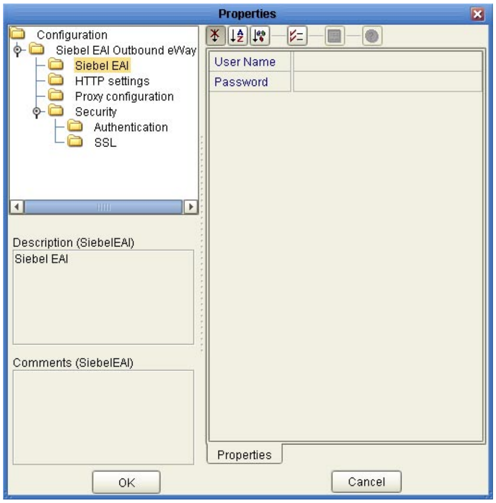
The Adapter Environment Configuration properties contain parameters that define how the adapter connects to and interacts with other Java CAPS components within the Environment. The Environment properties are accessed from the NetBeans IDE Services window.

▼ To Configure the Environment Properties

1. **From the NetBeans Services window, expand the CAPS Environment node.**

2. **Expand the Environment created for your project and locate the External System for your specific adapter.**

3. **Right-click the External System and select Properties from the popup menu. The Environment Configuration Properties window appears.**



Description (SiebelEAI)
Siebel EAI

Comments (SiebelEAI)

FIGURE 1 Adapter Environment Configuration Properties Editor

4. **From the Properties Editor, click on any folder to display the default configuration properties for that section.**

5. **Click on any property field to make it editable.**

6. **Once you have finished modifying the properties, click OK to save your changes and close the editor.**

Configuring Oracle Applications Adapter Environment Properties

The Oracle Applications Adapter configuration parameters, accessed from the Environment Explorer tree, are organized into the following sections:

- "Outbound Oracle Applications Adapter Properties" on page 7.
- "Outbound Oracle Adapter Properties with XA support" on page 9.

Outbound Oracle Applications Adapter Properties

The Outbound Oracle Applications Adapter properties, accessed from the Environment Explorer tree, are organized into the following sections:

- "JDBC Connector Settings" on page 7.
- "Connection Retry Settings" on page 8.

JDBC Connector Settings

The **JDBC Connector Settings** section of the Outbound Oracle Applications Environment contains the top-level parameters displayed in the following table.

TABLE 1 Outbound Adapter Environment JDBC Connector Settings

Name	Description	Required Value
Description	Enter a description for the database.	A valid string.
ServerName	Specifies the host name of the external database server.	Any valid string.
DatabaseName	Specifies the name of the database instance used on the Server.	Any valid string.
PortNumber	Specifies the I/O port number on which the server is listening for connection requests.	A valid port number. The default is 1521.
User	Specifies the user name that the Adapter uses to connect to the database.	Any valid string.
Password	Specifies the password used to access the database.	Any valid string.

TABLE 1 Outbound Adapter Environment JDBC Connector Settings *(Continued)*

Name	Description	Required Value
DriverProperties	Use the JDBC driver that is shipped with this Adapter. Often times the DataSource implementation needs to execute additional methods to assure a connection. You must identify the additional methods in the Driver Properties.	Any valid delimiter. Valid delimiters are: "<method-name-1> #<param-1>#<param-2>##......... <param-n>##<method-name-2># <param-1>#<param-2>#........ <param-n>##......##" For example: to execute the method setURL, give the method a String for the URL "setURL#<url>##".
Delimiter	This is the delimiter character to be used in the DriverProperties prompt.	The default is **#**.
TNSEntry	Specifies the TNS name for the Oracle instance specified in TNSNAMES.ORA. If a TNS name is specified, then the OCI driver is used, which further requires installation of the Oracle client. If a TNS name is not specified, then the thin driver is used.	A valid TNS name if using the OCI driver; otherwise do not enter any value.
MinPoolSize	The minimum number of physical connections the pool keeps available at all times. 0 (zero) indicates that there are no physical connections in the pool and new connections are created as needed.	A valid numeric value. The default is **2**.
MaxPoolSize	The maximum number of physical connections the pool keeps available at all times. 0 (zero) indicates that there is no maximum.	A valid numeric value. The default is **10**.
MaxIdleTime	The maximum number of seconds that a physical connection may remain unused before it is closed. 0 (zero) indicates that there is no limit.	A valid numeric value.

Connection Retry Settings

The **Connection Retry Settings** section of the Outbound Oracle Applications Environment contains the top-level parameters displayed in the following table.

TABLE 2 Outbound Adapter Environment Connection Retry Settings

Name	Description	Required Value
ConnectionRetries	Specifies the number of retries to establish a connection with the Oracle database upon a failure to acquire one.	An integer indicating the number of attempts allowed to establish a connection. The configured default is **0**.
ConnectionRetry Interval	Specifies the configured length of the pause before each reattempt to access the destination file. This property is used in conjunction with the property **ConnectionRetries**.	An integer indicating the configured length of the time (in milliseconds) before each reattempt to access the destination file. The configured default is **1000** (1 second).

Outbound Oracle Adapter Properties with XA support

The Outbound Oracle Applications Adapter properties with XA support, accessed from the Environment Explorer tree, are organized into the following sections:

- "JDBC Connector Settings (with XA support)" on page 9.
- "Connection Retry Settings (with XA support)" on page 10.

JDBC Connector Settings (with XA support)

The **JDBC Connector Settings** section of the Outbound XA Oracle Applications Environment contains the top-level parameters displayed in the following table.

TABLE 3 Outbound XA Adapter Environment JDBC Connector Settings

Name	Description	Required Value
Description	Enter a description for the database.	A valid string.
ServerName	Specifies the host name of the external database server.	Any valid string.
PortNumber	Specifies the I/O port number on which the server is listening for connection requests.	A valid port number. The default is **1521**.
Database Name	Specifies the name of the database instance used on the Server.	Any valid string.
User	Specifies the user name that the Adapter uses to connect to the database.	Any valid string.

TABLE 3 Outbound XA Adapter Environment JDBC Connector Settings *(Continued)*

Name	Description	Required Value
Password	Specifies the password used to access the database.	Any valid string.
DriverProperties	Use the JDBC driver that is shipped with this Adapter. Often times the DataSource implementation needs to execute additional methods to assure a connection. You must identify the additional methods in the Driver Properties.	Any valid delimiter. Valid delimiters are: "<method-name-1>#<param-1>#<param-2>##.........<param-n>##<method-name-2>#<param-1>#<param-2>#........<param-n>##......##" For example: to execute the method setURL, give the method a String for the URL "setURL#<url>##".
Delimiter	This is the delimiter character to be used in the DriverProperties prompt.	The default is **#**.
TNSEntry	Specifies the TNS name for the Oracle instance specified in TNSNAMES.ORA. If a TNS name is specified, then the OCI driver is used, which further requires installation of the Oracle client. If a TNS name is not specified, then the thin driver is used.	A valid TNS name if using the OCI driver; otherwise do not enter any value.
MinPoolSize	The minimum number of physical connections the pool keeps available at all times. 0 (zero) indicates that there are no physical connections in the pool and new connections are created as needed.	A valid numeric value. The default is **2**.
MaxPoolSize	The maximum number of physical connections the pool keeps available at all times. 0 (zero) indicates that there is no maximum.	A valid numeric value. The default is **10**.
MaxIdleTime	The maximum number of seconds that a physical connection may remain unused before it is closed. 0 (zero) indicates that there is no limit.	A valid numeric value.

Connection Retry Settings (with XA support)

The **Connection Retry Settings** section of the Outbound XA Oracle Applications Environment contains the top-level parameters displayed in the following table.

TABLE 4 Outbound XA Adapter Environment Connection Retry Settings

Name	Description	Required Value
Connection Retries	Specifies the number of retries to establish a connection with the Oracle database upon a failure to acquire one.	An integer indicating the number of attempts allowed to establish a connection. The configured default is **0**.
Connection Retry Interval	Specifies the configured length of the pause before each reattempt to access the destination file. This property is used in conjunction with the property **ConnectionRetries**.	An integer indicating the configured length of the time (in milliseconds) before each reattempt to access the destination file. The configured default is **1000** (1 second).

Configuring the PeopleSoft HTTP Client Adapter Environment Properties

This task describes how to set the environment map properties of the PeopleSoft Adapter.

The PeopleSoft HTTP Client Adapter properties, accessed from the Environment Explorer tree, are organized into the following sections:

- “HTTP Settings” on page 11.
- “Proxy Configuration” on page 13.
- “Security and Authentication” on page 13.
- “Security and SSL” on page 13.
- “PeopleSoft Settings” on page 15.
- “PeopleSoft Settings and PeopleTools 8.42 Settings” on page 15.
- “PeopleSoft Settings and PeopleTools 8.13 Settings” on page 17.

HTTP Settings

The HTTP Settings section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 5 Environment Configuration - HTTP Settings

Name	Description	Required Value

URL	Specifies the default URL used to establishing an HTTP connection.
	The Sun Enterprise Service Bus uses the PeopleSoft Adapter to send an HTTP post request to PeopleSoft's HTTP listening connector. The PeopleSoft HTTP listening connector monitors specific ports for incoming HTTP messages. It is implemented as a Java HTTPServlet object running inside WebLogic's application server.
	For PeopleTools 8.13, use the following:
	- Apache:
	`http:// PSFTHOST /servlets/psft.pt8.gateway. Gatewayservlet`
	- WebLogic:
	`http:// PSFTHOST /servlets/gateway`
	- PeopleTools 8.42:
	`http:// PSFTHOST :90/PSIGW/HttpListeningConnector` `where, **PSFTHOST** is the PeopleSoft server host name. You can verify the 8.42 HTTP listening connector servlet by verifying the web.xml.`
	Note – `The URL parameter does not support LDAP values.`
		The default URL used for establishing an HTTP connection.

Content type	Specifies the default Content-Type header value to include when sending a request to the server.	The default Content-Type header value. The configured default is: `text/xml;charset=iso_8859-1`
Encoding	Specifies the default encoding used when reading or writing textual data.	The default encoding used when reading or writing textual data. The configured default is **ASCII**.

Proxy Configuration

The **Proxy configuration** section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 6 Environment Configuration - Proxy configuration

Name	Description	Required Value
Proxy host	Specifies the hostname of the HTTP proxy server.	The hostname (string) of the HTTP proxy server.
Proxy port	Specifies the port of the HTTP proxy host.	The port number of the HTTP proxy server. The configured default is **8080**.
Proxy username	Specifies the username for accessing the HTTP proxy server.	A user name (login) for the HTTP proxy server.
Proxy password	Specifies the password required for accessing the HTTP proxy host.	A password for the HTTP proxy server.

Security and Authentication

The **Security and Authentication** section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 7 Environment Configuration - Security and Authentication

Name	Description	Required Value
Http username	Specifies the username used to authenticate the Web site specified by the URL.	A user name with access permission.
Http password	Specifies the password used to authenticate the Web site specified by the URL.	A password linked to the user name.

Security and SSL

The **Security and SSL** section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

Note – SSL is not currently supported for the PeopleSoft Adapter. This section is reserved for future product enhancement.

TABLE 8 Environment Configuration - Security and SSL

Name	Description	Required Value
Protocol SSL	Specifies the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol used when establishing an SSL connection with the server.	Select the appropriate protocol. The options are: ■ No SSL ■ TLS ■ TLSv1 ■ SSLv3 ■ SSLv2 ■ SSL The configured default is **No SSL**.
JSSE Provider Class	Specifies the fully qualified name of the JSSE provider class.	The name of the JSSE provider class. The configured default value is **com.sun.net.ssl.internal.ssl.Provider.**
X509 Algorithm Name	Specifies the X509 algorithm name to use for the trust and key manager factories.	The X509 algorithm name to use for the trust and key manager factories. The configured default is **SunX509**.
Verify hostname	Specifies whether hostname verification is done on the server certificate during the SSL handshake.	**True** or **False**. **True** indicates that hostname verification is performed on the server certificate during the SSL handshake. The configured default is **False**.
KeyStore type	Specifies the keystore type for the keystore used for key/certificate management when establishing SSL connections.	The keystore type. The configured default is **JKS**.
KeyStore	Specifies the keystore used for key/certificate management when establishing SSL connections.	The keystore used for key/certificate management.
Keystore username	Specifies a username for accessing the keystore used for key/certificate management when establishing SSL connections.	A user name (login) with permission to access the keystore.
Keystore password	Specifies the password for accessing the keystore used for key/certificate management when establishing SSL connections.	A password associated with the KeyStore username to access the keystore.

TABLE 8 Environment Configuration - Security and SSL *(Continued)*

Name	Description	Required Value
TrustStore type	Specifies the truststore type of the truststore used for CA certificate management when establishing SSL connections.	The truststore type. The configured default is **JKS**.
TrustStore	Specifies the truststore used for CA certificate management when establishing SSL connections.	The name of the truststore.
TrustStore password	Specifies the password for accessing the truststore used for CA certificate management when establishing SSL connections.	A password that permits access to the truststore.

PeopleSoft Settings

The **PeopleSoft Settings** section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 9 Environment Configuration - PeopleSoft Settings

Name	Description	Required Value
PeopleTools Version	Specifies the version of PeopleTools installed. The value options are: ■ **8.42**: PeopleTools version 8.42 ■ **8.13**: PeopleTools version 8.13	Select **8.13** or **8.42**. The configured default is **8.42**.

PeopleSoft Settings and PeopleTools 8.42 Settings

The **PeopleSoft Settings and PeopleTools 8.42 Settings** section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

The PeopleTools settings must match the configurations for the PeopleSoft server.

At minimum, you must specify the following properties:

- MessageName
- DestinationNode
- RequestingNode
- MessageVersion

TABLE 10 Environment Configuration - PeopleSoft Settings and PeopleTools 8.42 Settings

Name	Description	Required Value
Message Name	Specifies the name of the message.	The name of the message.
Message Type	Specifies the type of message being sent. The type options are: ■ **sync**: Synchronous message ■ **async**: Asynchronous message ■ **ping**: Ping message	Select **sync**, **async**, or **ping**.
Requesting Node	Specifies the name of the node sending the request.	The name of the node sending the request.
Destination Node	Specifies the name of the node that receives the message. This parameter is optional when you specified a default target node using the **Default Application Server Jolt** connect string properties in the **integrationGateway.properties** file.	The name of the node that receives the message.
FinalDestination	Specifies the name of the node that ultimately receives the message. This is common when a PeopleSoft Integration Broker hub is used.	The name of the node that ultimately receives the message.
Message Version	Specifies the message version.	The message version.
Non Repudiation	Specifies whether the message content in the request should be processed using nonrepudiation logic.	**True** or **False**. **True** indicates that nonrepudiation logic will be used to process the message content of the request.
OrigNode	Specifies the name of the node that started the process. This property is optional.	The name of the node that started the process.
OrigProcess	Specifies the originating process by which the message was initially generated.	The originating process by which the message was initially generated.
OrigUser	Specifies the user ID for the user from which the message was initially generated. This property is optional.	The user ID for the user from which the message was initially generated.

TABLE 10 Environment Configuration - PeopleSoft Settings and PeopleTools 8.42 Settings *(Continued)*

Name	Description	Required Value
Password	Specifies the password as entered in the target node's definition for the source node. The target node authenticates the password when it receives the message. This parameter is only required if password authentication is enabled for the source node definition in the target database.	The password, as it is presented in the target node's definition for the source node.

PeopleSoft Settings and PeopleTools 8.13 Settings

The **PeopleSoft Settings and PeopleTools 8.13 Settings** section of the PeopleSoft HTTP Client Adapter Environment properties contains the top-level parameters displayed in the following table.

The PeopleTools settings must match the configurations for the PeopleSoft server.

At minimum, you must specify the following properties:

- MessageVersion
- FromNode
- ToNode
- Channel
- PublicationProcess
- Subject

TABLE 11 Environment Configuration - PeopleSoft Settings and PeopleTools 8.13 Settings

Name	Description	Required Value
Message Version	Specifies the message version.	The message version.
ToNode	Specifies the name of the node for which the message is intended. This must correspond to an entry in the node lookup table on the gateway servlet, and the name of the local node (node definition) on the receiving PeopleSoft system.	The name of the node for which the message is intended.
FromNode	Specifies the name of the node from which messages originate. The node name must match the node definition for the third party system as defined in the receiving PeopleSoft system.	The name of the node from which the messages originate.
Channel	Specifies the name of the message channel containing the message.	The name of the message channel.

TABLE 11 Environment Configuration - PeopleSoft Settings and PeopleTools 8.13 Settings *(Continued)*

Name	Description	Required Value
Publication Process	Specifies the application-defined name of the program that generated the message. This may be required by the application.	The application-defined name of the program that generated the message.
Password	Specifies the password associated with the destination node. This value is stored in the PeopleSoft database and must be communicated to the system administrators for the publishing system. If the node definition on the sending system has a node group defined, the password will be present. If the node definition on the receiving system has a node group defined, the password must be present and must match the node group password.	The password associated with the destination node.
DefaultData Version	Specifies the default message version for the sending system.	The default message version.
Originating Node	Specifies the name of the node that originally published the message. This property is used to prevent circular publishing. If not in the XML file, the system sets it to the publishing node name.	The name of the node that originally published the message.
Publication ID	Specifies the system generated identifier for the publication. The fields, FromNode, Channel, and PublicationID, uniquely identify the publication. If the FromNode is specified and the Publication ID is omitted, the publication ID is set to the next available publication ID on that channel within the subscribing PeopleSoft database.	The system generated identifier for the publication.
Publisher	Specifies the application-defined operator ID class that published the message. This may be required by the application.	The application-defined operator ID class that published the message.
SubChannel	Specifies the name of the subchannel that contains the message. Messages in the same channel, but in different subchannels, are assumed to refer to distinct objects (for example, different POs or different employees), and are processed in parallel if possible. This field contains the concatenated values that represent the subchannel. For example, if the subchannel is Business Unit, Journal ID, then the value of this field is M04123456789 where Business Unit = M04 and Journal ID = 123456789. Include this field if the subscribing PeopleSoft system has a defined subchannel, otherwise, it may be omitted.	The name of the subchannel that contains the message. See the description for the naming format.
Subject	Specifies the name of the message as defined in the PeopleSoft system.	The name of the message as defined in the PeopleSoft system.

TABLE 11 Environment Configuration - PeopleSoft Settings and PeopleTools 8.13 Settings *(Continued)*

Name	Description	Required Value
Subject Detail	Specifies the application defined subtype of the message name.	The application defined subtype of the message name.

Configuring SAP BAPI Adapter Environment Properties

The SAP BAPI Environment System consists of the following properties categories.

- "Inbound SAP BAPI Adapter" on page 19.
- "Outbound SAP BAPI Adapter" on page 22.

Inbound SAP BAPI Adapter

The inbound Adapter Environment properties include server connection parameters that are required to implement the project, and are configured in the inbound Adapter Environment Properties window.

The Inbound SAP BAPI Adapter includes the following configuration section:

- "Server Connection Settings" on page 19.
- "Server Security Settings" on page 21.
- "MDB Settings" on page 22.

Server Connection Settings

The following are the Server Connection Settings.

TABLE 12 Inbound SAP BAPI Adapter—Server Connection Settings

Name	Description	Required Value
Gateway Hostname	Specifies the gateway hostname of the SAP application server.	An alphanumeric string. Do not omit leading zeros. There is no default setting.

TABLE 12 Inbound SAP BAPI Adapter—Server Connection Settings *(Continued)*

Name	Description	Required Value

Router String (optional)	Specifies the router string needed to access the SAP Application Server.
	This property is optional; use it only to gain access to an SAP system that is behind a firewall.
	The string is composed of the hostnames or IP addresses of all the SAP routers that are in between this application server and the SAP gateway host. For example, if there are two routers, **saprouter1**, and **saprouter2**, in order, from the application server to the SAP, as follows:
	`saprouter1:       204.79.199.5 saprouter2: 207.105.30.146`
	The router string in this case is as follows:
	`/H/204.79.199.5/H/207.105.30.146/H/`
	Do not omit the "/H/" tokens to begin, separate, and end the routers.
		A valid router string.
		There is no default setting.

Gateway Service	Specifies the gateway service of SAP The gateway service of the SAP system sends transactions.	The SAP recommended value is the string **sapgw** concatenated with the SAP system number. For example, if the system number is **00**, the gateway service is **sapgw00**. There is no default setting.
Program ID	Specifies the **Program ID** used to register the SAP JCo server of the Adapter with SAP.	Program ID is shown in the SAPGUI transaction SM59. This entry must match the SAPGUI exactly; this entry is case sensitive. There is no default setting.
Application Server Hostname	Specifies the host name of the SAP application server.	Any valid Hostname. There is no default setting.
System Number	Specifies the system number of the SAP application server. Use this property when you are not using SAP load balancing.	Any numeric value. The default setting is 00.
Client Number	Specifies the SAP client number used to access the system.	An alphanumeric string. Do not omit leading zeros. There is no default setting.

TABLE 12 Inbound SAP BAPI Adapter—Server Connection Settings *(Continued)*

Name	Description	Required Value
User	Specifies the user ID used to log on to the SAP system.	Any alphanumeric value. There is no default setting.
Password	Specifies the password for the logon user.	An alphanumeric string. There is no default setting.
Language	Specifies the logon language used for SAP access by the Adapter.	A base language is required. Languages include: ■ EN– English ■ DE– German ■ JA– Japanese ■ KO– Korean The default is **EN**, English.
System ID	Specifies the system ID of the SAP instance.	Any valid SAP System ID. There is no default setting.
Character Set	Sets the character encoding of the connecting SAP system.	Unicode or Non-unicode. The default value is **Non-unicode**.

Server Security Settings

The following Server Security Settings are used.

TABLE 13 Inbound SAP BAPI Adapter—Server Security Settings

Name	Description	Required Value
Enable SNC	Specifies whether the SNC is enabled or not.	**Yes** or **No**. The default is **No**.
SNC Level of Protection	Specifies the level of protection to use for the connection.	Possible values: ■ 1: Authentication only ■ 2: Integrity protection ■ 3: Privacy protection ■ 8: Use the value from snc/data_protection/use on the application server ■ 9: Use the value from snc/data_protection/max on the application server There is no default setting.

TABLE 13 Inbound SAP BAPI Adapter—Server Security Settings *(Continued)*

Name	Description	Required Value
SNC Library Path	Specifies the path and file name of the external library.	The default is the system-defined library as defined in the environment variable SNC_LIB.
SNC My Name	Specifies the SNC My Name.	There is no default setting.

MDB Settings

The following MDB Settings are used.

TABLE 14 Inbound SAP BAPI Adapter—MDB Settings

Name	Description	Required Value
Max Pool Size	Specifies the maximum number of physical connections the pool should keep available at all times. 0 (zero) indicates that there is no maximum.	Any numeric value. The default is **1000**.

Outbound SAP BAPI Adapter

The outbound Adapter Environment properties include client connection parameters that are required to implement the project using the Adapter in outbound mode communication. These parameters are configured in the outbound Adapter Environment Properties window.

The Outbound SAP BAPI Adapter includes the following configuration sections:

- "Client Connection Settings" on page 22.
- "Client Security Settings" on page 24.
- "Connection Retry Settings" on page 25.
- "Connection Pool Settings" on page 25.

Client Connection Settings

The following Client Connection Settings are used.

TABLE 15 Outbound SAP BAPI Adapter— Client Connection Settings

Name	Description	Required Value
Application Server Hostname	Specifies the host name of the SAP application server.	Any valid Hostname. There is no default setting.

TABLE 15 Outbound SAP BAPI Adapter— Client Connection Settings *(Continued)*

Name	Description	Required Value
System Number	Specifies the system number of the SAP application server. Use this property when you are not using SAP load balancing.	Any numeric value. The default setting is **00**.
Client Number	Specifies the SAP client number used to access the system.	An alphanumeric string. Do not omit leading zeros. There is no default setting.
User	Specifies the user ID used to log on to the SAP system.	Any alphanumeric value. There is no default setting.
Password	Specifies the password for the logon user.	An alphanumeric string. There is no default setting.
Language	Specifies the logon language used for SAP access by the Adapter.	There are no required values. ■ EN– English ■ DE– German ■ JA– Japanese ■ KO– Korean The default is **EN**, English.
System ID	Specifies the System ID of the SAP instance.	Any valid SAP System ID. There is no default setting.
Gateway Hostname (optional)	Specifies an Gateway host name for the Application Server. This parameter is optional and should be configured when NOT using SAP Load Balancing. **Note –** Do not specify any optional Router String here, as the value is prepended to the Gateway Hostname.	An alphanumeric string. Do not omit leading zeros. There is no default setting.
Gateway Service (optional)	Specifies an Gateway Service for the Application Server. This parameter is optional and should be configured when NOT using SAP Load Balancing.	The SAP recommended value is the string **sapgw** concatenated with the SAP system number. For example, if the system number is **00**, the gateway service is **sapgw00**. There is no default setting.

TABLE 15 Outbound SAP BAPI Adapter— Client Connection Settings *(Continued)*

Name	Description	Required Value
Message Server Hostname	Specifies the host name of the Message Server IF using Load Balancing. **Note** – Do not specify any optional Router String here, as the value will be prepended.	There is no default value.
Application Server Group	Specifies the name of the group of SAP Application Servers that will be sharing the workload. This parameter should be configured ONLY when using SAP Load Balancing.	There are no required values. There is no default setting.

Router String (optional)	Specifies the router string needed to access the SAP Application Server.
	This property is optional; use it only to gain access to an SAP system that is behind a firewall.
	The string is composed of the hostnames or IP addresses of all the SAP routers that are in between this application server and the SAP gateway host. For example, if there are two routers, *saprouter1*, and *saprouter2*, in order, from the application server to the SAP, as follows:
	`saprouter1:       204.79.199.5 saprouter2: 207.105.30.146`
	The router string in this case is as follows:
	`/H/204.79.199.5/H/207.105.30.146/H/`
	Do not omit the “/H/” tokens to begin, separate, and end the routers.
		A valid router string.
		There is no default setting.

Client Security Settings

The following Client Security Settings are used.

TABLE 16 Outbound SAP BAPI Adapter — Client Security Settings

Name	Description	Required Value
Enable SNC	Specifies whether the SNC is enabled or not.	**Yes** or **No**. The default is **No**.
SNC Partner Name	Specifies the AS ABAP SNC name.	You can find the application server SNC name in the profile parameter **snc/identity/as**. For example: p:CN=ABC, O=MyCompany, C=US

TABLE 16 Outbound SAP BAPI Adapter — Client Security Settings *(Continued)*

Name	Description	Required Value
SNC Level of Protection	Specifies the level of protection to use for the connection.	Possible values: ■ 1: Authentication only ■ 2: Integrity protection ■ 3: Privacy protection ■ 8: Use the value from snc/data_protection/use on the application server ■ 9: Use the value from snc/data_protection/max on the application server There is no default setting.
SNC Library Path	Specifies the path and file name of the external library.	The default is the system-defined library as defined in the environment variable SNC_LIB.
X.509 Certificate	Specifies the X.509 certificate information.	There is no default setting.
SNC My Name	Specifies the SNC My Name.	There is no default setting.

Connection Retry Settings

The following Connection Retry Settings are used.

TABLE 17 Outbound SAP BAPI Adapter — Connection Retry Settings

Name	Description	Required Value
Connection Retries	Number of retries to establish a connection upon failure to acquire one.	The default is **0**.
Connection Retry Interval	Milliseconds of pause before each reattempt to access the SAP system. Used in conjunction with the **Connection Retry Count** setting.	The default is **1000**.

Connection Pool Settings

The following Connection Pool Settings are used by the external database.

TABLE 18 Outbound SAP BAPI Adapter — Connection Pool Settings

Name	Description	Required Value
Steady pool size	The minimum number of physical connections the pool should keep available at all times. 0 (zero) indicates that there should be no physical connections in the pool and that new connections should be created as needed.	The default number of connections is **2**.
Maximum pool size	The maximum number of physical connections the pool should contain. 0 (zero) indicates that there is no maximum.	The default number of connections is **10**.
Max Idle Timeout in Seconds	A timer thread periodically removes unused connections. This parameter defines the interval at which this thread runs. This thread removes unused connections after the specified idle time expires. It allows the user to specify the amount of time a connection can remain idle in the pool. When this is set to greater than 0, the container removes or destroys any connections that are idle for the specified duration. A value of 0 specifies that idle connections can remain in the pool indefinitely.	The default is **300**.

Configuring the Siebel EAI Adapter Environment Properties

This task describes how to set the environment properties of the Siebel EAI Adapter.

The Adapter Environment Configuration properties contain parameters that define how the adapter connects to and interacts with other Java CAPS components within the Environment. When you create a new Siebel EAI External System, you may configure the type of External System required.

Available External System properties include:

- "Siebel EAI" on page 26.
- "HTTP Settings" on page 27.
- "Proxy Configuration" on page 27.
- "Security" on page 28.

Siebel EAI

Siebel EAI includes the configuration parameters listed in the table.

TABLE 19 Environment Configuration — Siebel EAI

Name	Description	Required Value
User Name	Specifies the user name.	No default value.

TABLE 19 Environment Configuration — Siebel EAI *(Continued)*

Name	Description	Required Value
Password	Specifies the user password.	No default value.

HTTP Settings

HTTP Settings includes the configuration parameters listed in the table.

TABLE 20 Environment Configuration — HTTP Settings

Name	Description	Required Value
URL	Specifies the default URL to be used for establishing an HTTP or HTTPS connection. If HTTPS protocol is specified, SSL must be enabled.	`http://siebel/eai_enu/start.swe` **Note –** The **URL** property does not support LDAP entries.

Proxy Configuration

Proxy Configuration includes the configuration parameters listed in the table.

TABLE 21 Environment Configuration — Proxy Configuration

Name	Description	Required Value
Proxy Host	The host name of the HTTP proxy. This specifies the HTTPS proxy host to which requests to an HTTP server or reception of data from an HTTP server may be delegated to a proxy. This sets the proxy port for secured HTTP connections.	A valid HTTPS proxy host name.
Proxy Port	The port of the HTTPS proxy.	A valid HTTP proxy port. The default is **8080**.
Proxy Username	Specifies the user name required for authentication to access the web site specified by the **URL** property.	A valid user name. **Note –** The user name is required by URLs that require HTTP basic authentication to access the web site. Be sure to enter a value for this property before you enter a value for the **Proxy password** properties.

TABLE 21 Environment Configuration — Proxy Configuration *(Continued)*

Name	Description	Required Value
Proxy Password	Specifies the password required for authentication to access the web site specified by the **URL** property.	The appropriate password. **Note –** Be sure to enter a value for the **Proxy username** properties before entering this property.

Security

The Environment Configuration Security properties are used to perform HTTP authentication and SSL connections. They include the following configuration sections:

- "Authentication" on page 28.
- "SSL" on page 28.

Authentication

Details for the Authentication settings used for HTTP authentication are detailed in the table.

TABLE 22 Environment Configuration — Security and Authentication

Name	Description	Required Value
HTTP Username	Specifies the user name for authenticating the web site specified by the URL.	A valid user name. **Note –** Enter a value for this property before you enter a value for the **HTTPpassword** properties.
HTTP Password	Specifies the password used for authenticating the web site specified by the URL.	A valid password. **Note –** Be sure to enter a value for the **HTTPusername**properties before entering this property.

SSL

Details for the SSL settings used for SSL connections are detailed in the table.

TABLE 23 Environment Configuration — Security and SSL

Name	Description	Required Value
Protocol SSL	The SSL protocol to use when establishing an SSL connection with the server. If the protocol is not set by this method, the default protocol type, **TLS** (Sun JSSE), is used.	If you are using the default Sun JSSE provider, choose one of the following settings: **TLSv1** **TLS** **SSLv2** **SSLv3** **SSL** If you are running the Sun Application Server on AIX, choose one of the following settings: **SSL-TLS** **TLSv1** **TLS** **SSLv3** **SSLv2** **SSL** For details on these settings, see the appropriate JSSE documentation.
JSSE Provider Class	Specifies the fully qualified name of the JSSE provider class. For more information, see the Sun Java Web site at: `http://java.sun.com`	The name of a valid JSSE provider class. The default is **com.sun.net.ssl.internal.ssl.Provider** If you are running the Sun Application Server on AIX, specify **com.ibm.jsse.IBMJSSEProvider**.
X509 Algorithm Name	Specifies the X509 algorithm name to use for the trust and key manager factories.	The name of a valid X509 algorithm. The default is **SunX509**. If you are running the Sun Application Server on AIX, specify **IbmX509**.
Verify Hostname	See “Verify hostname” on page 31 for further information.	

TABLE 23 Environment Configuration — Security and SSL *(Continued)*

Name	Description	Required Value
KeyStore Type	Specifies the default KeyStore type. The keystore type is used for key/certificate management when establishing an SSL connection. If the default KeyStore type is not set by this method, the default KeyStore type, JKS, is used.	
KeyStore	Specifies the default KeyStore file. The keystore is used for key/certificate management when establishing SSL connections.	A valid package location. There is no default value.
KeyStore Username	The username for accessing the keystore used for key/certificate management when establishing SSL connections. **Note –** If the keystore type is PKCS12 or JKS, the keystore username properties is not used. PKCS12 and JKS keystore types require passwords for access but do not require user names. If you enter a value for this property, it is ignored for PKCS12 and JKS.	
KeyStore Password	Specifies the default KeyStore password. The password is used to access the KeyStore used for key/certificate management when establishing SSL connections.	There is no default value.
TrustStore Type	The TrustStore type of the TrustStore used for CA certificate management when establishing SSL connections. If the TrustStore type is not set by this method, the default TrustStore type, **JKS**, is used.	A valid **TrustStore** type.
TrustStore	Specifies the default TrustStore. The TrustStore is used for CA certificate management when establishing SSL connections.	A valid **TrustStore** name. There is no default value.
TrustStore Password	Specifies the default TrustStore password. The password is for accessing the TrustStore used for CA certificate management when establishing SSL connections.	A valid **TrustStore** password. There is no default value.

Additional SSL Section Notes

Following are additional notes related to the properties in the SSL section.

Verify hostname

Description

Determines whether the host name verification is done on the server certificate during the SSL handshake.

You can use this property to enforce strict checking of the server host name in the request URL and the host name in the received server certificate.

Required Values

True or **False**; the default is **False**.

Additional information

Under some circumstances, you can get different Java exceptions, depending on whether you set this property to **True** or **False**. This section explains what causes these exceptions.

For example, suppose the host name in the URL is `localhost`, and the host name in the server certificate is `localhost.stc.com`. Then, the following conditions apply:

- If **Verify hostname** is set to **False**:

  Host name checking between the requested URL and the server certificate is turned *off*.

  You can use an incomplete domain host name, for example, `https://localhost:444`, or a complete domain host name, for example, `https://localhost.stc.com:444`, and get a positive response in each case.
- If **Verify hostname** is set to **True**:

  Host name checking between the requested URL and the server certificate is turned *on*.

  Note – If you use an incomplete domain host name, for example, `https://localhost:444`, you can get the exception `java.io.IOException: HTTPS hostname wrong`.

  You must use a complete domain host name, for example, `https://localhost.stc.com:444`

  Note – If the Java Software Developer's Kit (SDK) version used by the application server and the corresponding application server property setting do not match, you can get the exception `java.lang.ClassCastException`.

Adapter Environment Properties

Adapter External System properties must be configured from within the Environment. Until you have successfully configured all adapters for your Java CAPS project, your project cannot be properly executed or deployed. The following list identifies the Siebel EAI adapter properties. There are four Environment Configuration categories that the Siebel EAI adapter implements.

Configuring the SWIFT Alliance Gateway Adapter Environment Properties

A Project's environment properties can be modified after the adapters have been created in the Connectivity Map and the External Systems have been added to the Project's Environment.

▼ To Configure the SWIFT AG Adapter Environment Properties

1. **From the Environment Explorer tree, right-click the SAG External System and select Properties from the shortcut menu. The Properties Editor appears.**

2. **Make any necessary modifications to the Environment parameters of the SWIFT AG Adapter, and click OK to save the settings.**

SWIFT AG Adapter Environment Properties

The SWIFT Alliance Gateway Adapter Environment properties are organized into the following sections:

- "Transport" on page 32.
- "Connection Pool Settings" on page 34.

Transport

The **Transport** section of the **SWIFT AG Adapter Environment properties** contains the top-level properties displayed in the table.

TABLE 24 Environment Configuration - Transport

Name	Description	Required Value
Read From RA CFG File	Specifies the manner in which you provide the transport information. You can get RA transport information in two ways: 1. Enter the RA (resource adapter) configuration file name to read all transport information from an existing RA configuration file for your SAG RA environment. 2. Get them one by one from the adapter configuration parameters defined in the rest of this section. If this parameter is specified (not blank), it indicates that you are choosing the first option, and the RA configuration file name is expected for this parameter (for example, sagta_ra.cfg). The other parameters in this section (Host Name, Port Number, and so forth) will be ignored. If this parameter is not specified (blank), it indicates that you are choosing the second option, the other parameters in this section (Host Name, Port Number, and so forth) must be specified to provide the required transport information.	Any one of the following: - Leave the value empty (blank) to use the transport information specified in the rest of this section (Host Name, Port Number, and so forth). - Enter the RA configuration file name. All transport information is taken from the existing RA configuration file for your SAG RA environment.
Host Name	Specifies the name or IP address of the host to which you are connecting.	The host name or IP address.
Port Number	Specifies the port number of the SAG host to which the RA connects.	The port number of the SAG host to which the RA connects. The configured default is **48002**.
Ftla Port Number	Specifies the Ftla port number, the number of the port on the SAG host through which File Transfers will take place.	The Ftla port number. The configured default is **48003**.
Server DN	Specifies the Server DN, Distinguished Name used for SWIFT Alliance Gateway authentication.	The Server DN.
CA Certificate	Specifies the file that contains the Certification Authority (CA) certificate.	The CA Certificate.
SSL Mode	Specifies whether the current connection is using data encryption (SSL).	**True** or **False** depending upon whether data encryption is used. **True** indicates that encryption is used. The configured default is **True**.

Connection Pool Settings

The Connection Pool Settings section is specific for the RA connection pool of Sun Java System Application Server only. Please refer to the corresponding documentations along with your product for more details.

The **Connection Pool Settings** section of the **SWIFT AG Adapter Environment properties** contains the top-level properties displayed in the table.

TABLE 25 Environment Configuration - Connection Pool Settings

Name	Description	Required Value
Steady Pool Size	Specifies the steady pool size. The steady pool size represents the minimum number of RA connections to be maintained. When it is set to greater than 0, the container not only pre-populates the RA connection pool with the specified number, but also attempts to ensure that there is always this many RA connections in the free pool. This ensures that there are enough RA connections in the ready to serve state to process user requests. This parameter does not necessarily guarantee that no more than steady-pool-size instances exist at a given time. It only governs the number of instances that are pooled over a long period of time. For example, suppose an idle stateless session container has a fully-populated pool with a steady-pool-size of 10. If 20 concurrent requests arrive for the RA connection component, the container creates 10 additional instances to satisfy the burst of requests. The advantage of this is that it prevents the container from blocking any of the incoming requests. However, if the activity dies down to 10 or fewer concurrent requests, the additional 10 instances are discarded.	An integer indicating the steady pool size. The configured default is **1**.
Max Pool Size	Specifies the maximum pool size. This number represents the maximum number of RA connections in the pool. A value of **0** indicates that the pool is unbounded.	An integer indicating the maximum pool size. A value of **0** indicates that the pool is unbounded. The configured default is **32**.

TABLE 25 Environment Configuration - Connection Pool Settings *(Continued)*

Name	Description	Required Value
Max Wait Time in Millis	Specifies the maximum wait time in milliseconds. If an RA connection is not available, the caller must wait this long before another RA connection is created. A value of **0** indicates that an exception is thrown if there is no RA connection available. If the pool is completely utilized and the timer expires, an exception will be delivered to the application. **Note –** This element is deprecated for the bean pool container for Sun Java System Application Server.	An integer indicating the maximum wait time in milliseconds. The configured default is **60000**.
Pool Idle Timeout In Seconds	Specifies the pool idle timeout in seconds. This serves as a hint to the server. A timer thread periodically removes unused RA connections. This parameter defines the interval at which this thread runs. This thread removes unused RA connection that have an expired timeout. This allows you to specify the amount of time that an RA connection instance can be idle in the pool. When pool-idle-timeout-in-seconds is set to greater than 0, the container removes or destroys any RA connection instance that is idle for this specified duration. It is the maximum time that a component can remain idle in the pool. After this amount of time, the pool can remove this bean. A value of 0 specifies that idle RA connections can remain in the pool indefinitely.	An integer indicating the pool idle timeout in seconds. A value of 0 indicates that an idle RA connection may remain in the pool indefinitely. When the value is greater than 0, the container removes or destroys any RA connection instance that is idle for this specified duration. The configured default is **300**.

Configuring Websphere MQ Adapter Environment Properties

The WebSphere MQ Adapter parameters, accessed from the Environment Explorer tree, are organized into the following sections:

- "Inbound MQSeries Adapter — Inbound Adapter Environment Configuration" on page 36.
- "Outbound MQSeries Adapter (XA) — Outbound Adapter Environment Configuration" on page 37.
- "Outbound MQSeries Adapter (XA) — Connection Retry Settings" on page 38.
- "Outbound MQSeries Adapter (XA) — Connection Pool Settings" on page 39.
- "Outbound MQSeries Adapter — Outbound Adapter Environment Configuration" on page 40.
- "Outbound MQSeries Adapter — Connection Retry Settings" on page 41.
- "Outbound MQSeries Adapter — Connection Pool Settings" on page 42.
- "Outbound MQSeries Adapter — Connection Establishment Mode" on page 43.
- "Accessing Non-Local Queue Managers and Non-Local Queues" on page 43.

Inbound MQSeries Adapter — Inbound Adapter Environment Configuration

The **Inbound MQSeries Adapter — Inbound Adapter Environment Configuration** section of the WebSphere MQ Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 26 Inbound MQSeries Adapter — Inbound Adapter Environment Configuration

Name	Description	Required Value
Host Name	Specifies name of the computer on which the queue manager resides. This property must be left blank to cause the Adapter to use Bindings mode rather than Client mode. Bindings mode allows the Adapter to communicate directly with queue manager without a TCP/IP connection. In this mode, the Adapter and the queue manager need to be installed on the same machine. When using a Client mode connection, the Adapter communicates with the queue manager using a TCP/IP-based connection.	The name of the specific queue manager host. Leave the value blank to cause the Adapter to use **Bindings** mode.
Port Number	Specifies the number of the listen port on which the queue manager is bound.	A number indicating the port on which the queue manager is bound.
Queue Manager Name	Specifies the name of the local queue manager to which the Adapter connects. **Note –** Use only a local queue manager name in the Adapter Environment Configuration, whether bindings or Client mode is used. See “Accessing Non-Local Queue Managers and Non-Local Queues” on page 43.	The name of the local queue manager.
Channel Name	Specifies the name of the channel being used.	The name of the channel.
Coded Character Set ID	Specifies the Client Coded Character Set ID (CCSID). When left blank, the Adapter uses a default, platform-dependent CCSID. The Adapter must use a Client CCSID compatible with the queue manager’s CCSID, in order that character-based data sent to or received from the queue manager is encoded/decoded properly. If, for any reason, it becomes necessary to send character data that utilizes a different CCSID than the one specified by this setting to a queue manager, then you may invoke the Adapter OTD’s MsgHeader.setCharacterSet method from the Collaboration to temporarily override the setting.	A supported CCSID (integer) value, or none at all (blank). For a table of supported CCSID, please see the entry for the variable, **MQEnvironment.CCSID** in IBM document SC34-6066-00, **WebSphere MQ Using Java**, of your WebSphere MQ software installation.

TABLE 26 Inbound MQSeries Adapter — Inbound Adapter Environment Configuration *(Continued)*

Name	Description	Required Value
UserID	Specifies the user ID required to access the queue manager. If none is required, leave this parameter blank.	A User ID required to access the queue manager.
Password	Specifies the user password required to access the queue manager. If a password is not required, leave this parameter blank.	A user password that grants access to a specific queue manager.
SSL Enabled	When SSL is enabled, all communications are sent over a secure channel.	**Yes** or **No**. The configured default is **No**.

Outbound MQSeries Adapter (XA) — Outbound Adapter Environment Configuration

The **Outbound MQSeries Adapter (XA) — Outbound Adapter Environment Configuration** section of the WebSphere MQ Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 27 Outbound MQSeries Adapter (XA) — Outbound Adapter Environment Configuration

Name	Description	Required Value
Host Name	Specifies name of the computer on which the queue manager resides. This property must be left blank to cause the Adapter to use Bindings mode rather than Client mode. Bindings mode allows the Adapter to communicate directly with queue manager, without a TCP/IP connection. In this mode, the Adapter and the queue manager need to be installed on the same machine. When the Adapter is configured to use a Client mode connection, the Adapter communicates with the queue manager using a TCP/IP-based connection.	The name of the specific queue manager host. Leave the value blank to cause the Adapter to use **Bindings** mode. **Note** – WebSphere MQ Adapter (outbound) support for XA requires Bindings mode. The Adapter's HostName and Channel Name property values must be left blank for the Adapter to operate in Bindings mode.
Port Number	Specifies the number of the listen port on which the queue manager is bound.	A number indicating the port on which the queue manager is bound.

TABLE 27 Outbound MQSeries Adapter (XA) — Outbound Adapter Environment Configuration *(Continued)*

Name	Description	Required Value
Queue Manager Name	Specifies the name of the local queue manager to which the Adapter connects. **Note –** Use only a local queue manager name in the Adapter Environment Configuration, whether bindings or Client mode is used. See "Accessing Non-Local Queue Managers and Non-Local Queues" on page 43.	The name of the local queue manager.
Channel Name	Specifies the name of the channel being used.	The name of the channel.
Coded Character Set ID	Specifies the Client Coded Character Set ID (CCSID). When left blank, the Adapter uses a default, platform-dependent CCSID. The Adapter must use a Client CCSID compatible with the queue manager's CCSID, in order that character-based data sent to or received from the queue manager is encoded/decoded properly. If, for any reason, it becomes necessary to send character data that utilizes a different CCSID than the one specified by this setting to a queue manager, then you may invoke the Adapter OTD's MsgHeader.setCharacterSet method from the Collaboration to temporarily override the setting.	A supported CCSID (integer) value, or none at all (blank). For a table of supported CCSID, please see the entry for the variable, **MQEnvironment.CCSID** in IBM document SC34-6066-00, **WebSphere MQ Using Java**, of your WebSphere MQ software installation.
User ID	Specifies the user ID required to access the queue manager. If none is required, leave this parameter blank.	A User ID required to access the queue manager.
Password	Specifies the user password required to access the queue manager. If a password is not required, leave this parameter blank.	A user password that grants access to a specific queue manager.
SSL Enabled	When SSL is enabled, all communications are sent over a secure channel.	**Yes** or **No**. The configured default is **No**.

Outbound MQSeries Adapter (XA) — Connection Retry Settings

The **Outbound MQSeries Adapter (XA) — Connection Retry Settings** section of the WebSphere MQ Adapter Environment properties provides parameters for retrying outbound Adapter connection establishment. This section contains the top-level parameters displayed in the following tables.

TABLE 28 Environment Configuration - Outbound MQSeries Adapter (XA) - Connection Retry Settings

Name	Description	Required Value
Connection Retry Count	Specifies the maximum number of attempts made to connect to the destination queue manager. If the queue manager cannot be accessed for any reason, this setting specifies how many reattempts are made to complete the processing.	An integer indicating the maximum number of connection attempts. The configured default is **0**.
Connection Retry Interval	Specifies the amount of time (in milliseconds) between attempts to connect to the destination queue manager or queue. This is the pause between each reattempt to access the destination queue manager. Used in conjunction with the **Connection Retry Count** setting.	An integer indicating the wait time in milliseconds between connection attempts. The configured default is **1000**.

Outbound MQSeries Adapter (XA) — Connection Pool Settings

The **Outbound MQSeries Adapter (XA) — Connection Pool Settings** section of the WebSphere MQ Adapter Environment properties provides parameters for controlling the outbound Adapter's connection pool size. This section contains the top-level parameters displayed in the following table.

TABLE 29 Environment Configuration - Outbound MQSeries Adapter (XA) - Connection Pool Settings

Name	Description	Required Value
Steady Pool Size	Specifies the minimum number of physical connections the pool will keep available at all times. A value of **0** (zero) indicates that there will be no physical connections in the pool and that new connections will be created as needed.	An integer indicating the maximum number of connection kept available. The configured default is **2**.
Max Pool Size	Specifies the maximum number of physical connections the pool can contain. A value of **0** (zero) indicates that there is no maximum.	An integer indicating the maximum pool size. The configured default is **10**.

TABLE 29 Environment Configuration - Outbound MQSeries Adapter (XA) - Connection Pool Settings *(Continued)*

Name	Description	Required Value
Max Idle Timeout	Specifies the amount of time, in seconds, before an unused connection is removed from the pool. When this is set to greater than **0**, the container removes or destroys any connections that are idle for the specified duration. A value of **0** indicates that idle connections can remain in the pool indefinitely. **0** (zero) indicates that there is no maximum.	An integer indicating the idle time in seconds. The configured default is **300**.

Outbound MQSeries Adapter — Outbound Adapter Environment Configuration

The **Outbound MQSeries Adapter — Outbound Adapter Environment Configuration** section of the WebSphere MQ Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 30 Environment Configuration - Outbound MQSeries Adapter — Outbound Adapter Environment Configuration

Name	Description	Required Value
Host Name	Specifies name of the computer on which the queue manager resides. This property must be left blank to cause the Adapter to use Bindings mode rather than Client mode. Bindings mode allows the Adapter to communicate directly with queue manager, without a TCP/IP connection. In this mode, the Adapter and the queue manager need to be installed on the same machine. When the Adapter is configured to use a Client mode connection, the Adapter communicates with the queue manager using a TCP/IP-based connection.	The name of the specific queue manager host. Leave the value blank to cause the Adapter to use **Bindings** mode. **Note –** WebSphere MQ Adapter (outbound) support for XA requires Bindings mode. The Adapter's HostName and Channel Name property values must be left blank for the Adapter to operate in Bindings mode.
Port Number	Specifies the number of the listen port on which the queue manager is bound.	A number indicating the port on which the queue manager is bound.

TABLE 30 Environment Configuration - Outbound MQSeries Adapter — Outbound Adapter Environment Configuration *(Continued)*

Name	Description	Required Value
Queue Manager Name	Specifies the name of the queue manager to which the Adapter connects. **Note –** Use only a local queue manager name in the Adapter Environment Configuration, whether bindings or Client mode is used. See "Accessing Non-Local Queue Managers and Non-Local Queues" on page 43.	The name of the local queue manager.
Channel Name	Specifies the name of the channel being used.	The name of the channel.
Coded Character Set ID	Specifies the Client Coded Character Set ID (CCSID). When left blank, the Adapter uses a default, platform-dependent CCSID. The Adapter must use a Client CCSID compatible with the queue manager's CCSID, in order that character-based data sent to or received from the queue manager is encoded/decoded properly. If, for any reason, it becomes necessary to send character data that utilizes a different CCSID than the one specified by this setting to a queue manager, then you may invoke the Adapter OTD's MsgHeader.setCharacterSet method from the Collaboration to temporarily override the setting.	A supported CCSID (integer) value, or none at all (blank). For a table of supported CCSID, please see the entry for the variable, **MQEnvironment.CCSID** in IBM document SC34-6066-00, **WebSphere MQ Using Java**, of your WebSphere MQ software installation.
UserID	Specifies the user ID required to access the queue manager. If none is required, leave this parameter blank.	A User ID required to access the queue manager.
Password	Specifies the user password required to access the queue manager. If a password is not required, leave this parameter blank.	A user password that grants access to a specific queue manager.
SSL Enabled	When SSL is enabled, all communications are sent over a secure channel.	**Yes** or **No**. The configured default is **No**.

Outbound MQSeries Adapter — Connection Retry Settings

The **Outbound MQSeries Adapter — Connection Retry Settings** section of the WebSphere MQ Adapter Environment properties provides parameters for retrying outbound Adapter connection establishment. This section contains the top-level parameters displayed in the following table.

TABLE 31 Environment Configuration - Outbound MQSeries Adapter - Connection Retry Settings

Name	Description	Required Value
Connection Retry Count	Specifies the maximum number of attempts made to connect to the destination queue manager. If the queue manager cannot be accessed for any reason, this setting specifies how many reattempts are made to complete the processing.	An integer indicating the maximum number of connection attempts. The configured default is **0**.
Connection Retry Interval	Specifies the amount of time (in milliseconds) between attempts to connect to the destination queue manager. This is the pause between each reattempt to access the destination queue manager or queue. Used in conjunction with the **Connection Retry Count** setting.	An integer indicating the wait time in milliseconds between connection attempts. The configured default is **1000**.

Outbound MQSeries Adapter — Connection Pool Settings

The **Outbound MQSeries Adapter — Connection Pool Settings** section of the WebSphere MQ Adapter Environment properties provides parameters for controlling the outbound Adapter's connection pool size. This section contains the top-level parameters displayed in the following table.

TABLE 32 Environment Configuration - Outbound MQSeries Adapter - Connection Pool Settings

Name	Description	Required Value
Steady Pool Size	Specifies the minimum number of physical connections the pool will keep available at all times. A value of **0** (zero) indicates that there will be no physical connections in the pool and that new connections will be created as needed.	An integer indicating the maximum number of connection kept available. The configured default is **2**.
Max Pool Size	Specifies the maximum number of physical connections the pool can contain. A value of **0** (zero) indicates that there is no maximum.	An integer indicating the maximum pool size. The configured default is **10**.

TABLE 32 Environment Configuration - Outbound MQSeries Adapter - Connection Pool Settings *(Continued)*

Name	Description	Required Value
Max Idle Timeout	Specifies the amount of time, in seconds, before an unused connection is removed from the pool. When this is set to greater than **0**, the container removes or destroys any connections that are idle for the specified duration. A value of **0** indicates that idle connections can remain in the pool indefinitely. **0** (zero) indicates that there is no maximum.	An integer indicating the idle time in seconds. The configured default is **300**.

Outbound MQSeries Adapter — Connection Establishment Mode

The **Outbound MQSeries Adapter — Connection Establishment Mode** section of the WebSphere MQ Adapter Environment properties contains the top-level parameters displayed in the following table.

TABLE 33 Environment Configuration - Outbound MQSeries Adapter - Connection Establishment Mode

Name	Description	Required Value
Connection Mode	Specifies whether the Adapter automatically connects to the external system upon startup or connects using manual mode. When set to **Manual**, the Adapter will not connect to the external system on startup, and instead expects the user to initiate the connection by invoking the MQ Adapter OTD's **connectToQueueManager** method. Manual mode is only available when using Java Collaboration Definitions. This allows you to dynamically connect to different Queue Managers. Any parameters assigned in the Java Collaboration will override the same parameters specified in the Connectivity Map or Environment properties.	**Automatic** or **Manual**. The configured default is **Automatic**.

Accessing Non-Local Queue Managers and Non-Local Queues

When used with alias queues and remote queues, the WebSphere MQ Adapter functions with several restrictions. Alias queues and remote queues with local queue definitions may be accessed in the same way as actual local queues, through the use of the Adapter OTD's accessQueue(String) method. Remote queues without local queue definitions need to use the accessQueue(String, String) method instead.

Also, when alias queues or remote queues are used, the Adapter cannot proactively verify the connection (and reconnect, if necessary) before each OTD operation. This is because the Adapter verifies connections by querying queue objects, and it is not possible to query alias queues and remote queues. This means that when alias queues or remote queues are used with the Adapter, the Collaboration is responsible for recovering connection failures itself, including reestablishing the queue manager and queue connections as needed. For more information, refer to the WebSphere MQ Adapter Javadoc.

Connecting to a Remote WebSphere MQ Queue

When an Adapter connects to a local queue manager and accesses one of its queues, that queue is a local queue. When an Adapter connects to a remote queue manager and accesses one of its queues, then that queue, is also a local queue. In WebSphere MQ terms, a remote queue is a queue that is managed by a queue manager other than the one to which the application (in this case, the Adapter) is connected.

For example, say that there are two queue managers, QM1 and QM2. QM1 manages a queue (Q1) and runs on Host1. QM2 manages a queue (Q2) and runs on Host2.

Furthermore, say that need to send messages to Q2, but the Adapter may only communicate with Host1 (that is, Host2 is unreachable from the system in which the Adapter is executing). By creating the appropriate channels and a remote queue definition (R1 on QM1), messages sent to R1 can be shuttled automatically to Q2 on QM2.

For this example, the Queues and the Adapter are configured as follows:

▼ Creating a Channel and Remote Queue Definition

1. **If either QM1 or QM2 do not have a transmission queue defined, create one. Both queue managers require one transmission queue each. In this example, assume that both queue managers have the transmission queue 'xmit'.**

2. **Create a Sender Channel for QM1 that points to Host2 and transmission queue xmit. The name of the channel must match the Receiver Channel created in the next step.**

3. **Create a Receiver Channel for Q2. The name of the channel must match the Sender Channel created in the previous step.**

4. **In QM1, create a Remote Queue Definition (R1). Designate Q2 as its remote queue, QM2 as its remote queue manager, and xmit as its transmission queue.**

5. **Configure the MQ Adapter to connect to Host1, QM1, and have it put messages into queue R1.**

Note – Messages cannot be read/GET from remote queues, only PUT. In the example situation above, to read the messages placed in QM2:Q2 through R1, an Adapter needs to connect directly to QM2 (Host2), thereby interacting with Q2 as a local queue.