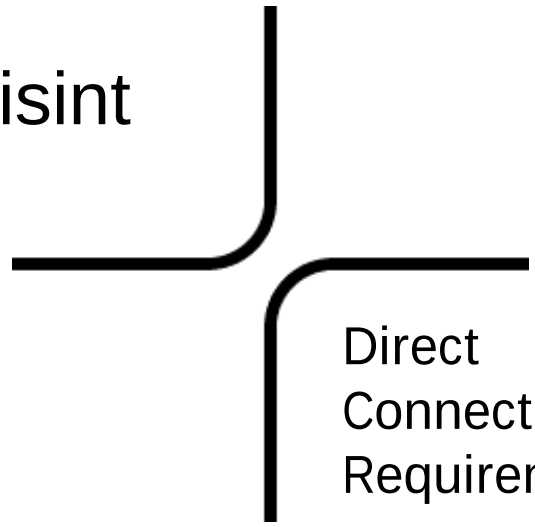

Direct Connectivity Requirements v0.4

Compilation started on July 30, 2003
Compiled by:
Tracey Birkenhauer
tbirkenh@covisint.com

TABLE OF CONTENTS

1 Overview

Trading partners can directly connect to the Covisint Connect data messaging hub via communication protocols that include FTP, HTTP(S) and WebSphere MQ. Transport options include the public Internet, Advanced Network Exchange (ANX), European Network Exchange (ENX) or other Virtual Private Networks (VPNs). For more information, please see the "Connectivity Matrix," Figure 1. Each trading partner will determine the pipeline and protocol they will use to exchange messages.

These options and relative requirements are briefly described in the remainder of this document. For more technical information, please review the attached connectivity user guides.

For many trading partners, the connectivity option will be clear and pre-defined. Others may require assistance to determine the best integration solution based on specific requirements and capabilities. There is no single or preferred solution. Each trading partner must determine the proper approach independently, based on current and projected circumstances.

It is assumed that readers of this document:

- will implement one of the available connectivity options.
- possess the technical expertise to implement one of the available connectivity options.

If you require technical assistance or have specific questions, contact connectsupport@covisint.com.

Connectivity Options	Configuration Options	Access	Transport	Message Packaging	On-Ramp Available
FTP Connector	Mailbox Push/Push (Put/Put)	Manual/automated Automated only	xNX or VPN	ebXMLite or none	yes
HTTP(S) Connector	Mailbox Post/Post	Manual/automated Automated only	xNX/VPN/Public Internet/SSL	ebXMLite or none	Yes
WebSphere MQ Connector	Put/Put	Automated only	xNX, VPN or public Internet (using IPT)	ebXMLite or none	yes

Figure 1: Connectivity Matrix

Covisint Connect messaging hub - Logical Architecture

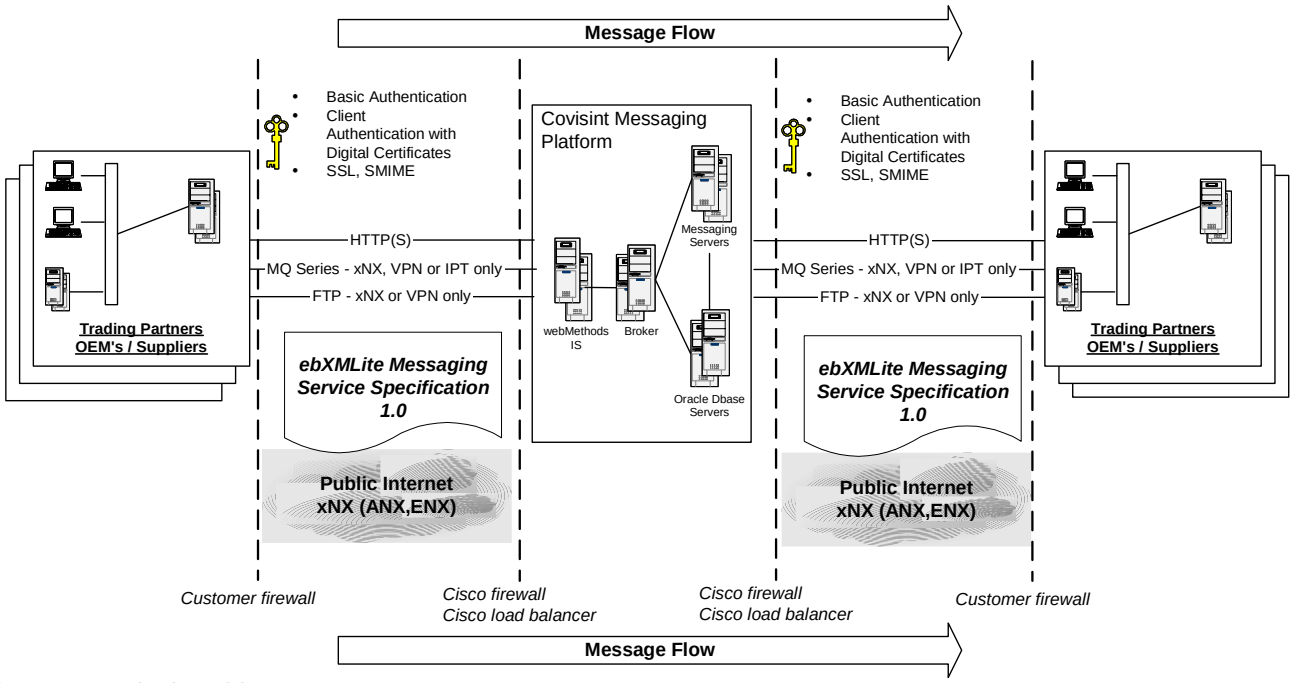

Figure 2: Logical Architecture

2 FTP Connector

With the FTP Connector, you can use FTP commands to exchange information with your trading partners through the Covisint messaging hub.

FTP Connector users must know the appropriate FTP commands and how to use them appropriately. The FTP Connector interface allows users with standard FTP client software and TCP/IP communications over ANX, ENX or VPN to execute the following actions:

- Submit business documents to be processed by the Covisint messaging hub.
- Retrieve business documents from a Covisint messaging hub mailbox.

2.1 FTP Overview

Covisint has implemented FTP access to the messaging hub using a custom FTP server. File transfers use normal FTP commands. In other words, FTP commands such as “get” and “put” are no different than standard FTP used today.

2.2 FTP Requirements

Our requirements assume FTP users have a secure Internet connection over a VPN or ANX/ENX.

2.3 FTP Functional Description

Covisint does not provide the FTP client necessary to access the FTP Connector. See the list of tested FTP clients below.

Platform	OS Version
Sun	Sun Solaris 2.6 - Sun Solaris 5.9
Microsoft Windows	98/2000/XP

The FTP Connector does not support the Record or Block transfer structures, but does meet the minimum requirements for the RFC 959 FTP implementation.

The “push/pull” approach is common when a customer does not operate an FTP server. This approach allows the customer to use standard FTP client software to “push” data to an FTP server.

3 HTTP(S) Connector (Post-Post)

With the "Post-Post" type of connectivity, you can use a Web server and programmatic HTTP(S) client to exchange information with your trading partners. To use the HTTP(S) Connector, you should have prior knowledge of the HTTP(S) protocol, Web servers and TCP/IP networking basics.

3.1 HTTP(S) Connector (Post-Post) Overview

The HTTP(S) Connector is a component of the Covisint Connect messaging hub. It supports two modes of connectivity - "Post-Post" mode and "Mailbox" mode. “Mailbox” mode is explained below.

The HTTP(S) Connector in the "Post-Post" mode allows a trading partner (TP) with a standard HTTP(S) server and/or client software to perform the following tasks:

- Connect to Covisint using a unidirectional or bi-directional TCP/IP link over the public Internet, VPN tunnel or ANX/ENX networks.
- Submit business documents to be processed by Covisint using a regular programmatic client on the inbound (to Covisint) HTTP connection.
- Get business documents from Covisint using a regular Web server on the outbound (from Covisint) HTTP connection.
- Perform secure communications over SSL (HTTPS), if required.

All trading partners have the choice of inbound-only, outbound-only or bi-directional connectivity with the HTTP(S) Connector "Post-Post" mode.

3.2 HTTP(S) Connector (Post-Post) Requirements

Before you can connect, some necessary communication requirements must be satisfied. The following table lists the connectivity information for the HTTP(S) Connector:

Connection	IP Address	Port
Public Internet	64.37.249.63 (https://messaging.covisint.com)	443
ANX	206.18.241.63	443
ENX	To be determined, contact connectsupport@covisint.com	TBD
VPN	To be determined, contact connectsupport@covisint.com	TBD
Messaging Admin on public Internet	https://connect.covisint.com	443

When using the public Internet, secure HTTP over SSL (HTTPS) is required. For a highly secure VPN connection, plain HTTP should be used since double encryption reduces communication channel performance. When using secure ANX or ENX networks, you may request HTTPS for additional connection-level security, though it's not required.

3.3 HTTP(S) Connector (Post-Post) Functional Description

On the inbound flow to Covisint, the HTTP(S) Connector accepts client posts, extracts message data and optional routing information from the HTTP POST request and sends it to the Covisint Connect Document Recognition Service. The HTTP(S) Connector acknowledges all successful posts by sending a Tracking ID back to the client.

On the outbound flow from Covisint, the HTTP(S) Connector posts the message to the trading partner's Web server. The message payload is contained in the body of the HTTP POST request. The Tracking ID is supplied in the HTTP POST request header.

4 HTTP(S) Connector (Mailbox)

With the HTTP Mailbox, you can use a Web browser or programmatic HTTP client to exchange information with your trading partners through the Covisint messaging hub. To use the HTTP Mailbox, you should have prior knowledge of HTTP(S) protocol, Web servers and TCP/IP networking basics. The loopback test implies the basic knowledge of EDI document standards.

4.1 HTTP(S) Connector Mailbox Overview

The HTTP Mailbox is a component of the HTTP Connector. It allows users with standard HTTP(S) client software or a Web browser to perform the following tasks:

- Connect to the Covisint messaging hub using unidirectional (to Covisint) TCP/IP link over the public Internet, VPN tunnel or ANX/ENX networks.
- Submit business documents to be processed by the Covisint messaging hub.
- Retrieve business documents from their Covisint messaging hub Mailbox.

4.2 HTTP(S) Connector Mailbox Requirements

Before connecting to the messaging hub HTTP Mailbox, the necessary communication requirements must be satisfied. The following table lists the connectivity information for the HTTP Mailbox:

Network	IP Address	Port
Public Internet	64.37.249.63 (messaging.covisint.com)	443
ANX	206.18.241.63	443
ENX	To be determined, contact connectsupport@covisint.com	TBD
VPN	To be determined, contact connectsupport@covisint.com	TBD

4.3 HTTP(S) Connector Mailbox Functional Description

On the inbound flow to Covisint, the HTTP Mailbox accepts the client posts, extracts the message data and routing information and sends it to the Covisint messaging hub's Document Recognition Service. The HTTP mailbox acknowledges all successful posts by sending a so-called messaging hub Tracking ID back to the client.

On the outbound flow from Covisint, the HTTP Mailbox is able to return the mailbox directory and any of the available messages, queued on the mailbox database table. All outbound data is returned as the body of the HTTP response. That is why, from a network perspective, the HTTP mailbox requires inbound-only TCP/IP connection - from the customer to the Covisint messaging hub.

5 WebSphere MQ Connector

Due to the nature of the WebSphere MQ Connector (formerly called MQ Series) protocol, Covisint and each trading partner will jointly design and perform most of the configuration steps. Because of this, no technical description is available for this connectivity option in this document. To establish an MQ Connector communication channel with Covisint, both the trading partner and Covisint must perform, agree upon and communicate a set of system configurations. Typically, trading partners write their own MQ Connector client program to send messages to and retrieve messages from Covisint. If your client program requires Covisint to do some special processing of the message, (i.e., to manipulate MQMD or RFH headers), please contact Covisint to jointly design and implement a solution. Trading partners can connect to the Covisint Connect messaging hub using the WebSphere MQ Connector and MQ Connector via MQIPT.

5.1 MQ Connector Overview

Once communication channels are established between a trading partner's MQ queue manager and Covisint's MQ queue manager, they can complete the following tasks:

- Send business documents to Covisint that will be routed to their trading partners.
- Receive business documents from their trading partners via the Covisint messaging hub.

Connect to Covisint using WebSphere MQ Queue Manager

Due to security considerations, Covisint supports this connectivity option over ANX, ENX or Internet VPN.

Connect to Covisint using WebSphere MQ Queue Manager and MQ Internet Pass Thru

MQ Internet pass-thru is a WebSphere extension that can be used to implement a messaging integration solution between two remote sites across the Internet.

Covisint supports this connectivity option over the public Internet. Covisint recommends using the following protocols and security settings:

- MQ native or HTTP tunneling
- SSL encryption
- Client certificate authentication

5.2 MQ Connector Requirements

Covisint's requirements assume that trading partners have IBM WebSphere MQ 5.x and/or MQIPT 1.x and an MQ client program capable of sending and receiving messages.

For the safety of the message, we recommend that trading partners configure MQ channels as "**normal**" type and only send "**persistent**" and "**non-expire**" messages to Covisint.
For those trading partners who are using MQIPT with SSL and client authentication, they must provide their CA's certificate. Covisint uses Verisign as its certificate authority. Obtain the Verisign certificate at http://www.verisign.com/.