covisint
a subsidiary of Compuware Corporation

AS2 Connector

Product Revision Level 2.1.0

Table of Contents

INTRODUCING AS2 CONNECTOR

This user guide contains information you will need to exchange messages with Covisint using the AS2 Protocol.

The AS2 protocol enables trading partners to securely exchange business data for XML, binary and EDI or any other data describable in MIME on HTTP or SMTP. Data is packed in standard MIME content type. Cryptographic Message Syntax (S/MIME) security body parts are used to implement data security, authentication and privacy based on the standard encryption and digital signature algorithms.

This document assumes that you have knowledge of the AS2 protocol, HTTP(S), Web servers and TCP/IP networking basics. The connectivity test implies basic knowledge of EDI document standards. The intended audience for this document includes TP integration developers, network engineers and customer connection support staff and third-party organizations. Contact connectsupport@covisint.com with questions or concerns.

AS2 Specification - Overview

This section briefly described the AS2 specification. Please refer to the AS2 specification for details at http://www.ietf.org/internet-drafts/draft-ietf-ediint-as2-15.txt.

The complete loop of secure B2B exchange of EDI or other data using AS2 protocol involves the following steps:

1. The sender sends a signed and encrypted EDI message to the receiver on HTTP. The HTTP request from the sender includes standard HTTP headers as specified by the specification and the AS2 HTTP header extensions. One of the extension requests a signed acknowledgement. The acknowledgement is called Message Disposition Notification (MDN).

2. The receiver decrypts the message and verifies the signature resulting in the verified integrity of data and authenticity of the sender.

3. The receiver returns a signed receipt i.e. MDN. The MDN includes the hash of the signature (Message Integrity Check - MIC value) from the received message, indicating to the sender that the received message was verified and/or decrypted properly.

4. The sender verifies the MDN and validates the MIC to confirm that the message was successfully and securely delivered.

The EDI data is sent as a MIME/SMIME messages. Encryption and digital signature are both optional. Thus there are four modes of sending a message:

1. Signed and encrypted – recommended
2. Signed only
3. Encrypted only
4. No signature, No encryption – The EDI payload is sent in a MIME message. This option is not recommended for secure transmission using AS2 protocol.

AS2 Header extensions:

The AS2 specification defines a set of extensions to the HTTP header for sending the message. They are:

1. Message-Id: Message Identifier
2. AS2-Version: Version of the AS2 protocol.
3. AS2-From: Value identifying the sender of the message. This can be a value that is a DUNS number, or any identifier that is mutually agreed between trading partners.
4. AS2-To: Value identifying the receiver of the message. This can be a value that is a DUNS number, or any identifier that is mutually agreed between trading partners.
5. Disposition-notification-to: Sender requests an MDN from the receiver by placing this header in the message.

6. Receipt-Delivery-Option: The sender requests an asynchronous MDN by placing this header field. It specifies the URL to which the MDN should be posted. Absence of this field indicates a request for a synchronous MDN.
7. Disposition-Notification-Options: This header has a detailed syntax. It indicates if the sender requests a signed MDN and the MIC algorithm(s) to be used by the receiver while computing the MIC over the payload.

Message Disposition Notification (MDN): The MDN is an acknowledgement receipt sent by the receiver that indicates a secure and successful receipt of the message. The MDN is formatted as a MIME multipart/report that has two parts:

- Human readable MIME part
- Machine readable MIME part

The MDN is digitally signed if requested by the sender. The machine-readable MIME part of the MDN includes a MIC that is computed on the received message. The algorithm specified in the request is used to compute the MDN. An MDN is also sent as negative acknowledgement, if there are errors while decrypting the message, verification of digital signature or any other processing error. Please refer to the specifications for details of the syntax of the MDN.

Overview – AS2 Connector

The AS2 Connector is a component of the Covisint Connect messaging hub. Covisint Connect supports AS2 on HTTP(S) only. It supports the entire AS2 specification in both directions. Thus you can

- Send and receive unsigned – unencrypted data.
- Send and receive signed data.
- Send and receive encrypted data.
- Send and receive signed-encrypted data.
- Do not request a receipt
- Request unsigned receipt.
- Request signed receipt.
- Request synchronous receipt.
- Request asynchronous receipt.

All trading partners have the choice of inbound-only, outbound-only or bi-directional connectivity with the AS2 Connector.

Covisint Connect AS2 Features:

- Covisint recommends signed-encrypted exchange of data, with requests for signed receipts.
- Covisint support both "sha1" and "md5" message digest algorithms on digital signatures for all messages sent to Covisint. Covisint uses "sha1" message digest algorithms only for digital signatures for all messages sent from Covisint.
- Covisint will assign an AS2 Identifier for exchanging messages via the AS2 protocol.
    - For messages sent to Covisint, the AS2 Identifier should be set as the value of "AS2-From" header field. "AS2-To" should be set to "COVISINT".
    - For messages sent from Covisint, the AS2 Identifier will be set as the value of "AS2-To" header field. "AS2-From" will be set to "COVISINT".

HOW TO PERFORM INITIAL SETUP – AS2 CONNECTOR

Obtain User ID and Password to access Covisint Connect

Please register at Covisint Web site (http://www.covisint.com/services/connect/connectBuy.shtml)to get access to the Covisint Connect application. Covisint provides you with an account and password to access the administration Web application that allows you to manage your trading partner profile, channels, relationships and view the transaction log.

Determine Type and Attributes Of Network Connection

Before you can connect, some necessary communication requirements must be satisfied. The following table lists important connectivity information for the AS2 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

The following URL should be used for all AS2 HTTP posts:

https://messaging.covisint.com/invoke/AS2Connector.inbound/receive

Provide Covisint with Type and Attributes of Network Connection to Your AS2 Server

E-mail your connectivity information (network type, IP address, URL, username, password) and connection test scenario to connectsupport@covisint.com. Use the Trading Partner Web Server Configuration Form in the Appendix.

How to set up AS2 Sending Channel

An AS2 Sending channel should be set up on Covisint Connect to send AS2 messages to Covisint. Go to the Connect administration web application to request an AS2 sending channel.

The steps to set up an AS2 sending channel are as follows:

1) Click on the "Create Channel" link under the "Channels" tab.

2) Select "Active Sending" and click continue.

3) Select "AS2" and click continue.

4) A web page will display a form to specify the "AS2 Sending Channel" configuration. This form has multiple sections described below.

5) Channel Properties:

   a) Channel Name – Give this any meaningful name.

   b) Channel Wrapper – Set it to the default value of "None".

6) AS2

   a) Certificate with Your Public Key – If you intend to send signed and/or encrypted AS2 messages to Covisint, your public certificates should be loaded to connect. Use this option to select an existing certificate. If you need to upload the certificate, click the "Add Certificate" option.

   b) AS2-From Id – Specify the Covisint provided AS2 Identifier in this field. This value should be used in "AS2-From" header while sending messages to Covisint.

   c) Username for Async MDN – This is an optional field. It is the user name to be used for basic authentication by Covisint Connect to post an asynchronous MDN receipt.

   d) Password for Async MDN – This is an optional field. It is the password to be used for basic authentication by Covisint Connect to post an asynchronous MDN receipt.

7) Channel Authentication – Optional basic authentication credentials used to send AS2 messages to Covisint Connect.

8) Enter the "Request Notes" and click the continue button.

9) Review the selections and click "Create Channel" to create the channel.

10) A Covisint Connect representative will contact you to activate and test the AS2 channel. They will provide Covisint's public certificates as needed.

How to set up AS2 Receiving Channel

An AS2 Receiving channel should be set up on Covisint Connect to receive AS2 messages from Covisint. Go to the Connect administration web application to request an AS2 receiving channel.

The steps to set up an AS2 receiving channel are as follows:

1) Click on the "Create Channel" link under the "Channels" tab.

2) Select "Active Receiving" and click continue.

3) Select "AS2" and click continue.

4) A web page will display a form to specify the "AS2 Receiving Channel" configuration. This form has multiple sections described below.

5) Channel Properties:

   a) Channel Name – Give this any meaningful name.

   b) Channel Wrapper – Set it to the default value of "None".

6) AS2

   a) Certificate with Your Public Key – If you intend to receive signed and/or encrypted AS2 messages from Covisint, your public certificates should be loaded to connect. Use this option to select an existing certificate. If you need to upload the certificate, click the "Add Certificate" option.

   b) Delivery URL- Specify the URL of your AS2 service. Do not use DNS names in the URL. Specify a public IP address of your server, e.g. *https://12.23.23.21/AS2/accept*

   c) Handler – Do not touch this field. Leave it to its default value.

   d) Request MDN Receipt – Specify if Covisint should request a receipt. Covisint recommends setting this value to "Yes".

   e) Synchronous MDN – This field shows up only if you selected *Yes* for item *d)*. Specify if the MDN receipt should be synchronous or not.

   f) Signed MDN - This field shows up only if you selected *Yes* for item *d)*. Specify if the MDN receipt should be signed. Covisint recommends setting this value to "Yes".

   g) AS2 Mode - Specify if the message transmission mode as Signed, Encrypted, Signed Encrypted or none. We recommend setting it to "Signed Encrypted".

   h) AS2-To Id – Specify the Covisint provided AS2 Identifier in this field. Covisint Connect will use this value in "AS2-To" header while sending messages.

i) Number of Tries - Specifiy number of retry attempts for reliable delivery.

j) Retry Interval - Specify retry interval in seconds.

7) Channel Authentication – Optional basic authentication information for your AS2 server required to send AS2 messages from Covisint Connect.

8) Enter the "Request Notes" and click the continue button.

9) Review the selections and click "Create Channel" to create the channel.

10) A Covisint Connect representative will contact you to activate and test the AS2 channel. They will provide Covisint's public certificates as needed.

APPENDIX

TP AS2 Configuration Form

Complete the form below and submit to connectsupport@covisint.com.

Covisint TP Web Server Configuration Form	
Covisint-assigned Trading Partner ID	
Trading Partner company name	
Company postal address	
Corporate Web Site	
Administrative contact (e-mail, phone, pager)	
Technical contact (e-mail, phone, pager)	
Network type (Internet, ANX, ENX, VPN)	
Web server DNS name	
Web server IP address	
Inbound URL	
Desired AS2 ID	
Desired AS2 Mode	
Desired MDN Mode	
Username	
Password	Send in separate e-mail
Connection test scenario	

Glossary

The following terms are used in the guide:

ANX - Advanced Network Exchange (formerly Automotive Network Exchange) used throughout North America. ANX is a TCP/IP network comprised of trading partner subscribers, certified service provider and network points allowing for efficient and secure electronic communications among subscribers, with only a single connection.

AS2 Connector – A Covisint Connect messaging hub component that provides access to messaging hub services using the AS2 protocol.

Basic Authentication - A secure method of authentication that uses HTTP and HTTP over SSL (HTTPS), in which the server authenticates via the user name and password obtained from the HTTP client

EDI - The Electronic Data Interchange group of standards.

ENX - European Network Exchange

HTTP – Hypertext Transfer Protocol, an application-level protocol standard (defined in RFC2616) used on IP networks, such as the Internet, to transfer Web content between computers.

ISA, GS, ST - EDI standard definitions for the specific parts of a business document.

SSL - Secure Socket Layer protocol that provides data encryption, server authentication, message integrity and optional client authentication for TCP/IP connections.

TCP – A transport-level protocol widely used on IP networks, including the Internet.

TP – Trading Partner

VPN - Virtual Private Network, which is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.