

OpenAS2 Server Application

Table of Contents

1. Introduction.....	2
2. Glossary.....	2
3. Installing OpenAS2.....	2
3.1. System Requirements.....	2
3.2. Installing Application.....	3
3.3. Tuning Java.....	4
4. Configuration.....	4
5. Application Configuration.....	5
5.1. AS2 Message Tracking.....	5
5.2. Overriding Certificate Store Password.....	7
5.3. Resend Retry Configuration.....	7
5.4. File Name Parsing.....	8
6. Partner Configuration.....	8
6.1. Partner Definition.....	9
6.2. Partnership Definition.....	9
6.3. Configuring the AS2 Message ID.....	9
6.4. Transfer Encoding.....	10
6.5. Supported Encoding Algorithms.....	10
6.6. Message Compression.....	10
6.7. Custom Mime Headers.....	11
6.7.1. Static Header Values.....	11
6.7.2. Dynamic Header Values From File Name.....	11
Delimiter Mode.....	11
Regular Expression Mode.....	12
6.7.3. Adding Custom Headers To HTTP.....	13
6.8. Setting Dynamic Attributes From File Name.....	13
7. Certificate Configuration.....	14
7.1. Creating And Importing.....	14
7.2. Supporting Multiple Private Certificates.....	15
8. Logging System.....	15
8.1. Log Level Configuration.....	16
8.2. Email Logging Configuration.....	16
9. MDN Configuration.....	17
9.1. Asynchronous MDN Receiver Configuration.....	17
9.2. Asynchronous MDN Sender Configuration.....	17
10. Configuring HTTPS Transport.....	18
10.1. Inbound Transfers.....	18
10.2. Outbound Transfers.....	18
11. Running OpenAS2.....	18
11.1. Starting OpenAS2.....	19
11.2. Command Entry.....	20
11.3. Automated Launching As UNIX Daemon.....	21
11.3.1. INIT.D Service.....	21
11.3.2. SYSTEMD Service.....	22
12. Testing OpenAS2 Transfers.....	22

12.1. Using HTTPS Transport.....	22
13. Troubleshooting OpenAS2.....	23
13.1. Canonicalization For MIC Algorithm.....	23
13.2. Binary Encoding.....	23
13.3. HTTP Restricted Headers.....	24
13.4. CMS Algorithm Protection.....	24
13.5. SSL Certificate Exceptions.....	24
13.6. Java Versions Prior To 1.6.....	26
13.7. Mime Body Part Logging.....	26
13.8. TLSv1.2.....	26
14. Partner AS2 Compatibility Settings.....	26
15. Remote Control.....	27
16. Dynamic Variables.....	27
17. Appendix: config.xml file structure.....	29
18. Appendix: partnership.xml file structure.....	37
19. Appendix: command.xml file structure.....	39
20. Appendix: Updating database structure.....	39
21. Appendix: Creating database DDL for external databases.....	40

1. Introduction

The OpenAS2 application enables you to transmit and receive AS2 messages with EDI-X12, EDIFACT, XML, or binary payloads between trading partners. The AS2 implementation conforms with [RFC4130](#).

This document describes how to install, configure and use OpenAS2. In this document a partner can be either your own company or a company you will be exchanging data with using AS2.

The sample configurations in this document are based on Unix type OS but in general the only significant difference is that it may be necessary to use “\” instead of “/” for folder name separators on Windows based machines but because the application is Java it should work fine leaving the “/” for the most part as Java will do the conversion if necessary.

This document is valid for version 2.2.0 and up.

2. Glossary

EDI – Electronic Data Interchange

MDN - Message Disposition Notification

3. Installing OpenAS2

3.1. System Requirements

To be able to run the OpenAS2, you will need:

1. Java™ installed on the machine you intend to run the OpenAS2 server on – this document uses Java 1.6.

2. The OpenAS2 package version you wish to use. The downloadable packages can be found here: <https://sourceforge.net/projects/openas2/files>
3. Java Cryptography Extension (JCE) policy files - you can download the correct version from the Java website. Search “Java Cryptography Extension Unlimited Strength” to find the right cryptography extension for your version of Java. The current link for Java8 is [here](#).

3.2. Installing Application

The following steps will provide an installed app on a target machine:

1. Unzip the downloaded OpenAS2 package into a suitable location, which we will call `<install_dir>`.

NOTE: Typical values for `<install_dir>` locations are `/opt/OpenAS2` under Linux®/Unix or `C:\OpenAS2` under Microsoft® Windows®.

2. For the encryption and certificate management to work correctly, you must have the proper JCE policy files installed in your version of Java (see system requirements above). The downloaded zip archive contains the two files `local_policy.jar` and `US_export_policy.jar`. Install them into your Java location under `<JAVA_HOME>/lib/security`. Back up the existing files before installing these new ones. There are numerous detailed articles on the web for installing these files if you need more information.

The file structure will look something like the figure below without the data and logs folders which are created automatically by the server when it starts based on configuration if they do not exist.

Name	Date Modified	Size	Kind
bin	Today 13:52	--	Folder
commons-logging.properties	3 August 2015 23:38	66 bytes	Java p...ies
gen_p12_key_par.sh	27 July 2015 19:07	2 KB	shell script
start-openas2.bat	Today 00:06	3 KB	MacVi...ume
start-openas2.sh	2 August 2015 22:55	999 bytes	shell script
build.xml	4 August 2015 17:52	3 KB	XML text
config	4 August 2015 22:53	--	Folder
as2_certs.p12	27 July 2015 19:17	5 KB	person...S#
commands.xml	16 August 2010 09:58	1 KB	XML text
config.xml	3 August 2015 23:21	4 KB	XML text
emailtemplate.txt	16 August 2010 09:58	166 bytes	text
partnerships.xml	3 August 2015 22:41	2 KB	XML text
data	Yesterday 23:38	--	Folder
OpenAS2A_OID-OpenAS2B_OID	Yesterday 23:38	--	Folder
OpenAS2B_OID-OpenAS2A_OID	4 August 2015 22:56	--	Folder
resend	4 August 2015 22:55	--	Folder
temp	Yesterday 23:38	--	Folder
toAny	4 August 2015 22:55	--	Folder
toOpenAS2A	Yesterday 23:37	--	Folder
toOpenAS2B	Yesterday 23:38	--	Folder
lib	4 August 2015 22:53	--	Folder
logs	Today 00:05	--	Folder
log-08042015.txt	4 August 2015 22:56	3 KB	text
log-08052015.txt	Yesterday 23:38	5 KB	text
log-08062015.txt	Today 14:03	216 bytes	text
manifest.mf	1 August 2015 08:46	68 bytes	Unix E...le F
src	1 August 2015 22:34	--	Folder

3.3. Tuning Java

The default settings for the Java virtual machine in the startup script (start_openas2.sh or start_openas2.bat) will work for installations on most machines for low volume/small file size transfers. However, if your system will be transferring large files you will need to increase memory allocation. If you expect to support very high AS2 traffic you will need to increase memory allocation and possibly tune the garbage collector to get reasonable performance.

How much you can increase memory allocation to Java will depend on how much RAM is installed on the system running OpenAS2 and how many other processes will be running concurrently that will also require memory. Most systems deploy with at least 8GB RAM these days so increasing memory allocation from the default amount in the startup script should not cause adverse affects to the system.

To increase memory allocation you need to increase the heap space. This is set using the -Xmx option. You could increase this from the 384m (m = MB) default setting to 1g or 2g to get good performance for large files or busy systems and for very large files given enough RAM you can set it to 6g or 8g. Search for “-Xmx” in the startup script and adjust accordingly.

For garbage collection you may want to allocate a more appropriate garbage collector than the default parallel collector that is the default in Java. In Java 7 and up, the G1 collector is ideal if you use large heap space allocation. To enable it add this to the command line parameter:

```
-XX:+UseG1GC
```

4. Configuration

This section explains the details of the configuration files and how they link together.

The OpenAS2 server uses four files to configure and execute:

1. config.xml – configures the application
2. partnerships.xml – configures the partners and partnerships
3. as2_certs.p12 – stores the PKCS12 certificates for all partners
4. commands.xml – stores the commands that the application will support. This file should not be modified

IMPORTANT: A restart of the application is required to load any configuration changes.

The folder containing the config.xml file defines the *home* configuration parameter that can be used to reference other files on the file system relative to a known base folder in the app. This is done by encapsulating *home* in percentage signs (%*home*%). All files can be referenced relative to this parameter and it is how the default config.xml file defines the location of other configuration and data file locations used by the OpenAS2 application.

5. Application Configuration

The file named “config.xml” configures the modules that will be activated by the AS2 server when it starts up. This file can be located anywhere within the disk subsystem on which the OpenAS2 application runs as it is passed into the application as a startup parameter.

Some of the key configuration settings in the config.xml file are:

- define the modules to be activated in the OpenAS2 application
- override module default classes in the AS2 code base
- enhance or change behaviour of modules and the inputs and outputs of the modules.
- define the location of the certificates keystore and password
- define the location of the partnerships configuration file
- specify the listening ports

See appendices for a detailed definition of the config.xml file structure.

There are 2 listening ports for inbound connections (see partnerships.xml config for outbound connections) used for:

1. receiving messages and synchronous MDN's – default port number 10080
2. receiving asynchronous MDN's - default port number 10081

The port numbers are arbitrary and defaulted to a number above 1024 that does not require root access to listen on (normally on Unix type systems any port below 1024 requires root access). The port values are important to the partner you will be communicating with if they will be sending AS2 messages to your system. For outbound only systems, it is only necessary to have a listener for asynchronous MDN's if using that mechanism for MDN's.

Each module has a number of attributes that can be configured on the module element to control and change how the module behaves.

5.1. AS2 Message Tracking

As of version 2.1.0 the system will track key events in the message transmission and reception process and invokes any configured action handlers that can then process the information in some way. The default deployment of OpenAS2 supports a database tracking module that will write the message state to an embedded H2 database. As an AS2 message is processed, key points are logged to the database for a given message as a single record. As the message reaches the next state, the system overwrites the previous state.

The database tracking uses the module "org.openas2.processor.msgtracking.DbTrackingModule".

Configuration parameters for the database tracking functionality are shown in the table below.

Function	Attribute Name	Default Value
Database name	db_name	openas2

Function	Attribute Name	Default Value
Database user name	db_user	sa
Database password	db_pwd	OpenAS2
Database file directory – used for embedded database	db_directory	%home%/config/DB
Use Embedded Database	use_embedded_db	true
Escape character for SQL strings	sql_escape_character	' (single quote)
JDBC connect string	jdbc_connect_string	jdbc:h2:\$component.db_directory\$/\$component.db_name\$
JDBC Driver – not necessary if using at least JDBC 4.0	jdbc_driver	org.h2.Driver
Force loading of the JDBC driver class. Use if there are issues with JDBC	force_load_jdbc_driver	false
Provide JDBC access to H2 via TCP	tcp_server_start	true
H2 Listening port for the JDBC access	tcp_server_port	9092
H2 Password for the TCP server	tcp_server_password	openas2

Use of an external database can be configured for any database that has a JDBC driver such as Oracle, MySql or Postgresql.

To use an external database, the “**use_embedded_db**” must be set to “**false**” and the appropriate settings changed in the database tracking module XML. Below is a sample configuration for using Postgresql database:

```
<module classname="org.openas2.processor.msgtracking.DbTrackingModule"
  use_embedded_db="false"
  force_load_jdbc_driver="false"
  db_user="sa"
  db_pwd="OpenAS2"
  db_name="openas2"
  db_directory="%home%/DB"
  jdbc_driver="org.postgresql.Driver"
  jdbc_connect_string="jdbc:postgresql://localhost:5432/$component.db_name$"
  sql_escape_character=""
/>
```

The user name and password can be changed using either a JDBC connection or the command line tool as described below. It is recommended that a readonly user is added for reading data from the database.

To connect to the H2 database whilst OpenAS2 is running use this JDBC connect string:

```
jdbc:h2:tcp://localhost:9092/openas2
```

To query the database from the command line, you must have OpenAS2 running then use this command:

```
java -cp [path to OpenAS2 install]/lib/h2-1.4.192.jar org.h2.tools.Shell -user sa -password OpenAS2 -url
jdbc:h2:tcp://localhost:9092/openas2
```

There is a file named db_ddl.sql file located in the config folder that can be used to create the necessary table structure if your DB becomes corrupted. The simplest way to recreate the database

table is using this command whilst OpenAS2 is running:

```
java -cp [path to OpenAS2 install]/lib/h2-1.4.192.jar org.h2.tools.RunScript -user sa -password OpenAS2 -url jdbc:h2:tcp://localhost:9092/openas2 -script [path to OpenAS2 install]/config/db_ddl.sql
```

The above is for the version of H2 deployed with OpenAS2 version 2.1.0. If you use a different version of H2 then change the jar name to reflect this.

NOTE: The version of H2 deployed with the application only works in Java 7 or higher. Download the older version of H2 that was compiled with support for Java 1.6 if you wish to use Java 6: <https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/h2database/h2-2014-01-18.zip> (Replace the jar in the OpenAS2 lib folder with that version and change the startup script to include the replaced version of H2, delete the files in <installDir>/config/DB, restart OpenAS2 server and recreate the database using the command referenced above).

See appendixes for information on creating external database DDL statements and updating the existing database if the schema is changed in a new release.

5.2. Overriding Certificate Store Password

The certificate store password is stored as an XML attribute “password” on the <certificates> element. This can be overridden using the system property “**org.openas2.cert.Password**”. For improved security, it may not be desired to store the password in the XML file.

This can be passed into the application by adding the following to the java command:

- **-Dorg.openas2.cert.Password=myCertificateStorePassword**

This can be set by using an additional parameter to the batch script file so that it can be set as part of invoking the script. The UNIX shell script will support the password as a parameter. The Windows bat file will need to be enhanced.

5.3. Resend Retry Configuration

When failures occur transferring a message to a trading partner, the system will automatically try to resend the message. By default the system will retry indefinitely.

Restricting the retry attempts can be done at the processor level (applies to all partnerships configured on the server) and at the partnership level. Partnership configuration will override processor settings.

To define the processor level retry count, set the “**resend_max_retries**” attribute on the processor element to a valid integer.

Example snippet:

```
<processor classname="org.openas2.processor.DefaultProcessor"
pendingMDN="%home%/../data/pendingMDN3"
pendingMDNinfo="%home%/../data/pendinginfoMDN3"
resend_max_retries="10" >
```

To define the partnership level retry count, set an attribute element on the partnership with **name**

attribute value as “**resend_max_retries**” and a **value** attribute element to a valid integer.

Example snippet:

```
<partnership name="OpenAS2A-to-OpenAS2B">  
  <attribute name="resend_max_retries" value="3"/>  
  <sender name="OpenAS2A"/>
```

5.4. File Name Parsing

The name of the file passed into the OpenAS2 application for sending to a remote partner can be used to provide information to the AS2 handler that can be used to affect various aspects of how the file is handled.

When the file is picked up for processing by the directory poller, it will look for an attribute named “**format**” on the AS2DirectoryPollingModule component for that directory in the config.xml file. This attribute is used to break the actual file name into multiple parts and the values assigned to the relevant objects defined in the “**format**” attribute.

An example format in the config.xml is:

```
format="sender.as2_id, receiver.as2_id, attributes.filename"
```

The above format will set the AS2 sender and receiver ID as well as the name of the file sent in the AS2 message if configured to send a file name by tokenizing the file name using delimiters defined in the “**delimiter**” attribute. The delimiters for tokenizing defaults to “-.” so the actual name of the file as picked up from the file system will be parsed and split into tokens using either a dash (-) or a period (.) and therefore using the above format, the name of the actual file would have to be in the format XXX-YYY-ZZZ or XXX.YYY.ZZZ or any combination of dash or period and then the AS2 sender would be set to XXX, AS2 receiver to YYY and the name of the file as ZZZ. Any extra string tokens will be discarded so for instance a file name of “X-Y-Z.edi” parsed against the format string above would simply discard the “.edi” part of the file name. If you want the file name sent to the remote partner to be Z.edi then the delimiter attribute value would just be “-”.

The file name can also be configured to be parsed on a per partnership basis if a partner requires a different file name format to be sent or custom headers added to the AS2 message using partnership attributes as defined in section 6.7.2 Dynamic Header Values From File Name.

6. Partner Configuration

The file named partnerships.xml configures all the information relating to the partners you will be exchanging data with. See the appendix for information on the structure of this file.

It is important to keep in mind that the word **partner** refers to any entity specified as a recipient or sender of AS2 messages and includes your own company that you might be configuring the application for.

Each partner will require the following entries in the file:

- a **<partner>** element – key information defining the partner

- a **<partnership>** element - key information for defining a partnership between 2 partners
Separate **<partnership>** elements are required for inbound and outbound data for a specific partner pairing.
NOTE:It is necessary to have 2 elements even if data transfer is unidirectional.

6.1. Partner Definition

The **<partner>** element requires 3 attributes to enable AS2 partner identification:

1. partner name – this is the key to connect partnerships to a partner definition
2. AS2 identifier – this is the key for identifying the target/source partner and is included in AS2 message headers to allow the receiving partner to identify the source of the message and verify the target partner for the AS2 message. It is also used by the general directory polling module to look up the partner names and hence the partnership definition where the as2_id of the sender and receiver are part of the transferred file name.
3. X.509 certificate alias – identifies the alis of the certificates for this partner in the keystore. The encryption and decryption of messages requires the partners public or private key as appropriate

6.2. Partnership Definition

The **<partnership>** element identifies a **specific direction** of AS2 message transfer **from** one partner **to** another. The “name” attribute on the **<partnership>** element is not important but should be used to clearly identify the intended use of the partnership definition. It is suggested the name value uses the names of the source and destination partners something like xxx-to-yyy.

The **<partnership>** element encapsulates a number of child elements that are necessary to properly configure a partnership:

- **<sender name=”xxx”>** - identifies the sending partner definition such that xxx must match the “name” attribute of a **<partner>** element
- **<receiver name=”yyy”>** - identifies the receiving partner definition such that yyy must match the “name” attribute of a **<partner>** element
- **<as2_url>** - a fully qualified URI that provides the connection string to the remote partner for sending AS2 messages. If sending to another OpenAS2 server then the port number must match the value configured in the config.xml file of the remote OpenAS2 server.
- **<as2_mdn_to>** - necessary if an MDN response is required and can be any random string but is most commonly configured with an email address

6.3. Configuring the AS2 Message ID

The message ID used for uniquely identifying the message sent to a partner defaults to the following format:

OPENAS2-\$date.ddMMyyyyHHmmssZ\$-\$rand.UUID\$@\$msg.sender.as2_id\$_\$msg.receiver.as2_id\$

To change this globally for all partnership definitions, change the property in the config.xml file to

the desired format string using the attribute name “**as2_message_id_format**” in the “**properties**” element.

The message Id that is generated can be overridden on a partnership by partnership basis. To set it for a particular partnership, add an attribute named "messageid" to the partnership definition and use any dynamic parameters as specified in the dynamic parameters section of this document.

Something like this:

```
<partnership name="OpenAS2B-to-OpenAS2A">
  <sender name="OpenAS2B"/>
  <receiver name="OpenAS2A"/>
  <attribute name="protocol" value="as2"/>
  <attribute name="content_transfer_encoding" value="binary"/>
  <attribute name="messageid" value="ACME-$date.yyyyMMddHHmmssZ$-$rand.UUID$"/>
```

6.4. Transfer Encoding

As of version 1.3.7, the default content transfer encoding uses “**binary**” if not explicitly overwritten in the configuration. The default can be changed using the “**content_transfer_encoding**” attribute in the partnership.xml file. If you experience issues with failing to verify a partners AS2 inbound message because the message contains CR/LF data in it then you should switch to using “binary” for the transfer encoding. The sample partnership file sets the transfer encoding to “binary” for both partners.

6.5. Supported Encoding Algorithms

The currently supported encoding algorithms are:

- MD5
- SHA1
- SHA224
- SHA256
- SHA384
- SHA512
- CAST5
- 3DES
- IDEA
- RC2_CBC
- AES128 (CBC mode)
- AES192 (CBC mode)
- AES256 (CBC mode)
- AES256_WRAP

6.6. Message Compression

The application supports inbound compression automatically. There is no configuration for this option. To enable outbound compression requires setting “**compression_type**” attribute on the partnership definition for the outbound configuration. The only supported compression/decompression at this time is “**ZLIB**”. The default is no compression of sent messages.

By default compression will occur on the message body part prior to signing. The compression can be configured to occur after signing using the “**compression_mode**” attribute on the partnership definition for the outbound configuration. Set the attribute to “**compress-after-signing**” to enable this.

See partnership.xml appendix for configuration details.

6.7. Custom Mime Headers

Mime headers can be added to the outermost Mime body part for outbound messages and additionally added to the HTTP headers. The outermost Mime body part will depend on configuration of the partnership and could be the compressed, signed or encrypted part. In the case of the encrypted part being the outermost mime body part, the HTTP headers will not be visible until after decryption of the body part since encryption protects the content and the headers.

6.7.1. Static Header Values

Custom headers can be added as statically defined name/value pairs in a partnership attribute where the name and the value are separated by a colon. Multiple static headers are added using a semi-colon separated list between each name/value pair. The attribute name for this is “**custom_mime_headers**” and a sample entry of 2 static headers is shown below:

```
<attribute name="custom_mime_headers" value="X-CustomRoute: X1Z34Y ; X-CustomShape:oblong"/>
```

Note that spaces before or after the “;” and “:” separators will be excluded.

6.7.2. Dynamic Header Values From File Name

Dynamic headers require 2 attributes to configure their behaviour and there are 2 different modes of operation for extracting the value(s) for the defined header(s) from the file name:

1. delimiter mode
2. regular expression mode

Delimiter mode is relatively simple and does not require any special knowledge but regular expression mode may require someone with regular expression skills. Regular expression mode provides far greater flexibility for extracting the value(s) from a file name where specific character sequences or character counts are required.

Both modes use an attribute named “**custom_mime_header_names_from_filename**” to enter the list of header names but the format for the two are slightly different. The second attribute required has a different name for each of the modes,

“**custom_mime_header_name_delimiters_in_filename**” for delimiter mode and
“**custom_mime_header_names_regex_on_filename**” for regular expression mode.

IMPORTANT: if both delimiter mode and regular expression mode attributes are entered into a partnership then delimiter mode will be chosen irrespective.

Delimiter Mode

In delimiter mode, the values in the file name are separated by specifying one or more delimiters and the entire file name is parsed into a list of values using the delimiter(s)

defined. In order to accommodate file names that have more than just the values required for the custom headers, the list of header names are defined with a prefix that designates if the value in the list will be used as a header value or not. For an entry to be added as a header it must have the prefix “header.”. Any other prefix will cause that entry to be ignored. There must be as many header names defined as there are string sequences that would result from splitting the file name string by the delimiter(s) otherwise the system will throw an error.

Below is an example of a delimiter based configuration.

```
<attribute name="custom_mime_header_names_from_filename"
           value="header.X-Header1,header.Y-Header2, junk.extraStuff"/>
<attribute name="custom_mime_header_name_delimiters_in_filename" value="-_"/>
```

Using this configuration, given a file name **ABC-123-INVOICES.csv** there would be 2 headers added as:

X-Header1 value ABC

Y-Header2 value 123

If the file name was **ABC-123-H4FT_INVOICES.csv** the system would throw an error as there would be 4 string sequences extracted so you could fix this by appending junk.moreStuff to the “custom_mime_headers_from_filename” attribute.

Another example of delimiter mode in the partnership:

```
<attribute name="custom_mime_header_names_from_filename"
           value="header.X-Header1, other.string1,header.Y-Header2"/>
<attribute name="custom_mime_header_name_delimiters_in_filename" value="-"/>
```

Using this configuration, given a file name **ABC-123_TEST-INVOICES.csv** there would be 2 headers added as:

X-Header1 value ABC

Y-Header2 value INVOICES

Regular Expression Mode

Regular expression based mode uses Java regular expressions and requires that the regular expression is constructed in grouping mode where the number of groups in the regular expression exactly matches the number of header names in the “custom_mime_header_names_from_filename” attribute. The regular expression will be used to parse the file name to extract the values for the defined names in the attribute named “custom_mime_header_names_regex_on_filename”. Regular expressions can become extremely complex and this document will show some simple examples but there are many sites that provide regular expression tutorials if you need a complicated solution.

An example for a regular expression mode configuration is shown below:

```
<attribute name="custom_mime_header_names_from_filename" value="X-Header1,Y-Header2"/>
<attribute name="custom_mime_header_names_regex_on_filename" value="([^-]*)-([^.]*).csv"/>
```

Using this configuration, given a file name **ABC-123-INVOICES.csv** there would be 2 headers added as:

X-Header1 value ABC

Y-Header2 value 123-INVOICES

If the file name was **ABC-123-H4FT_INVOICES.csv** there would be 2 headers added as:

X-Header1 value ABC

Y-Header2 value 123—HFT_INVOICES

If the file name was **ABC-123-H4FT_INVOICES.txt** or **ABC_123.csv** the system would throw an error since there would be no match.

Another example for a regular expression mode configuration is shown below:

```
<attribute name="custom_mime_header_names_from_filename" value="X-Header1,Y-Header2"/>
<attribute name="custom_mime_header_names_regex_on_filename" value="([^-]*)-([^.]*).csv"/>
```

Using this configuration, given a file name **ABC-123-INVOICES.csv** there would be 2 headers added as:
X-Header1 value ABC
Y-Header2 value 123-INVOICES

6.7.3. Adding Custom Headers To HTTP

The following attribute set to value of “true” will additionally add the headers to the HTTP headers for both static and dynamic header mechanisms:

```
<attribute name="add_custom_mime_headers_to_http" value="true"/>
```

6.8. Setting Dynamic Attributes From File Name

Partnership attributes can be added to the partnership definition based on parsing the file name of the document to be sent using a regular expression. Dynamic attributes require 2 partnership attributes to configure their behaviour for extracting the value(s) for the defined attribute(s) from the file name.

1. “**attribute_names_from_filename**” - when added to a partnership it must contain a list of comma separated attribute names
2. “**attribute_names_regex_on_filename**” - defines the regular expression

The extracted name/value pairs can then be referenced in config using the format:
\$attributes.<attribute name>\$

Regular expressions uses Java regular expressions and requires that the regular expression is constructed in grouping mode where the number of groups in the regular expression exactly matches the number of attribute names in the “**attribute_names_from_filename**” attribute. Regular expressions can become extremely complex and this document will show some simple examples but there are many sites that provide regular expression tutorials if you need a complicated solution.

An example for a regular expression mode configuration is shown below:

```
<attribute name="attribute_names_from_filename" value="X-attribute1,Y-attribute2"/>  
<attribute name="attribute_names_regex_on_filename" value="([^-]*)-([^.]*).csv"/>
```

Using this configuration, given a file name **ABC-123-INVOICES.csv** there would be 2 attributes added as:

X-attribute1 value ABC
Y-attribute2 value 123-INVOICES

If the file name was **ABC-123-H4FT_INVOICES.csv** there would be 2 attributes added as:

X-attribute1 value ABC
Y-attribute2 value 123—HFT_INVOICES

If the file name was **ABC-123-H4FT_INVOICES.txt** or **ABC_123.csv** the system would throw an error since there would be no match.

Another example for a regular expression mode configuration is shown below:

```
<attribute name="attribute_names_from_filename" value="X-attribute1,Y-attribute2"/>  
<attribute name="attribute_names_regex_on_filename" value="([^-]*)-([^.]*).csv"/>
```

Using this configuration, given a file name **ABC-123-INVOICES.csv** there would be 2 attributes added as:

X-attribute1 value ABC

Y-attribute2 value 123-INVOICES

The above attributes could be referenced in config to set a more dynamic subject using something like this:

```
<attribute name="subject" value="Target product: $attributes.X-attribute1$ Sequence Count: $attributes.Y-attribute2$"/>
```

This would produce a subject looking like this:

Target product: ABC Sequence Count: 123-INVOICES

7. Certificate Configuration

NOTE: SHA1 certificates are no longer supported and are rapidly being phased out so you should use SHA256 for all partners that do support SHA256 certificates.

7.1. Creating And Importing

The certificate store used by default is a PKCS12 key store and stores all X.509 certificates for all trading partners. The location and name of the certificate keystore is defined in “**filename**” attribute of the “**certificates**” element in the config.xml file. The default deployment uses the file **<installDir>/config/as2_certs.p12**

The key store must contain the private key of your own X.509 certificate and the public key for each of your trading partners X.509 certificates.

The certificates must be stored with the matching alias as specified in the partner definition of each partner in the partnership.xml file.

There is a shell file to help generating certificates: **bin/gen_p12_key_par.sh**

An excellent open source visual keystore manager that will run on any OS and will allow importing and managing certificates in your keystore can be found here: <http://portecle.sourceforge.net/>

The following steps will create an X509 self signed certificate using OpenSSL:

```
openssl req -x509 -newkey rsa:4096 -keyout priv.key -out selfcert.crt -days 3650 -sha256
```

The generated certificate (**selfcert.crt** in the above command) can then be imported into the PKCS12 keystore using a command like this in the OpenAS2 command mode that is the default when starting openas2 from the command line or via the OpenAS2 remote app:

```
cert import <alias> <path+filename>
```

To create the public key for sending to the partner you can use this:

```
openssl x509 -pubkey -noout -in selfcert.crt > pubkey.cer
```

The file containing the public key will be **pubkey.cer**

If you wish to import the public and private key then you create the PKCS12 key store from the certificates:

```
openssl pkcs12 -export -in selfcert.crt -inkey priv.key -out certs.p12 -name my_new_partner_alias
```

The PKCS12 keystore now contains both public and private keys and can be imported into the keystore via the command interface or simply by replacing the existing keystore with the new one and setting the appropriate attributes in the config.xml file. It is important to use the “.p12” extension when importing certificates from a PKCS12 keystore as the importer requires the “.p12”

extension to detect that you are not importing a certificate directly but rather the certificates in a PKCS12 keystore.

The OpenAS2 command processor (or remote OpenAS2 app) import command for a PKCS12 keystore would be in this format:

```
cert import <alias> <path+filename> <keystore password>
```

7.2. Supporting Multiple Private Certificates

In the case where you need to support multiple certificates such as when one partner needs SHA1 and another needs SHA256 or when you want to set up different certificates per partner, follow these steps below.

The key to supporting multiple certificates is ensuring you use a separate **as2_id** and **x509_alias** attribute.

In the partnership.xml you would add another partner element pointing to a different certificate.

If for example you have a <partner> element definition for your company as below:

```
<partner name="MyCompany" as2_id="MyCompany_OID" x509_alias="MyCompanyCert" email="me@MyCompany.com"/>
```

For each additional certificate you support, you then add another <partner> element. If for instance you have SHA1 already deployed and working with existing partners and you create a SHA256 certificate to support a new partner, you add a new <partner> element something like this:

```
<partner name="MyCompany256" as2_id="MyCompany2_OID" x509_alias="MyCompanyCert256" email="me@MyCompany.com"/>
```

In your partnership definition for the partners using the SHA256 certificate you set the "**sender**" and "**receiver**" attribute as appropriate to point to the correct partner definition ("**MyCompany256**" per the example above) along with changing the SHA1 to SHA256 in the other relevant attributes as shown in the snippet below.

```
<partnership name="MyCompany256-to-MyPartner256">
  <sender name="MyCompany256"/>
  <receiver name="MyPartner256"/>
  <attribute name="protocol" value="as2"/>
  ...
</partnership>
```

Import the new certificate into the existing p12 keystore using the **alias** as defined in the **x509_alias** attribute above ("**MyCompany2Cert256**") and send the partner the matching public key for the new certificate along with the as2_id "**MyCompany256_OID**" that they will need to use so you can differentiate your target definition in the partnership file containing the SHA1 certificate from the SHA256 certificate. See the previous section for importing certificates into your existing keystore.

8. Logging System

Logging supports 6 levels that can be controlled by configuration. The logging output can be

directed to multiple destinations including:

- System console
- Local log files
- Email – log messages are emailed to a configured email address.
- Socket – log messages are written to a socket supporting remote logging

All log classes can be overridden or custom logger classes can be coded and included via configuration

8.1. Log Level Configuration

The logging system supports the use of either or both the ***commons-logging.properties*** file or a file named ***openas2log.properties*** to control the logging level. Properties in *openas2log.properties* will override *commons-logging.properties* entries. There is a *commons-logging.properties* file in the ***bin*** directory which is part of the classpath specified in the script file described in the section on running the application.

The properties in the ***openas2log.properties*** file should be prefixed by “***org.openas2.logging.***”

The following are the logging levels supported by the application in order of lowest(finest) to highest:

"TRACE", "DEBUG", "INFO", "WARN", "ERROR", "FATAL"

The logging levels are turned off by specifying the level you want on and all other levels higher than that level will also be turned on.

The default level is INFO and therefore WARN, ERROR and FATAL are also turned on by default. By adding a property level=DEBUG in the *common-logging.properties* file will result in DEBUG logging being enabled along with INFO, WARN, ERROR and FATAL

The same can be achieved by adding *org.openas2.logging.openas2log.level=DEBUG* in the *openas2log.properties* file.

8.2. Email Logging Configuration

The email logger uses the javax mail API to send ERROR level log messages. Some of the basic email configuration parameters are supported via config in the *config.properties* file as indicated in the appendix. The rest of the mail properties as listed in the Javamail API can be set by passing them as system properties on the command line by modifying the *start-openas2.sh* or *start-openas2.bat* file as appropriate or using the ***javax.mail.properties.file*** attribute on the email logger element.

The configuration values can overwrite each other depending on the source of the configuration value. The order of priority is as follows:

1. values set in the logger element attributes
2. entries in the file identified by ***javax.mail.properties.file***
3. entries using system properties

For example, to pass the port for connection you could add this to the command line:
-Dmail.smtp.port=529

To point to a properties file containing all the relevant information you would add something like this:

```
<logger classname="org.openas2.logging.EmailLogger"
        javax.mail.properties.file="%home%/java.mail.properties"
        from="openas2"
        ...
```

9. MDN Configuration

MDN's can be sent synchronously or asynchronously. By default the system will use synchronous MDN mechanism. Per the AS2 specification, an MDN will only be sent on receipt of an AS2 message if the “**Disposition-Notification-To**” header is present in the received message with a non-empty value. Although this value is specified to be configured with an email address, it is not utilized for any purpose in the AS2 protocol other than to indicate an MDN is required so can in fact be any random string. To set the “**Disposition-Notification-To**” header in an outbound message, the “**as2_mdn_to**” attribute must be set on the partnership.

The other attribute that must be set is the “**as2_mdn_options**”. This defines the encryption algorithm and other MDN settings as specified by the AS2 protocol and the value entered for this attribute will be sent in the “**Disposition-Notification-Options**” header of the AS2 message. Generally changing the encryption algorithm to suit the trading partner should be sufficient on this attribute.

9.1. Asynchronous MDN Receiver Configuration

In order to specify an asynchronous MDN response from a partner requires setting the following attribute on the partnership element in the partnership configuration:

- **as2_receipt_option** – set to the URL of the asynchronous MDN receiver to target the asynchronous MDN receiver module configured in the config file (ie. this is the URL that the partner will send the MDN to). The value set in this attribute will be sent in the “**Receipt-Delivery-Option**” header of the AS2 message to the trading partner. For testing using the default config file that comes with the OpenAS2 installation package, set this to: <http://localhost:10081>

Receiving an asynchronous MDN requires the “**AS2MDNReceiverModule**” module. This module declaration requires a port parameter in addition to the class and can be entered as a child member of the processor node in the config file as shown below:

```
<module classname="org.openas2.processor.receiver.AS2MDNReceiverModule" port="10081" />
```

9.2. Asynchronous MDN Sender Configuration

Sending an asynchronous MDN requires the “**AsynchMDNSenderModule**” module. This module declaration does not require any parameters other than the class and can be entered as shown below as a child member of the processor node in the config file:

```
<module classname="org.openas2.processor.sender.AsynchMDNSenderModule" />
```

10. Configuring HTTPS Transport

HTTPS transport using SSL is configured separately for inbound and outbound connectivity.

10.1. Inbound Transfers

Configuration for inbound is in the config.xml file. The requirements for receiving AS2 files using HTTPS are:

- JKS keystore containing the SSL certificate
- an appropriately configured As2ReceiverModule module element

The key attributes that configure HTTPS are:

- `protocol="https"`
- `ssl_keystore="%home%/ssl_certs.jks"` – points to the JKS certificate keystore
- `ssl_keystore_password="passwordforkeystorefile"`
- `ssl_protocol="TLS"`

See the appendix for details on the attributes.

10.2. Outbound Transfers

The partnership definition for the connection URL will also have to be set to the appropriate host name.

The key attributes that configure HTTPS are:

- `as2_url`
- `as2_mdn_to` (only if MDN is required)

If asynchronous MDN is in use and requires HTTPS then a **As2MDNReceiverModule** module needs to be configured in the same way as for the As2ReceiverModule class above.

If the target system being connected to uses self signed certificates, the following system property will have to be passed to the application in the java command line with a comma separated list (no spaces before or after comma) of the “Common Name” (CN) in the self signed certificate that will be returned by the target system:

```
-Dorg.openas2.cert.TrustSelfSignedCN=<Common.Name1>,<Common.Name2>,...
```

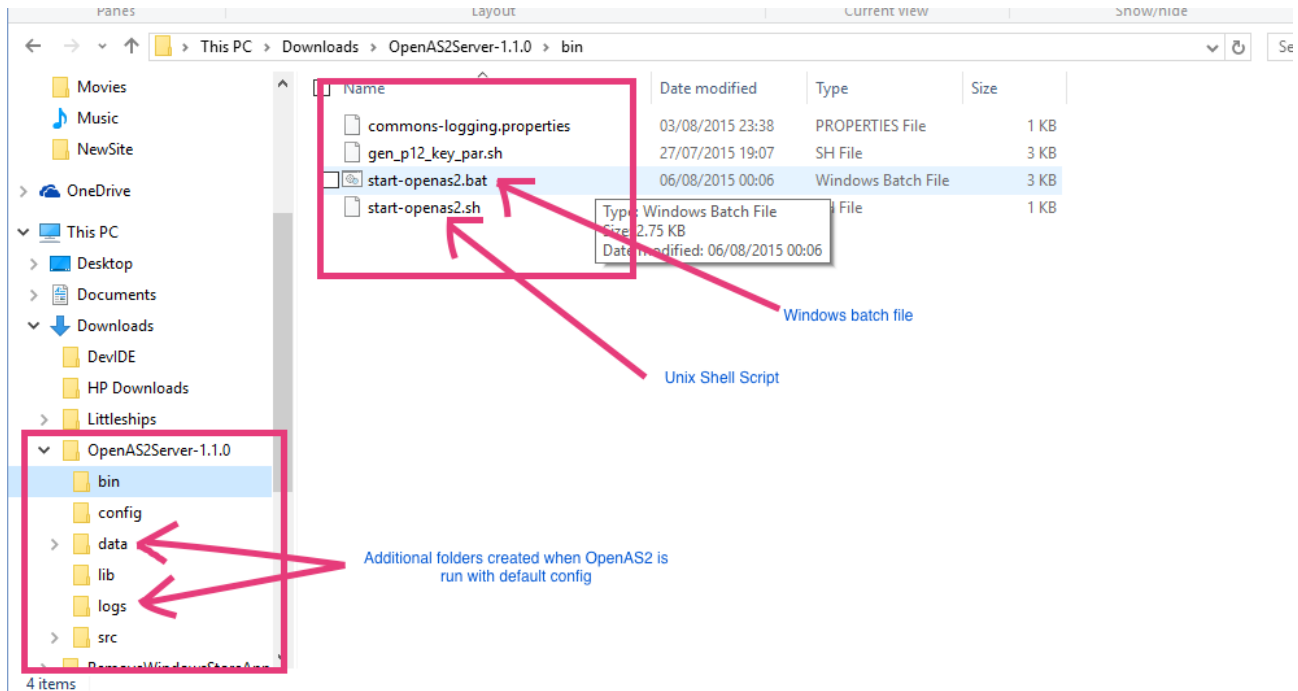
11. Running OpenAS2

OpenAS2 can be started from the command line in any operating system that supports Java or can be configured to run as a daemon using the appropriate mechanisms for the operating system.

The default deployment for OpenAS2 has a console logger enabled which means that all logging will be visible in the command line window that OpenAS2 is started from. The server can also be configured from the command line once the application is running by simply typing in commands once it has started. Because the logging will appear in the window it may make command entry difficult if there are active transfers at the time you try to enter commands and it may be desirable to switch off the console logger if you have no need for it.

11.1. Starting OpenAS2

The default install of the application is as in the figure below from a windows PC.



There are 2 executable script files in the **bin** folder of the AS2 application root as indicated in the screenshot above:

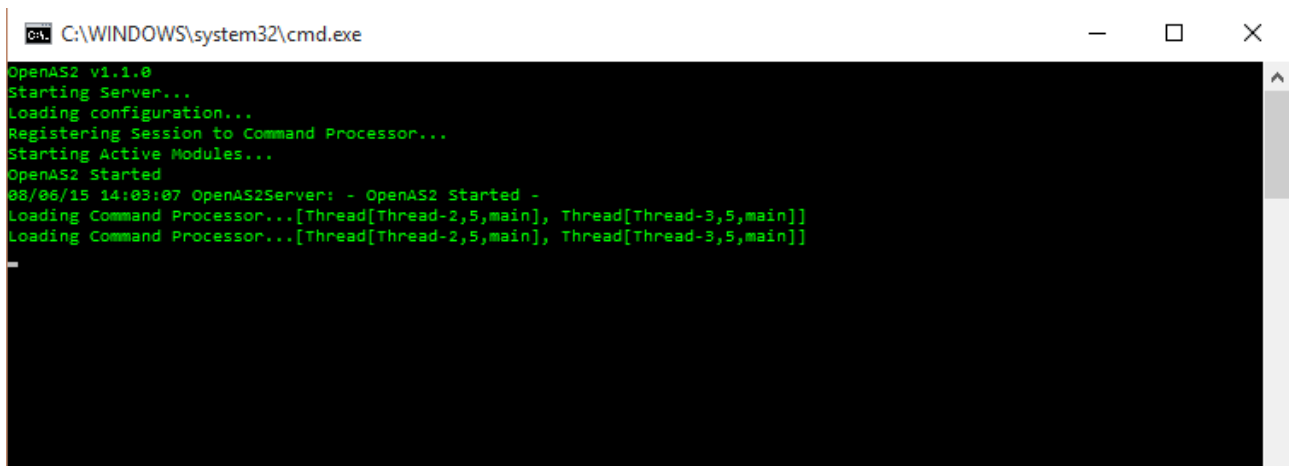
1. start-openas2.sh – for UNIX based systems
2. start-openas2.bat – for Microsoft Windows based system

It is not necessary to modify these files for the default install to work. If you choose to put the config.xml file in a different location than the default then you will need to edit the appropriate script file and set the path to the config.xml file appropriately.

Simply execute the script file and an AS2 server will start up. It will create the following folders along with sub folders when it starts assuming no change to the default config:

- logs – contains the norml program logging
- data – contains all the transferred files and any AS2 specific headers associated with AS2 transfers. This folder will have a number of sub folders for outbound and inbound files for different partners

In Microsoft Windows you should be able to double click the start-openas2.bat file and a command window will open as below.

A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The window has standard Windows window controls (minimize, maximize, close) in the top right corner. The command prompt shows the following output in green text on a black background:

```
OpenAS2 v1.1.0
Starting Server...
Loading configuration...
Registering Session to Command Processor...
Starting Active Modules...
OpenAS2 Started
08/06/15 14:03:07 OpenAS2Server: - OpenAS2 Started -
Loading Command Processor...[Thread[Thread-2,5,main], Thread[Thread-3,5,main]]
Loading Command Processor...[Thread[Thread-2,5,main], Thread[Thread-3,5,main]]
```

For Unix based systems such as Linux and OSX, open a terminal window and change directory to the “bin” folder of the install. The start_openas2.sh file should have execute permissions in which case simply type the name and press enter. If no execute permissions are set, either set the execute permission as needed or use “sh” to run the script:

```
/opt/OpenAS2:>sh opensas2.sh
```

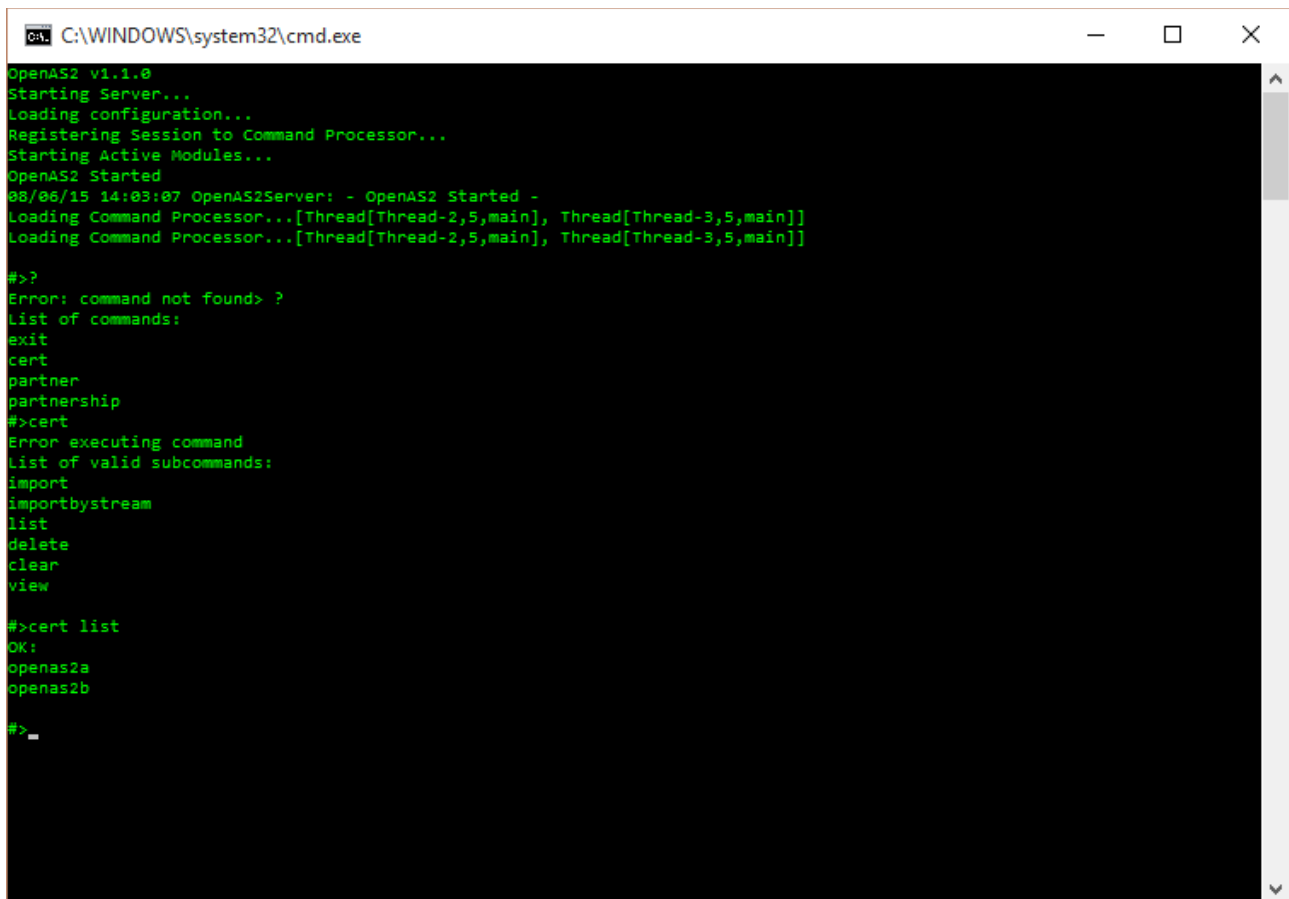
The output in a Unix based system will be identical to that in a Windows based system.

11.2. Command Entry

After startup of the OpenAS2 application, no command prompt is shown in the command line window initially but you can enter a command or just press <ENTER> to get a visible prompt. Typing ? Will show possible commands. Each command will list sub commands they require if you try to enter them without the appropriate parameters.

A screenshot showing command entry is shown below.

Command Entry



```
C:\WINDOWS\system32\cmd.exe
OpenAS2 v1.1.0
Starting Server...
Loading configuration...
Registering Session to Command Processor...
Starting Active Modules...
OpenAS2 Started
08/06/15 14:03:07 OpenAS2Server: - OpenAS2 Started -
Loading Command Processor...[Thread[Thread-2,5,main], Thread[Thread-3,5,main]]
Loading Command Processor...[Thread[Thread-2,5,main], Thread[Thread-3,5,main]]

#>?
Error: command not found> ?
List of commands:
exit
cert
partner
partnership
#>cert
Error executing command
List of valid subcommands:
import
importbystream
list
delete
clear
view
#>cert list
OK:
openas2a
openas2b
#>_
```

11.3. Automated Launching As UNIX Daemon

Although the application will launch as a daemon without any change to the default config, it is recommended that the following configuration changes are made to reduce unnecessary processing by modules that are redundant in this mode and filling the system logs with unwanted logging:

1. Remove the console logger – remove the element in the <loggers> element as shown below
<logger classname="org.openas2.logging.ConsoleLogger"/>
2. Remove the stream command processor in the <commandProcessors> element as shown below
<commandProcessor classname="org.openas2.cmd.processor.StreamCommandProcessor"/>

11.3.1. INIT.D Service

A sample “openas2.d” is provided in the bin directory of the install package. It provides support for starting and stopping the OpenAS2 application as a daemon using the init.d mechanism. Use the appropriate tool for the NIX operating system you are using to install the script in the /etc/init.d folder and create the soft links to launch the OpenAS2 application when the system starts.

First modify the **openas2.d** file to reflect the path where you have installed OpenAS2 then follow one of the options below.

On Redhat based systems as root:

```
$ cp <srcDir>/bin/openas2.d /etc/init.d/  
$ chkconfig --add openas2.d  
$ chkconfig --level 2345 openas2.d on
```

On Debian/Ubuntu based systems as root:

```
$ cp <srcDir>/bin/openas2.d /etc/init.d/  
$ chmod 750 /etc/init.d/openas2.d  
$ update-rc openas2.d defaults
```

11.3.2. SYSTEMD Service

A sample file **openas2.service** is provided in the bin folder of the install package.

First modify the **openas2.d** file to reflect the path where you have installed OpenAS2 then follow the steps below.

```
$ cp <srcDir>/bin/openas2.service /etc/systemd/system/  
$ systemctl daemon-reload  
$ systemctl enable openas2.service
```

Test that it works using the below commands:

```
$ systemctl enable openas2.service  
$ systemctl start openas2.service  
$ systemctl stop openas2.service
```

12. Testing OpenAS2 Transfers

The default configuration of the OpenAS2 configuration is set up for two partners named “OpenAS2A” and “OpenAS2B”. The system will effectively send messages to itself between the 2 configured partners. You can simply start the OpenAS2 server without any changes and then copy a file into the appropriate outbox as defined by the relevant module using the `org.openas2.processor.receiver.AS2DirectoryPollingModule` classes “**outboxdir**” attribute to send the file to the desired partner.

The default configuration provides for 2 partners OPENAS2A and OPENAS2B and will create outbox folders `<installDir>/data/toOpenAS2A` and `<installDir>/data/toOpenAS2B` for explicitly targeting a partner for any file dropped in one of those folders.

If you wish to run 2 OpenAS2 servers on the same machine then the ports on the 2nd instance of OpenAS2 as configured in the config.xml must be different to those configured on the first instance (see Application Configuration above). If using asynchronous MDN, the URL entry for the attribute “**as2_receipt_option**” in the partnerships.xml file for the 2nd instance must match the values configured in the 1st instances config.xml for hist name and port and vice-versa.

12.1. Using HTTPS Transport

To test on a local machine using the supplied sample self signed SSL certificate (config/ssl_certs.jks) you should create a localhost DNS entry. The sample certificate was generated for “www.openas2.localhost”.

This site will help in how to set up a local DNS:

http://www.selfsignedcertificate.com/development_tips.php

The As2ReceiverModule module element should be configured correctly. The key attributes that will work with the supplied sample certificate are already in the sample config file and should just be uncommented:

- `protocol="https"`
- `ssl_keystore="%home%/ssl_certs.jks"`
- `ssl_keystore_password="testas2"`
- `ssl_protocol="TLS"`

The partnership definition for the connection URL will also have to be set to the appropriate host name and use “https” instead of “http”:

```
<attribute name="as2_url" value="https://www.openas2.localhost:10080"/>
```

If asynchronous MDN is used then the as2_receipt_option attribute must be configured for SSL as well:

```
<attribute name="as2_receipt_option" value="https://www.openas2.localhost.com:10081"/>
```

The following system property will have to be passed to the application in the java command line:

```
-Dorg.openas2.cert.TrustSelfSignedCN=www.openas2.localhost
```

If you experience problems with SSL, try adding this to the startup command in the script file:
`-Djavax.net.debug=SSL`

13. Troubleshooting OpenAS2

This section provides some help in identifying issues with AS2 transfers or configuration and execution of the OpenAS2 application. Experience has shown that not all systems properly implement the AS2 specification or have an interpretation of the specification that is different to the OpenAS2 default implementation. To accommodate these differences, the OpenAS2 application has some configuration parameters to change the default behaviour on a per partnership basis that may help to accommodate the implementation anomalies for various other AS2 systems.

13.1. Canonicalization For MIC Algorithm

Some systems (including OpenAS2 prior to V1.3.7) do not canonicalize the MimeBodyPart as specified in the RFC when content transfer encoding is not “binary” (the OpenAS2 default is “binary” but can be set to other values using the “**`content_transfer_encoding`**” attribute on the prtnership). This manifests as errors that cause signature authentication failure that may specifically mention a mismatched MIC. To cater for this set the following attribute on the partnership:

```
<attribute name="prevent_canonicalization_for_mic" value="true"/>
```

13.2. Binary Encoding

If using a content transfer encoding algorithm other than “binary” results in authentication failures, try setting the attribute on the partnership:

```
<attribute name="content_transfer_encoding" value="binary"/>
```

13.3. HTTP Restricted Headers

Depending on the version of Java you are running, the HTTP class handling sending AS2 messages over HTTP that is part of the core Java distribution will automatically remove any restricted HTTP headers (see here for a discussion: <http://stackoverflow.com/questions/11147330/httpurlconnection-wont-let-me-set-via-header>).

This should not be a problem for modern AS2 implementations that OpenAS2 communicates with but there are reports that some systems respond with an HTTP 400 error code and reject the message if the “Content-Transfer-Encoding” header that is a restricted header (see section 19.4.5 here: <https://www.w3.org/Protocols/rfc2616/rfc2616-sec19.html>), is not present in the HTTP headers (it is present in the mime body part headers of the AS2 message).

To solve this uncomment the line in the startup script file containing this entry

```
-Dsun.net.http.allowRestrictedHeaders=true
```

IMPORTANT NOTE: This change cannot be made partner specific due to the way it is implemented in Java so all configured partners will then receive restricted HTTP headers so they may fail as a result of this change. Your only way around this is to run separate OpenAS2 instances.

13.4. CMS Algorithm Protection

Some AS2 systems do not support RFC6211.

The partner system will most likely not provide detailed information that this OID is the issue unless you request detailed logging from the partner but will manifest as authentication failures of some sort. Currently known systems that do not support this are IBM Sterling Integrator.

To disable the OID from being sent add this attribute to the partnership (from a security point of view to include it wherever possible as it plugs a security issue in CMS signed messages):

```
<attribute name="remove_cms_algorithm_protection_attr" value="true"/>
```

13.5. SSL Certificate Exceptions

Sometimes a partner uses a certificate that has intermediate providers not registered in your Java security keystore. Generally this will be manifested by an exception something like this:

javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)

at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1917)

at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:301)

at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:295)

at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1369)

In this case you will need to set up a local trusted certificate provider keystore containing the root or chained (intermediate) certificates that are missing.

Steps:

1. Run the class embedded in the OpenAS2 library jar:

```
java -cp <pathToOpenAS2LibFolder>/openas2-server.jar CheckCertificate <host name>[:port] <localKeystoreFile> [passphrase]
```

"<host name>[:port]" should be the same as what you have in the partnerships "as2_url" attribute EXCLUDING the "https://"

"<localKeystoreFile>" is the name you want to give to your local keystore (e.g jssechaincerts)

"[passphrase]" is the password for the keystore - it will default to "changeit" if you do not provide one`

NOTE: If there is no existing keystore you want to add it to then leave out the password otherwise it will throw an error. You can use the keytool utility that comes with java to change the keystore password if you wish but since it does not contain any private keys there is little point in changing the password but if you do then you will have to pass the new password in to the OpenAS2 app using the ***javax.net.ssl.trustStorePassword*** property.

If the class only receives a single certificate as response from the remote host it generally indicates that the root certificate is not trusted and will need installing into a keystore for use by the OpenAS2 application. The output from the class should make it clear it was unable to successfully complete an SSL handshake and it will import the certificate (root or chain as necessary) into the keystore.

2. Add the local cert store to the OpenAS2 startup by adding this to the startup command in the relevant batch file you are using to start OpenAS2:
`-Djavax.net.ssl.trustStore=<pathToKeystore>/<localKeystoreFile>`

NOTE: If you ran the CheckCertificate mechanism a second time but point it at the keystore it created the first time round it should successfully complete the handshake and there will be no messages to say it is missing a certificate.

For example, run it once like this:

```
java -cp openas2-server.jar CheckCertificate as2.xyz.com:98765 jssechaincerts
```

Then run it like this:

```
java -Djavax.net.ssl.trustStore=jssechaincerts -cp openas2-server.jar CheckCertificate as2.xyz.com:98765 jssechaincerts2
```

The second instantiation uses the keystore from the first instantiations output and it should not create a new certificate in keystore "jssechaincerts2"

13.6. Java Versions Prior To 1.6

Prior to java 1.6, the Javabeans Activation Framework is NOT included in the standard Java install. Download the 1.1.1 version and extract from the zip file from this web page:

<http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-java-plat-419418.html#jaf-1.1.1-fcs-oth-JPR> 

The activation.jar must be placed into the “lib” folder of the OpenAS2 server install and added to the class path in the shell or batch file as appropriate.

13.7. Mime Body Part Logging

Sometimes it may be necessary to see what is actually in the mime body parts received from a partner. OpenAS2 provides a mechanism to enable logging of either received message mime body parts or received MDN mime body parts. These are enabled using OpenAS2 startup variables in the startup script in combination with TRACE level logging. Both the DOS and Unix scripts provide these variables but are commented out near the top of the batch file and you can simply uncomment and start the application.

IMPORTANT: this could produce large log files so use sparingly and disable as soon as possible.

The startup variables are:

logRxdMsgMimeBodyParts=true

logRxdMdnMimeBodyParts=true

13.8. TLSv1.2

It appears that although Java7 does support TLSv1.2 it is not enabled by default (refer here: https://blogs.oracle.com/java-platform-group/entry/diagnosing_tls_ssl_and_https)

If you need to use the protocol, add the following to the top of the batch shell script that starts OpenAS2:

Windows: **set EXTRA_PARMS=%EXTRA_PARMS% -Dhttps.protocols=TLSv1.2**

Linux/Unix/OSX: **EXTRA_PARMS=\$EXTRA_PARMS -Dhttps.protocols=TLSv1.2**

14. Partner AS2 Compatibility Settings

The below table provides configuration settings for other AS2 systems that are known to work based on user feedback.

PLEASE FEEL FREE TO PROVIDE SETTINGS FOR ANY SYSTEMS THAT REQUIRE A CHANGE FROM THE DEFAULT PROVIDED WITH THE OPENAS2 INSTALL PACKAGE TO COMMUNICATE WITH OTHER AS2 SYSTEMS.

Where the field is left blank, the setting is unknown and the default that comes with OpenAS2 will probably work.

AS2 System	Allow Restricted Headers (startup script property: sun.net.http.allowRestrictedH eaders)	Prevent Canonicalization For MIC (partner attribute: prevent_cononicalization_for_ mic)	Remove CMS Algorithm Protection (partner attribute: remove_cms_algorithm_ protection_attrib)
IBM Sterling	false		true
IBM Datapower	false		true
Mendelson	false	true	
Seeburger	?	?	?
Oracle Integration B2B	false	false	false

15. Remote Control

By default the OpenAS2 server application will start up a command processor as a socket listener allowing remote connection to the OpenAS2 server to execute commands. The OpenAS2 remote application is part of the application package but is not necessary to use it if you have no remote access requirement and should be disabled in the config.xml file if not using it by removing or commenting out the **<commandProcessor>** element with classname value **org.openas2.cmd.processor.SocketCommandProcessor**

You can set the port that the command processor listens on using the **portId** parameter.

```
<commandProcessor
classname="org.openas2.cmd.processor.SocketCommandProcessor" portId="14321"
userid="userID" password="pWd"/>
```

The remote control application will need to connect to the specified port with the specified user ID and password.

The connection uses an anonymous secure socket cipher and may require changing this if your Java implementation does not support the default cipher which is

TLS_DH_anon_WITH_AES_256_CBC_SHA for the latest release. This cipher is not available in older Java versions and it may be necessary to switch to SSL_DH_anon_WITH_RC4_128_MD5

To switch cipher you will need to start the OpenAS2 server and the remote command client passing the cipher name as a system property using the -D switch that can be added to the batch script that starts the application. The property must be named “**CmdProcessorSocketCipher**”.

e.g java -D**CmdProcessorSocketCipher=SSL_DH_anon_WITH_RC4_128_MD5** ...

16. Dynamic Variables

Variables can be used in configuration files for run time replacement of strings. In the case of headers and attributes the reference can be used to change its value. Some variables are specific to certain processor modules and not supported for all situations where dynamic variables can be used. The variables used in the configuration files are as follows:

\$date.xxx\$ - create date strings in a defined format

where **xxx** is any valid character formatting string defined in `java.text.SimpleDateFormat`

for example: **\$date.YYYY\$** gets the four digit year

\$msg.xxx.yyy\$ - accesses various information contained in the AS2 message.

Typically used by file modules to configure the name of files used to persist the message payload.

The “**xxx**” part can be any one of the following:

- **sender** – accesses the “sender” element of the partnership in use for the current message. “**yyy**” can be any attribute name within the “sender” element
eg. **\$msg.sender.as2_id\$** - retrieves the AS2 ID of the sender of the message
- **receiver** - accesses the “receiver” element of the partnership in use for the current message. “**yyy**” can be any attribute name within the “receiver” element
eg. **\$msg.receiver.as2_id\$** - retrieves the AS2 ID of the receiver of the message
- **attributes** – accesses any attributes on the message. The attribute name is used in place of “**yyy**”
e.g **\$msg.attribute.filename\$** accesses the name of the file contained in the AS2 message
- **headers** - accesses any headers on the message. The header name is used in place of “**yyy**”
e.g **\$msg.headers.content-type\$** accesses the content type header for the AS2 message
- **content-disposition** - used to access any content-disposition attribute in the received message content disposition where the attribute identifier is used in place of “**yyy**”
e.g **\$msg.content-disposition.filename\$** accesses the name of the file received from the partner

\$mdn.zzz\$ for message mdn parameters, used by EmailLogger and MDNFileModule

where **zzz** can be any of the following values:

- **msg** – requires “**zzz**” to be in the form “**xxx.yyy**” and can access data points as defined for **\$msg.xxx.yyy\$** format dynamic variables above
- **sender** – gets the `as2_id` of the sender
- **receiver** – gets the `as2_id` of the receiver
- **text** - gets the text portion of the MDN
- **attributes** – requires “**zzz**” to be in the form “**xxx.yyy**” and can access data points as defined for **\$msg.xxx.yyy\$** format dynamic variables above
- **headers** – requires “**zzz**” to be in the form “**xxx.yyy**” and can access data points as defined for **\$msg.xxx.yyy\$** format dynamic variables above

eg.: **\$mdn.text\$** gets the text portion of the MDN

\$rand.zzz\$ can be used on most strings to produce random strings.

Produces a random UUID or a 0 padded random number of a defined number of digits where **zzz** can be any string of any number of characters

- if “**zzz**” is “**UUID**” or “**uuid**” (e.g **\$rand.UUID\$**) then it produces a random UUID
- for any other string of characters other than UUID, the number of characters in the string determines the number of digits in the random number that is

generated and will be zero padded

e.g \$rand.1234\$ - creates a 4 digit random number between 0000 and 9999

\$rand.ax1fg4c5\$ - creates an 8 digit random number between 00000000 and 99999999

\$exception.xxx\$ -used by EmailLogger

where **xxx** can be any of the following

- name - retrieves name of the exception
- message – retrieves the exception message
- trace – retrieves the trace log for the exception

eg.: **\$exception.trace\$** gets the trace log of the exception

\$component.xxx\$ -used in module configuration

where **xxx** can be any of the attribute names specified above the attribute in the same module element. Can be used to simplify setting hard coded strings into a concatenated string used by the server module. See the DB tracking module definition for an example

17. Appendix: config.xml file structure

- Node: **openas2**
 - Node: **certificates**

Attributes

classname

describes the Java class to process the certificate file.

for example: *org.openas2.cert.PKCS12CertificateFactory*

filename

defines the file name containing the certificates

for example: *%home%/certs.p12*

password

opens the file using this password

for example: *test*

NOTE: this can be overridden using a java system property when starting the application:

-Dorg.openas2.cert.Password=<somePassword>

interval

describes how often the file should be check up for updates. Specified in seconds.

for example: *300*

- Node: **partnerships**

Describes the OpenAS2 classes to handle the trading partner identifications.

Attributes

classname

describes the Java class to process the partnerships file

for example: *org.openas2.partner.XMLPartnershipFactory*
defines the file name containing the partnerships definitions
describes
for example: *%home%/partnerships.xml*

- Node: **loggers**

Describes the OpenAS2 logging classes to use. **You must include -Dorg.apache.commons.logging.Log=org.openas2.logging.Log in your startup call or as a property in the commons-logging.properties file. See <http://commons.apache.org/logging/guide.html#commons-logging-api.jar> for more information.**

Do not use this node when using other logging packages (e.g. log4j) with the OpenAS2 package.

- Node: **logger** (for E-mail logging)

Optional, if not specified no E-mail logging is performed.

Attributes

classname

describes the Java class to process E-mail logging
for example: *org.openas2.logging.EmailLogger*

show (Optional)

describes what level of logging to handle

Possible values

- all = all exceptions (terminated or not) and info
- terminated = all terminated exceptions **Default value**
- exceptions = all non-terminated exceptions

for example: *terminated*

from

defines the source email address

for example: *logger@openas2.org*

from_display

defines the displayed text of the source email address

for example: *Openas2*

to

defines the recipient email address

for example: *your@e-mailaddress.com*

smtpserver

describes the SMTP server to process outgoing e-mail

for example: *mySillyMailerDot.com*

smtpport

defines the SMTP server port to connect to

for example: *587*

smtpauth

defines whether authentication is required for the SMTP server
(Possible values: true, false)

for example: *true*

smtpuser

defines user name if authentication is required for the SMTP

server

smtppwd

defines user password if authentication is required for the SMTP server

subject

describes the e-mail to the receiving party

for example: *\$exception.name\$: \$exception.message\$ (only relevant a specific exceptions type)*

bodytemplate

defines the file that contains the body of the message

for example: *%home%/emailtemplate.txt*

- Node: **logger** (for file logging)

Optional, if not specified no file logging is performed.

Attributes

classname

describes the Java class to log messages

for example: *org.openas2.logging.FileLogger*

filename

defines the name of the output log file.

for example: *%home%/log-\$date.MMddyyyy\$.txt*

show (Optional)

describes what level of logging to handle

Possible values

- all = all exceptions (terminated or not) and info **Default value**
- terminated = all terminated exceptions
- exceptions = all non-terminated exceptions
- info = all info log entries

for example: *terminated*

- Node: **logger** (for Console logging, writes to System.out)

Optional, if not specified no console logging is performed.

Attributes

classname

describes the Java class to log messages

for example: *org.openas2.logging.ConsoleLogger*

show (Optional)

describes what level of logging to handle

Possible values

- all = all exceptions (terminated or not) and info **Default value**
- terminated = all terminated exceptions
- exceptions = all non-terminated exceptions
- info = all info log entries

for example: *info*

- Node: **commands**

Describes the OpenAS2 command classes to use

Attributes

classname

describes the Java class to process the command file

for more information see [Command File](#)

for example: *org.openas2.app.XMLCommandRegistry*

filename

defines the name of the file command all possible commands

for example: *%home%/commands.xml*

- Node: **processor**

Describes the OpenAS2 class to handle the message processors.

Attributes

classname

describes the default Java class to handle outgoing message

for example: *org.openas2.processor.DefaultProcessor*

- Node: **module**

Module that sends out AS2 messages.

Attributes

classname

describes the Java class to send outgoing Messages

for example: *org.openas2.processor.sender.AS2SenderModule*

retry

defines the number of attempts for sending a message, default is -1 aka infinite.

for example *retries="3"* will stop sending the message after 3 failures.

connecttimeout

defines the millisecond count before a connection times out.

default value is 30000 or 30 seconds.

for example *connecttimeout="60000"* will time out after 60 seconds.

readtimeout

defines the millisecond count before a read times out. default value is 30000 or 30 seconds.

for example *readtimeout="60000"* will time out after 60 seconds.

- Node: **module**

Module that sends out AS2 MDNs asynchronously.

Attributes

classname

describes the Java class to send asynch MDN

for example:

org.openas2.processor.sender.AsynchMDNSenderModule

retry

defines the number of attempts for sending a message, default value is -1 (infinite.)

for example *retries="3"* will stop sending the message after 3 failures.

connecttimeout

defines the millisecond count before a connection times out.

default value is 30000 or 30 seconds.

for example *connecttimeout="60000"* will time out after 60 seconds.

readtimeout

defines the millisecond count before a read times out. default value is 30000 or 30 seconds.

for example *readtimeout="60000"* will time out after 60 seconds.

- Node: **module**

The following will describe a module to process outgoing message placed in a generic directory. The module determines the receiver and send from the file name placed in the directory (see [format](#) attribute). This module will look for files in specified directory and file names to send to the default message processor.

Attributes

classname

describes the Java class to process files to be sent to the AS2SenderModule for its delivery process.

for example:

org.openas2.processor.receiver.AS2DirectoryPollingModule

outboxdir

defines the directory where files are to be found.

for example: *%home%/toAny*

fileextensionfilter

defines the extension of the file name if file filtering is required.

The system will prefix the text entered in this attribute with a period and only files matching that extension will be picked up by the polling module

for example: *txt - this will only find files like test.txt but not mytxt*

errordir

defines directory where files containing errors are redirected to.

for example: *%home%/toAny/error*

interval

describes how often the directory is to be checked for work.

Specified in seconds. Default is 30 seconds.

for example: 5

delimiters

defines the characters used to parse the incoming file name.

Characters are separate the tokens: sender, receiver and file id.

for example: -.

format

describes the file name by the tokens sender, receiver and file id. May be in any order. Sender id and receiver id are as defined in the partnership.xml file.

for example: *sender.as2_id, receiver.as2_id, attributes.fileid* or *attributes.mimetype, attributes.mimesubtype, sender.name, receiver.name*

mimetype

describes the outgoing message mime message type.

for example: *application/EDI-X12*

- Node: **module**

Attributes

classname

describes the Java class to process files for a particular trading partner that are sent to the AS2SenderModule for its delivery process.

for example:

org.openas2.processor.receiver.AS2DirectoryPollingModule

outboxdir

defines the directory where outgoing message are defined.

for example: *%home%/toOpenAS2A/*

errordir

defines the directory where erroneous messages are left.

for example: *%home%/toOpenAS2A/error*

interval

describes how often the incoming directory is searched. Defined in seconds, default is 30 seconds.

for example: *5*

defaults

describes the AS2 sender and receiver ids as defined in the partnership.xml file.

for example: *defaults="sender.as2_id=OpenAS2A_OID, receiver.as2_id=OpenAS2B_OID"*

protocol

describes the AS2 protocol, which is AS2.

for example: *as2*

mimetype

describes the outgoing message mime message type.

for example: *application/EDI-X12*

- Node: **module**

Attributes

classname

describes the Java class to process incoming MDNs

for example: *org.openas2.processor.storage.MDNFileModule*

filename

describes

for example: *%home%/mdn/\$date.yyyy\$/\$date.MM\$/*

\$mdn.msg.sender.as2_id\$-\$mdn.msg.receiver.as2_id\$-\$mdn.msg.headers.message-id\$

protocol

describes

for example: *as2*

tempdir

describes

for example: *%home%/temp*

- Node: **module** Defines the module to handle messages.

Attributes

classname

describes the Java class to process and store incoming messages
for example:

org.openas2.processor.storage.MessageFileModule

filename

describes the location and formatted filename of the stored MDNs.

for example: *%home%/inbox/\$msg.sender.as2_id\$-\$msg.receiver.as2_id\$-\$msg.headers.message-id\$*

protocol

describes the AS2 protocol

for example: *as2*

tempdir (Optional)

defines temporary directory used to store MDNs during message processing.

for example: *%home%/temp*

- Node: **module**

Attributes

classname

describes the Java class to process handle incoming transfers
for example:

org.openas2.processor.receiver.AS2ReceiverModule

port

defines the port the server listens on.

for example: *10080*

errordir

defines directory where invalid incoming messages are stored.

for example: *%home%/inbox/error*

errorformat

defines the format of filenames for invalid incoming messages.

for example: *sender.as2_id, receiver.as2_id, headers.message-id*

protocol

optional and defaults to “http” if not present

set to “https” for SSL transport protocol

ssl_protocol

optional and defaults to “TLS” if not present

set to preferred SSL transport protocol

for example: *SSLv3*

ssl_keystore

The name of the file including path containing SSL certificate
only required for “protocol” attribute set to “https”
for example: %home%/ssl_certs.jks

ssl_keystore_password

The password to open the SSL keystore
only required for “protocol” attribute set to “https”
for example: mySecretPassword
*NOTE: this can be overridden using a java system property
when starting the application:*
-Dorg.openas2.sslPassword=<somePassword>

- Node: **module**

Attributes

classname

describes the Java class to send asynchronous MDN response
for example:
org.openas2.processor.receiver.AS2MDNReceiverModule

port

defines the port the server listens on.
for example: 10080

protocol

optional and defaults to “http” if not present
set to “https” for SSL transport protocol

ssl_protocol

optional and defaults to “TLS” if not present
set to preferred SSL transport protocol
for example: SSLv3

ssl_keystore

The name of the file including path containing SSL certificate
only required for “protocol” attribute set to “https”
for example: %home%/ssl_certs.jks

ssl_keystore_password

The password to open the SSL keystore
only required for “protocol” attribute set to “https”
for example: mySecretPassword
*NOTE: this can be overridden using a java system property
when starting the application:*
-Dorg.openas2.sslPassword=<somePassword>

- Node: **module**

Attributes

classname

describes the Java class to rehandle messages
for example:
org.openas2.processor.resender.DirectoryResenderModule

resenddir

defines the directory to find message to resend

for example: *%home%/resend*

erroridir
defines the director to store resend messages that are in error.
for example: *%home%/resend/error*

resenddelay
defines the wait time between resends. Defined in seconds.
Default is 60.
for example: *600*

18. *Appendix: partnership.xml file structure*

This file describes your company and your trading partners. This file requires modification to work with your application

- Node: **partnerships**

The root node.

- Node: **partner**

partner definition

Attributes

name

partner name as defined in OpenAS2 configuration file.

OpenAS2A

as2_id

partner name as defined in partnership node

OpenAS2A

x509_alias

Alias as defined in certificate file

openas2a

email

E-mail address of partner

as2a@MySillyMailerServer.com

- Node: **partnership**

defines partner relationships between sender and receiver

- Node: **partnership**

Attributes

name

Unique name of partnership relation. See filename parsing above.

OpenAS2A-OpenAS2B

- Node: **sender**

Attributes

name

Unique name of Sender

OpenAS2A

- Node: **receiver**

Attributes

name

Unique name of receiver
OpenAS2B

*The following is a list of nodes that use the node name of **attribute**. The subnodes of **attribute** use a name/value node naming pair structure.*

- Node: **attribute**
name is **protocol** defines the protocol to use with this partner.
value is **as2**
name="protocol" value="as2"
- Node: **attribute**
name is **subject** defines text used in E-mail subject line
value
name="subject" value="From OpenAS2A to OpenAS2B"
- Node: **attribute**
name is **as2_url** defines partners AS2 server's URL
value
name="as2_url" value="http://www.MyPartnerAS2Machine.com:10080"/>
- Node: **attribute**
name is **as2_mdn_to** when set this specifies that an MDN response is required and defines value of the "**Disposition-Notification-To**" header in the AS2 message sent to the partner. It is normally an email address but can be any string that is meaningful
value
name="as2_mdn_to" value="datamanager@mypartner.com"
- Node: **attribute**
name is **as2_receipt_option** defines asynchronous MDN server's URL
value
name="as2_receipt_option" value="http://www.MyAS2Machine.com:10081"
- Node: **attribute**
name is **as2_mdn_options** defines MDN option values for E-mail header
value
name="as2_mdn_options" value="signed-receipt-protocol=optional, pkcs7-signature; signed-receipt-micalg=optional, sha1"
- Node: **attribute**
name is **encrypt** defines encrypting algorithm name for E-mail header
value
name="encrypt" value="3des"
- Node: **attribute (optional)**
name is **content_transfer_encoding** defines what the header field should display
value 8bit (default), binary, ...
name="content_transfer_encoding" value="binary"

- Node: **attribute (optional)**
***name** is **compression_type** if defined it determines what the type of compression to use. Leave this attribute out if no compression is required*
value ZLIB (default) – no other supported options
name="compression_type" value="ZLIB"
- Node: **attribute (optional)**
***name** is **compression_mode** if defined it determines when compression occurs. If this attribute is not specified then compression occurs before signing.*
value – “compress-after-signing”
name="compression_mode" value="compress-after-signing"

19. Appendix: command.xml file structure

List of commands available to the OpenAS2 server Application.

- Node: **commands** the root node
 - Node: **multicommand**
 - attribute
 - name
 - value "cert|part", certificate commands or partnership commands
 - description
 - value is some useful text
 - Node: **command**
 - attribute
 - classname
 - value is a OpenAS2 classname that will process a command

20. Appendix: Updating database structure

The table structure for message tracking is stored in an XML file structure that uses the Apache DDLUtils project structure.

OpenAS2 includes a jar file that uses the Apache DDLUtils project to generate DDL statements to create or update the database to match the XML definition of the database and can also be used to automatically update the target database. Configuration for the database update functionality comprises 3 files located in the <installDir>/resources/DB folder:

1. openas2-schema.xml – the XML definition of the table used to capture AS2 message states
2. jdbc.properties.h2 – defines the connection parameters for the databases
3. build.xml – the Ant build file that invokes

Run this command in the directory containing the Ant build file to generate a DDL file containing statements to update the DB to match the XML definition:

```
ant -Djdbc.properties.file=jdbc.properties.h2
```

To directly update the database without generating a DDL file use this command:

```
ant -Djdbc.properties.file=jdbc.properties.h2 writeSchemaToDb
```

21. Appendix: Creating database DDL for external databases

The deployment package for OpenAS2 contains resources to generate DDL statements for the database table used to log AS2 message state. It supports the following database platforms:

- axion
- cloudscape
- db2
- derby
- firebird
- h2
- hsqldb
- interbase
- maxdb
- mckoi
- mssql
- mysql
- oracle
- postgresql
- sapdb
- sybase

To use a different database system than H2, follow these steps:

1. Create a database with the desired name , user and password in the target database system
2. Change the property named “platform” in the build.xml file to the required database platform
3. Set up a jdbc.properties file with the appropriate settings using the jdbc.properties.h2 file as a template.
4. Create the database table. To generate DDL statements to an SQL file that can then be used to apply to the database use this command:

```
ant -Djdbc.properties.file=jdbc.properties
```

To directly update the database without generating a DDL file use this command:

```
ant -Djdbc.properties.file=jdbc.properties writeSchemaToDb
```


5. Change the appropriate parameters in the config.xml file for the database tracking module.