

# OpenAS2 Server Application

## Table of Contents

1. Introduction.....	2
2. Glossary.....	2
3. Installing OpenAS2.....	2
4. Configuration.....	3
4.1. Application Configuration.....	3
4.1.1. Overriding Certificate Store Password.....	4
4.1.2. Resend Retry Configuration.....	4
4.2. Partner Configuration.....	5
4.2.1. Partner Definition.....	5
4.2.2. Partnership Definition.....	6
4.2.3. Transfer Encoding.....	6
4.2.4. Supported Encoding Algorithms.....	6
4.2.5. Message Compression.....	7
4.2.6. Custom Mime Headers.....	7
4.2.6.1. Static Header Values.....	7
4.2.6.2. Dynamic Header Values From File Name.....	7
4.2.6.3. Adding Custom Headers To HTTP.....	9
4.3. Certificate Configuration.....	9
4.4. Logging System.....	9
4.4.1. Log Level Configuration.....	9
4.4.2. Email Logging Configuration.....	10
4.5. MDN Configuration.....	10
4.5.1. Asynchronous MDN Receiver Configuration.....	11
4.5.2. Asynchronous MDN Sender Configuration.....	11
4.6. Configuring HTTPS Transport.....	11
4.6.1. Inbound Transfers.....	11
4.6.2. Outbound Transfers.....	12
5. Running OpenAS2.....	12
6. Testing OpenAS2 Transfers.....	14
6.1. Using HTTPS Transport.....	15
7. Troubleshooting OpenAS2.....	15
7.1. Canonicalization For MIC Algorithm.....	16
7.2. Binary Encoding.....	16
7.3. CMS Algorithm Protection.....	16
7.4. Java Versions Prior To 1.6.....	16
7.5. Mime Body Part Logging.....	16
8. Remote Control.....	17
9. Dynamic Variables.....	17
10. Appendix: config.xml file structure.....	18
11. Appendix: partnership.xml file structure.....	26
12. Appendix: command.xml file structure.....	28

# 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 1.3.7 and up.

## 2. Glossary

EDI – Electronic Data Interchange

MDN - Message Disposition Notification

## 3. Installing OpenAS2

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](#).

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. 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

## 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
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.

### 4.1. 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.

#### 4.1.1. 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.

#### 4.1.2. 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"/>
```

## 4.2. 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 not necessary to have 2 elements if data transfer is unidirectional.

### 4.2.1. 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 alias of the certificates for this partner in the keystore. The encryption and decryption of messages requires the partners public or private key as appropriate

#### 4.2.2. 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

#### 4.2.3. 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.

#### 4.2.4. 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

#### 4.2.5. 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.

#### 4.2.6. 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.

##### 4.2.6.1. 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.

##### 4.2.6.2. Dynamic Header Values From File Name

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

### Regular expression mode

In delimiter mode, the values in the file name are separated by specified 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 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 defines is entered into an 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

#### 4.2.6.3. 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"/>
```

## 4.3. Certificate Configuration

The certificate store used by default is a PKCS12 key store and stores all X.509 certificates.

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 can be found here:

<http://portecle.sourceforge.net/>

## 4.4. 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

### 4.4.1. 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.

#### 4.4.2. 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"
    ...
```

## 4.5. 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.

#### 4.5.1. 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" />
```

#### 4.5.2. 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" />
```

### 4.6. Configuring HTTPS Transport

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

#### 4.6.1. 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.

## 4.6.2. 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)

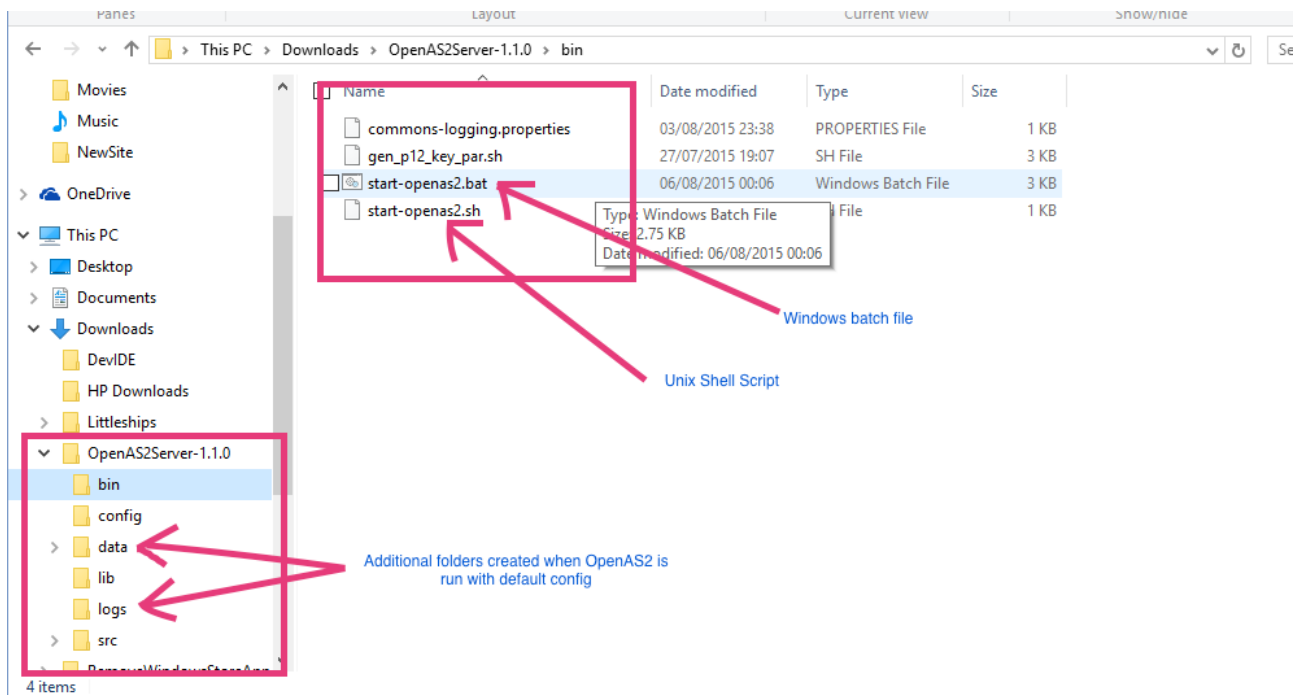
If asynchronous MDN is in use and requires HTTPS then a **As2MDNReceiverModule** module needs to be configured in the same way as for the `As2ReceiverModule` class above.

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>,...
```

## 5. Running 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

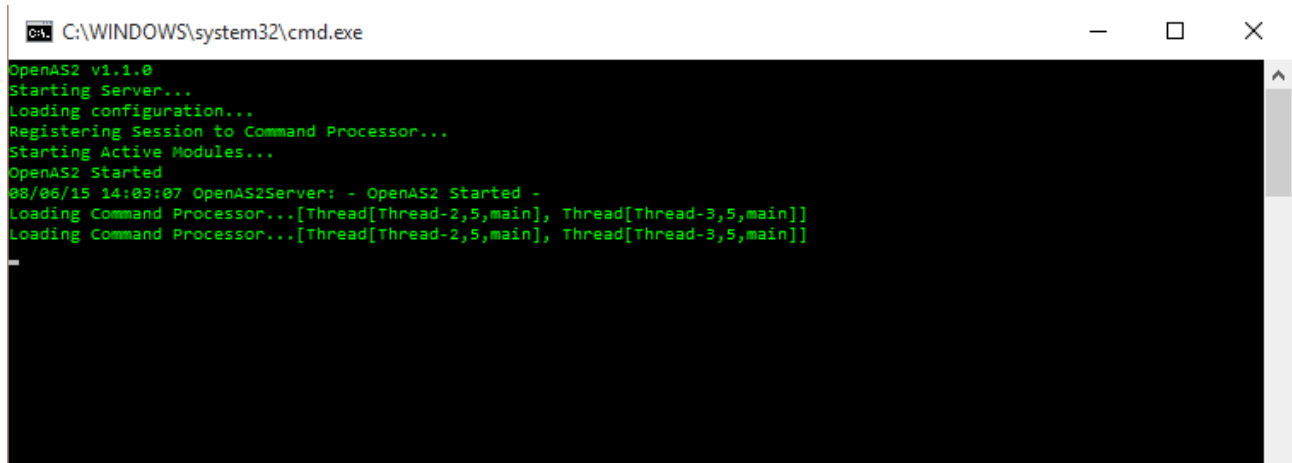
It is not necessary to modify these files for the default install to work. If you choose to put the `config.xml` file in a different location than the default then you will need to edit the appropriate

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.



```
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]]
```

No command prompt is shown 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 sample is shown below.

```
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

#> _
```

There will be some logging as the application starts and it will then provide a command prompt (you may need to press the ENTER key to see it due to logging events).

You can enter commands after startup by typing in the console window.

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.

## 6. 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 2<sup>nd</sup> 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 2<sup>nd</sup> instance must match the values configured in the 1<sup>st</sup> instances config.xml for hist name and port and vice-versa.

## 6.1. 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](http://www.openas2.localhost)”.

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

[http://www.selfsignedcertificate.com/development\\_tips.php](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
```

## 7. 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.

## 7.1. 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"/>
```

## 7.2. 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"/>
```

## 7.3. 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_attrib" value="true"/>
```

## 7.4. 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.

## 7.5. 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 receieved 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

## 8. 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** ...

## 9. Dynamic Variables

Variables can be used in configuration files for real time replacement of strings. Some variables are specific to certain processor modules. The variables used in the configuration files are as follows:

**\$date.xxx\$** ::: for date parameters

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 about the incoming message, used by MessageFileModule. The available options for this format of dynamic variable are:

1. **\$msg.sender.as2\_id\$** - retrieves the AS2 ID of the sender of the message
2. **\$msg.receiver.as2\_id\$** - retrieves the AS2 ID of the receiver of the message
3. **\$msg.attributes.yyy\$** - used to access any attribute on the message where the attribute

identifier is used in place of “yyy”

for example

4. `$msg.headers.yyy$` - used to access any header on the message where the header identifier is used in place of “yyy”
5. `$msg.content-disposition.yyy$` - used to access any content-disposition attribute in the message content disposition where the attribute identifier is used in place of “yyy”

Some attributes commonly found in an AS2 message content disposition include

- filename – the original name of the file that was sent
- 

**`$mdn.zzz$`** for message mdn parameters, used by EmailLogger and MDNFileModule where `zzz` can be any of the following values to get

- 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

for example: `$mdn.text$` gets the text portion of the MDN

**`$exception.xxx$`**, used by EmailLogger

where `xxx` can be any of the following values to get

- name
- message
- trace
- terminated

for example: `$exception.trace$` gets the trace log of the exception

## 10. 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*

erroridir

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*

## ***11. 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](mailto: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"*

## 12. 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