axway

B2Bi

Version 2.3.2
April 2018

ICAP User Guide

This documentation describes the following Axway software:

Contents

Native Anti - Virus/Malware for B2Bi 1

B2Bi natively provides a file Anti-virus / Malware hookup integration. It is based on ICAP, to avoid dependency on specific AV vendors.

The ICAP Inline Processor

Purpose

The Internet Content Adaptation Protocol (ICAP) Inline Processor allows an administrator to configure ICAP engines to secure B2Bi exchange processes. This provides data loss prevention (DLP) and anti-virus (AV) scans. This option is preferable to the alternative of using non-secure connections and adding SSL coding, typically recommended against because of the negative performance impact.

The ICAP functionality for B2Bi is embedded in an Inline Processor. It can be added to a trading pickup as an attribute and as a message handler processing action.

Configuring the ICAP Inline Processor

Initial deployment

After the latest version of B2Bi is installed, and prior to the configuration of ICAP scanning within B2Bi, you must:

Note The folder names may differ depending upon the version of B2Bi that is installed.

1. Locate the `avScanner.properties` file within this directory: `B2Bi_installation\Interchange\samples\icapAv\`
2. Deploy the configuration file (`avScanner.properties`) in this directory: `B2Bi_share\common\conf\avConf`
3. In the case of a B2Bi cluster, repeat this process on all the B2Bi cluster nodes.

Update the avScanner.properties file

The anti-virus inline processor requires the Av-scanning properties to be configured correctly. The properties are auto-documented in the avScanner.properties file.

Properties include *filters* that specify which files are not to be scanned, based on criteria such as:

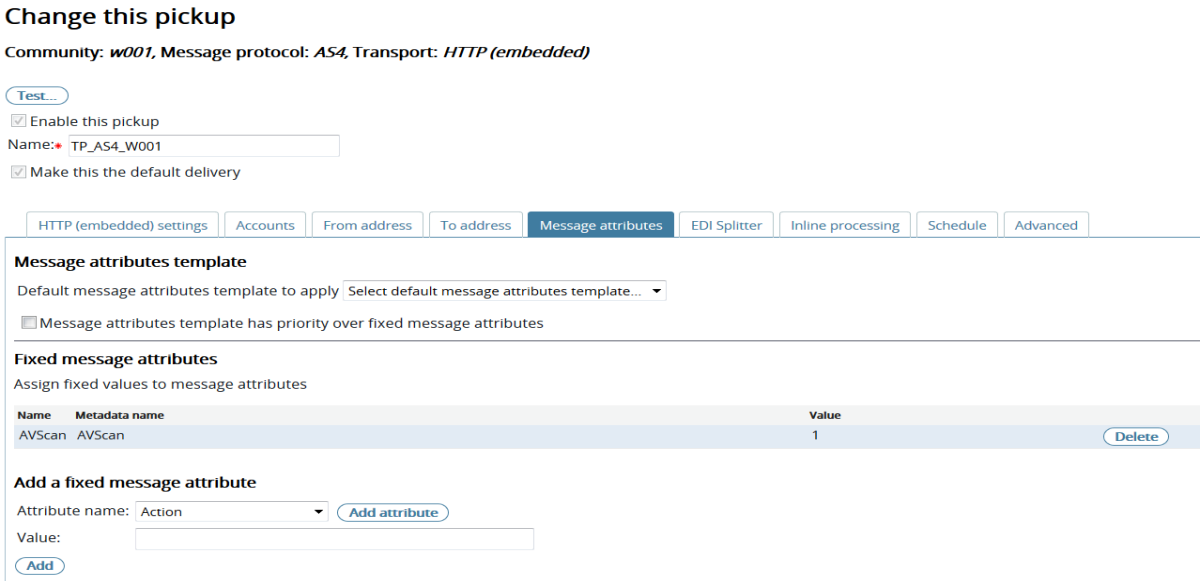
- max file size
- file extensions and/or file names
- protocols
- partners

Enable the AV-scanning

The following procedures explain how to enable AV-scanning in a trading pickup as a message attribute and the inline-processor in a message handler processing action.

Enable the AV-scanning as a message attribute on a trading pickup

1. Open a Trading or Application Pickup exchange definition.
2. Navigate to the **Message attributes** tab.
3. **Add a fixed value to messages** called for instance *AVScan* and set a value
4. **Save** the Trading pickup definition.



Enable the AV-scanning in a message handler processing action

1. Navigate to **Manage Trading Configuration**.
2. Select a Community.
3. Select **Processing** from the Community Map.
4. Select **Message Handler** from the Processing Map.
5. Select **Manage message processing actions**.
6. Select **Add a new message processing action**.
7. Create the condition that is required for the message handler processing action to execute. The condition contains the attribute set on the trading pickup and click **Next**.
8. Select as operator **Perform inline processing via a Java class** and use the following value in **Class Name: com.axway.antivirus.inlineprocessor.AntivirusProcessor**
9. Click **Next**.
10. Provide a friendly name and click **Finish**.

Monitoring the Scan process

Log file ->

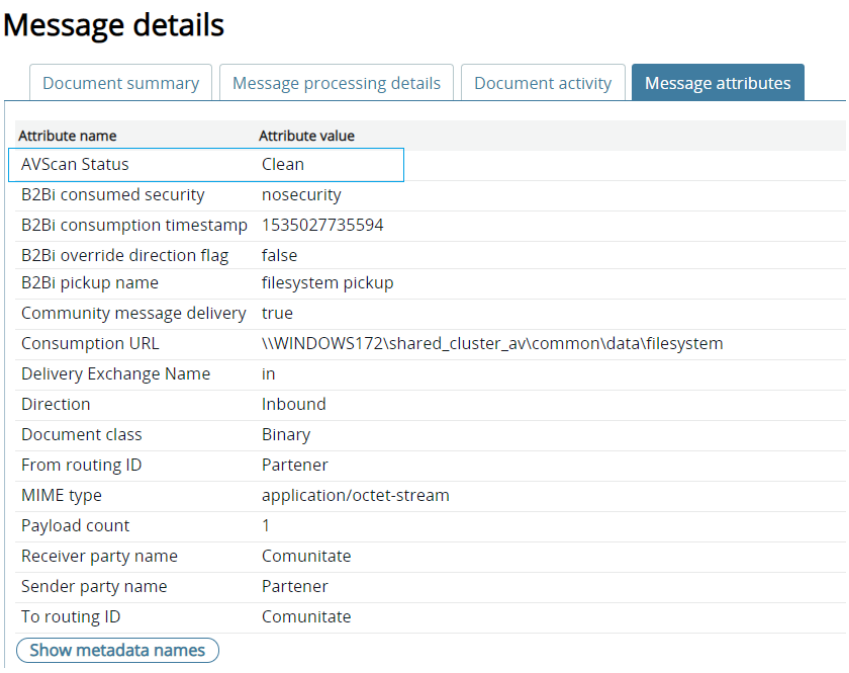
After enabling the virus scan in your configuration, when a file that matches the criteria is scanned, the following entries appear in the Trading Engine log (TE.log), for example:

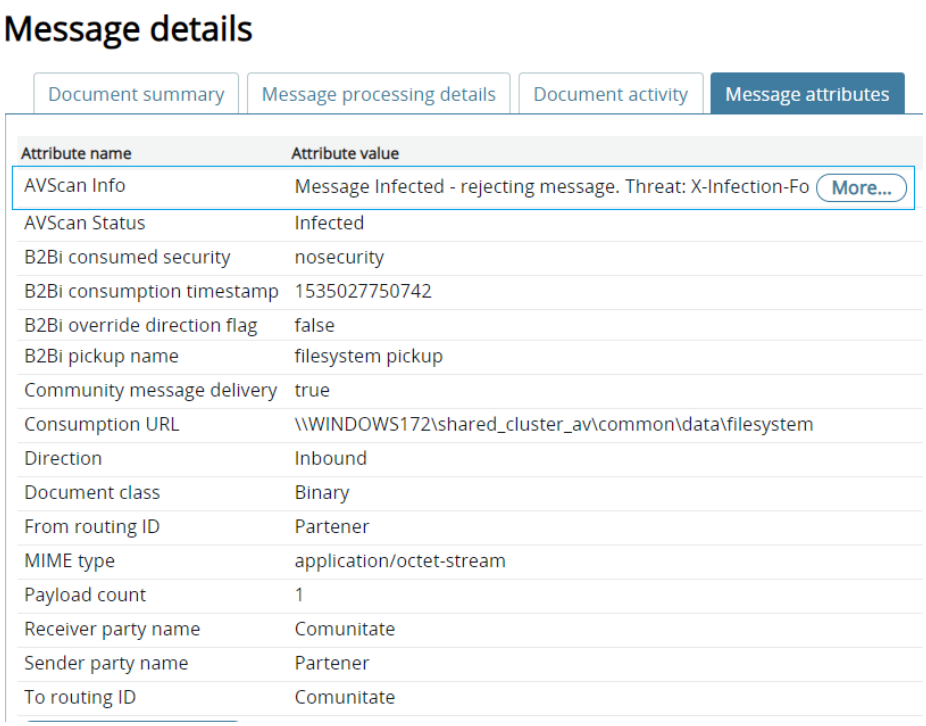
```
2018-08-23 06:18:50,726 - INFO  [Thread-1028]
(AntivirusConfigurationWatcher) - Antivirus configuration changed. File
affected: avScanner.properties.
2018-08-23 06:18:50,726 - INFO  [Thread-1028]
(AntivirusConfigurationManager) - Scanner configuration not present or
modified - attempting to load it.
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Scan from integrator value is: false
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Reject file on error value is: true
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus standard receive length is: 8192
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - The ICAP server version is: 1.0
```

```
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus hostname is: cos7-dev-
19.lab.buch.axway.int
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus port is: 1344
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus preview size is: 1024
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus service name is: squidclamav
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus standard send length is: 8192
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus connection timeout is: 2000
2018-08-23 06:18:50,741 - DEBUG [Thread-1028]
(AntivirusConfigurationHolder) - Antivirus maximum file size is: 60000000
2018-08-23 06:18:50,741 - INFO  [Thread-1028]
(AntivirusConfigurationManager) - Scanner configuration successfully
loaded.
```

The Message Tracker

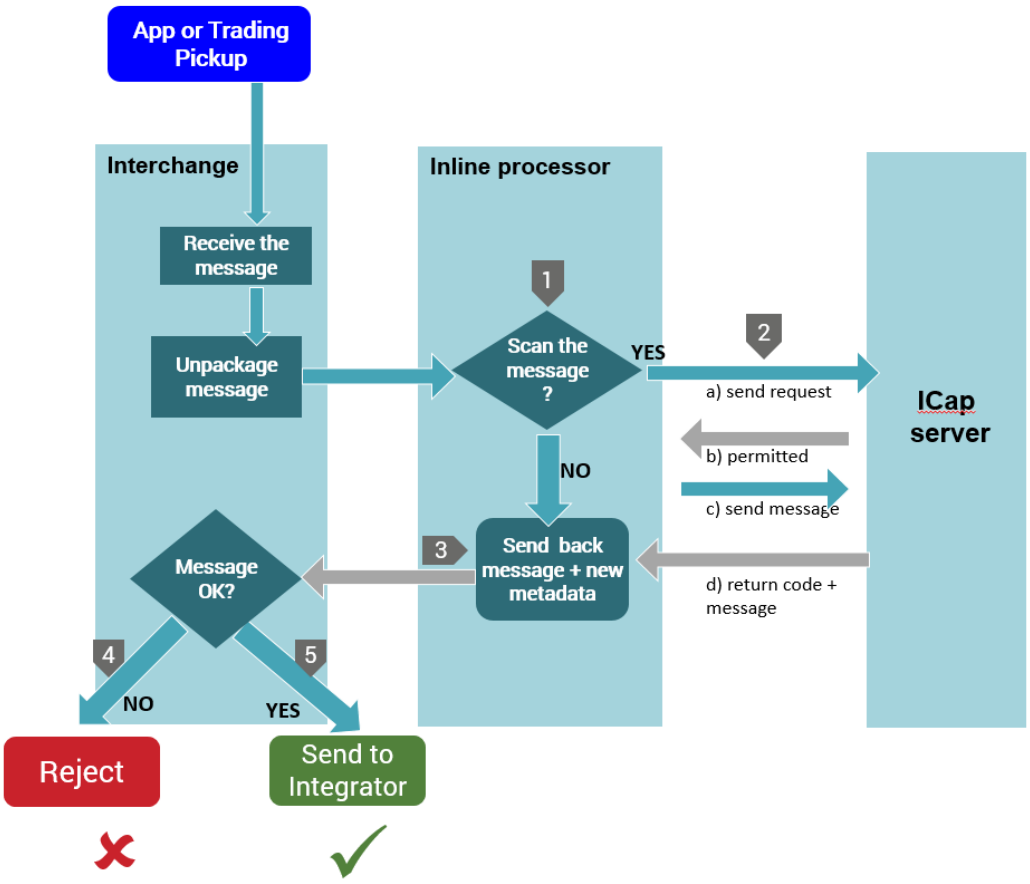
In Message Tracker, a metadata attribute is added that indicates the scan status of the message.




Message details
Document summary
Message processing details
Document activity
Message attributes
Attribute name
Attribute value
AVScan Info
Message Infected - rejecting message. Threat: X-Infection-Fo
More...
AVScan Status
Infected
B2Bi consumed security
nosecurity
B2Bi consumption timestamp
1535027750742
B2Bi override direction flag
false
B2Bi pickup name
filesystem pickup
Community message delivery
true
Consumption URL
\\WINDOWS172\shared_cluster_av\common\data\filesystem
Direction
Inbound
Document class
Binary
From routing ID
Partener
MIME type
application/octet-stream
Payload count
1
Receiver party name
Comunitate
Sender party name
Partener
To routing ID
Comunitate

How the scanning process works

The following diagram illustrates the ICAP file scanning process when the scanning option is activated:



1. If the message received from Interchange has restrictions defined in the `avScanner.properties` file, the Inline processor decides whether to scan the message or not
2. If the message is to be scanned, the dialog between the Inline processor and the ICAP server is as follows:
    a. The Inline processor sends the OPTIONS request to connect to the ICAP server
    b. The ICAP server indicates which type of request are permitted and gives back the maximum size of the preview the server can use.
    c. The Inline processor sends the message in chunks
    d. The ICAP server sends a code and a message

3. The inline processor sends the message with the new metadata back to Interchange - "AVScanStatus"- "AVScanInfo"
4. The message is rejected if it is Infected or if an ERROR occurred
5. The message is send to Integrator for processing.

Notes and limitations:

1. If the backup option is activated, and the files are infected, a backup of the file is saved on the system.
2. If the backup option is disabled, the files are deleted directly.
3. The payload of the infected files cannot be viewed or downloaded from the Message Tracker.
4. If a message has more than one attachments, and these are infected:
    - the infected attachment is not sent to processing
    - In the original message, the link for the failed attachment is still available