Axway B2Bi 2.2.1 Release Notes

Document version: July 8, 2016

Product version requirements

B2Bi 2.2.1 operates with the following B2Bi Client product version.

Axway product	Version	Service Pack
B2Bi Client	2.2.1	–
Mapping Services	3.1.1	–

The following Standards Libraries are released with B2Bi 2.2.1:

Standards Library	Version	Service Pack
Core EDI	1.4.0	–
Extended B2B	1.3.0	–
Financial	3.2.0	SP1

Implementations with other Axway products require the following versions for compatibility with B2Bi 2.2.1:

Axway product	Version	Service Pack
API Gateway	7.4.1	–
PassPort	4.6.0	SP9

Axway product	Version	Service Pack
Secure Transport	5.3.1	–
Sentinel	4.2.0	SP2
Transfer CFT	3.1.3	SP7
WebEDI	3.6.1	SP2

Each of the listed service packs is available as an individual download which can be obtained at support.axway.com.

For service pack installation procedures, see the *B2Bi Installation Guide* chapter "Apply service packs and patches".

New features and enhancements

Additional platform support

B2Bi has now been tested and validated for installation on the additional platforms:

- SUSE Enterprise Server (SLES) 12
- Oracle Linux 6.x and 7.x
- RHEL 7.1

Automated port allocation

The B2Bi Server installer now automatically allocates the required B2Bi ports during the installation and upgrade processes. There is no longer a Linux/UNIX requirement to manually assign ports.

Fully Qualified Domain Name support

You can now install B2Bi Server on Linux/UNIX machines configured with FQDN used as the host name.

Additional message handling support

You can now use B2Bi for the exchange of Edig@s 5.1 messages.

EDIFACT INOVERT32 is now a supported message format.

Cluster farms

You can now install multiple B2Bi server clusters in a farm environment for dramatically increased throughput.

Farm server installer

B2Bi now includes a new farm server installer for the installation of the coordinating server of the cluster farm environment.

Pickup groups

You can now organize application pickups and trading pickups into groups in which they can be activated, deactivated, exported, and imported together.

Custom metadata attributes

You can now create custom metadata attributes, associate them with messages consumed on application pickups, and use these attributes in your message processing flows.

Customizable retries

It is now possible to set the delay between message sending retries for each application and trading delivery.

B2Bi integration engine sequencing features

The B2Bi integration engine now provides enhanced sequential processing of messages and additional sequencing controls through the integration engine interface.

Link metadata services to integration engine pickups

You can now configure the pickups that reside on the integration engine ("application" type application pickups) to directly apply a metadata service to all messages consumed on the pickup.

Document agreements page access

You can now access the *Manage document agreements* page directly from the "Processing configuration" menu.

Single Sign On

B2Bi now supports Single Sign On in networks with SAML 2.0 based identity provider servers. Note that B2Bi does not accept SSO via SAML in combination with PassPort access management configurations.

SAML SSO enhancements

B2Bi now supports SAML Single Logout, SSO metadata configuration information through a dedicated B2Bi URL, and SHA256 signing of SAML requests and responses.

Support for POP3S and SMTPS

B2Bi now supports POP3S and SMTPS (POP3 and SMTP over TLS/SSL) for AS1 and generic email exchanges.

PGP over email

You can now configure trading pickups and deliveries to trade using PGP with SMTP embedded, SMTP/S global external, and SMTP/S partner-specific servers.

This function works only in Limited Message Processing mode (the B2Bi integration engine does not support PGP over email trading). To set a pickup to this mode, you must select the "Processing mode = Limited" option in the pickup's maintenance page..

The PGP configuration information is included in the system export/import package.

The B2Bi REST API also supports PGP configuration management for email pickups and deliveries, with the exception of PGP certificate handling.

AS4 two-way Message Exchange Patterns

B2Bi now supports the configuration of AS4 synchronous and asynchronous two-way Message Exchange Patterns (MEP).

Java 8 support

The B2Bi Server and the Secure Relay router agents run on machines with JRE 1.8 installed.

Secure Relay proxied CRL checking on LDAP servers

Secure Relay CRLs can now be checked on proxied LDAP servers.

Enhanced security for private keys

Additional security has been added to control which users can export from PFX files.

Windows B2Bi service

A single Windows B2Bi service now starts the entire B2Bi product. This replaces the individual services for the integration and trading engines.

Integration Services secure client connection to B2Bi servers

All connections from client Integration Services instances to B2Bi servers are SSL secured. Connection handshakes and object deployment are secured.

Sentinel: Simplified Sentinel tracking

Simplified Sentinel Tracked Objects now replaces the multiple Tracked Objects that were required to collect and display data about B2Bi message processing and system events.

Sentinel: Linking of rerouted messages

When messages are rerouted in B2Bi, the "ExchangeName" and "ExchangeURL" attributes are not sent to Sentinel in the "Delivered" event. This is by design because the message is not directed to its original destination. To enable enhanced visibility of the overall end-to-end flow of rerouted messages, in B2Bi 2.2, a common cyclelink is applied to both the re-routed message and the original message.

Sentinel: CycleIdSequence number incrementation for special cases

B2Bi now provides incremented CycleIDSequence numbers for the following event types that could not previously be tracked through an incrementing CycleIDSequence number:

- WebTrader non-trading events (Accessed, Moved, Renamed, Removed, Purged)

- Hosted FTP events (Downloading, Downloaded, Purged)

- Resend (and all subsequent events in the same life cycle)

Note that, unlike most CycleIdSequence numbers, for these cases the numbers are based on a Java timestamp so are longer than the typical one- or two-digit numbers for this attribute.

Sentinel: Override of default direction attributes

Message flow direction is a relative concept. In some production cases it makes good sense to modify the default direction labeling, for example to view Trading Partners as outbound senders, or to view Partner-to-Partner exchanges as internal exchanges. For cases such as these, you can override the Direction attribute to customize the message direction representation in Sentinel.

Sentinel - Manage Filtering and Custom objects

The functionality for controlling Sentinel message filtering and creating custom tracked objects have been removed from the B2Bi user interface *Integrate with Sentinel* page. To develop these special Sentinel features you now work in the B2Bi SDK (Software Devlopment Kit). For more information, see the *B2Bi Trading Engine Developer Guide*.

EDI Tracker tool renamed

The B2Bi integration engine client EDI Tracker tool has been enhanced and renamed "Document Tracker".

Integration Services

The B2Bi Client Integration Manager has been enhanced and renamed "Integration Services". From B2Bi 2.2.1, Integration Services is a standalone tool that resides only on B2Bi client machines. It no longer resides on instances of the B2Bi Server.

Simplified migration from XIB

When you use the Integration Services tool to migrate Axway Integration Broker (XIB) V2 configurations to B2Bi, the tool automatically creates the following objects in the B2Bi configuration:

- Components

- Services

- Pickups

- Deliveries

This enhancement eliminates the multiple configuration steps that were previously required after XIB migration.

Streamlined upgrades from Interchange implementations

The upgrade logic has been improved to simplify and accelerate upgrades from Interchange implementations.

Enhanced auditing

Operations that are executed from Integration Services and System Profile Manager through the deployment server are now automatically written to trace log as AUDIT-type entries with username, date, type and description. These events can be displayed through Trace Viewer searches.

Datamapper simulation

You can now run the Datamapper Simulator server locally on each of your client machines for faster simulation results.

Override default PGP signing certificates

B2Bi users can now specify an alternative PGP signing key for a partner or category in the Collaboration Settings.

New standards library format support

Refer to the standards library release notes for newly supported document formats.

New IBM MQ supported version

B2Bi has now been tested for the support of IBM MQ 8.0.

Virtualization support for x86/x64 based systems

Axway generally supports product installation and operation on VMware virtual machine platforms. For B2Bi support cases, Axway will investigate and troubleshoot a problem until it is determined that the problem is due to virtualization. If Axway suspects that a specific defect occurs because the system is virtualized and we cannot reproduce the problem in a non-virtualized environment, we will request you to either reproduce the defect on a non-virtualized environment and to contact the virtualization vendor for a resolution, or to switch to a non-virtualized platform.

Important note for FIPS implementations

This announcement applies to all B2Bi implementations that adhere to the Federal Information Processing Standards (FIPS). In B2Bi, FIPS is a license key-enabled option that turns on FIPS-compliant implementations of certain cryptographic algorithms.

The security provider libraries for FIPS have been updated in B2Bi 2.x. There is now stricter enforcement of the allowable key lengths in RSA Key Pair Generation, aligned with the following excerpt of the requirement. Full NIST requirements are available at:

http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

"This Standard specifies three choices for the length of the modulus (i.e., nlen): 1024, 2048 and 3072 bits. Federal Government entities shall generate digital signatures using one or more of these choices."

As a result, cryptographic functions that use alternate key lengths (for example, 512 or 4096) are blocked while in FIPS mode. This can render trading with existing certificates inoperable, including certificates imported from trading partners. Administrators of existing B2Bi installations or Interchange installations who upgrade to B2Bi 2.x, and who have keys of alternate lengths (512 and 4096 are most common) must do one of the following:

- Update (import new, or re-generate) any certificates that are not compatible (those not of a 1024, 2048, or 3072 length)

- Disable the key length enforcement.

  Caution: Disabling key length validation makes your environment non-FIPS compliant, and non-compliant with the Federal standard. It should only be used as a temporary measure.

Fixed problems

This section lists issues specifically resolved in this release.

Case ID	Internal ID	Description
	B2Bi	
00813153	D-100847 D-100809	**Issue:** When sending an AS4 message to a trading partner, the message is signed. However, when the partner sends back (synchronously) an unsigned receipt, the receipt is rejected by B2Bi. This result is compliant with AS4 standards, but may not satisfy production requirements. **Resolution:** A new setting in SystemProperties enables you to receive an unsigned receipt over a synchronous connection when sending a signed AS4 message to a trading partner. **Caution:** Incorrectly modifying values on the SystemProperties page can severely degrade product behavior. Do not modify values on this page without explicit guidance from Axway support.

Known issues and limitations

- (D-103483) **Upgrade from 1.5 - Inbound agreement EDIFACT Interchange partner ID is not automatically enabled**

Issue: When upgrading from B2Bi 1.5, if the Interchange partner ID was selected on an EDIFACT messaging profile, then after upgrade the inbound EDIFACT agreement has the Interchange partner ID grayed-out but disabled. The result is an inbound EDIFACT agreement in an invalid state with the inability to manually enable the Interchange partner ID.

Workaround: Recreate the inbound agreement.

- (D-103230) **Unable to use TLSv2 cipher - SSL_RSA_WITH_RC4_128_SHA in MQ8**

Issue: When setting the cipher suite value to SSL_RSA_WITH_RC4_128_SHA in B2BI, B2Bi fails to make calls to MQ. The supported TLSv2 cipher does not work after upgrade to B2Bi 2.2.1, which uses Java 8, update 66.

Workaround:

1. Go to `<B2Bi_install_directory>\Interchange\conf` and open `jvmArguments.xml` in an editor.

2. Add the line:

   `<Option>Djava.security.properties=../conf/mysecurity.conf</Option>`

3. Create a new file in the `../conf` directory called `mysecurity.conf`. In this newly created file, add the line:

   `jdk.tls.disabledAlgorithms=SSLv3, MD5withRSA, DH keySize < 7683`

   This line enables the RC4 encryption algorithm, which allows the cipher SSL_RSA_WITH_RC4_128_SH.

4. Restart B2Bi.

- (D-102799) **SSO: Unexpected error when accessing metadata profile on 6080 port**

   When accessing the SSO Metadata URL to view the Service Provider configuration on non-sso port (6080), when no service provider certificate is selected (SSO configuration is incomplete) an unexpected error is displayed in UI.

- **Secure Relay installation on AIX platforms**

   For installations on AIX platforms, both B2Bi Server and Secure Relay must use the same operating system.

- (D-101399) **A remote client should not connect directly to the embedded secured server when "Enable security termination in DMZ" is selected**

   When configuring a SSL secured B2Bi embedded server (HTTPS/FTPS), and when the server DMZ ports settings have both "Enable DMZ port forwarding" and "Enable security termination in DMZ" options selected, the remote unsecured client generates connection errors in the following cases:

   ○ HTTPS server – The client can send a message directly on the server with a HTTP partner delivery (the URL starts with http://)

   ○ FTPS server - The client can send the message with a FTP partner delivery in both explicit and implicit SSL modes. In the explicit mode there is an exception on the client side "Client closed connection before all replies could be sent" however the message transfer is made successfully.

   ○ SFTP server - It is not possible to use a non-secured client since it doesn't have an non-secured version.

- (D-101493) **Transfers from whitelisted partners fail when "Match IP Address Against Partner Definition" is selected on a pickup with DMZ security termination**

  Issue: When you configure a pickup with both "Enable IP address checking in DMZ" and "Match IP Address Against Partner Definition" selected, and then consume a message from a trading partner whose IP address in included in the master whitelist, the IP address passes the IP filtering in the DMZ Router Agent, but fails in the trading engine.

  Workaround: You should not configure both community-allocated user accounts and partner defined IP ranges together with "Match IP Address Against Partner Definition". In order to enable message consumption, you must do one of the following:

  ○ Deselect "Match IP Address Against Partner Definition" (leaving "Enable IP address checking in DMZ" selected)

  ○ Change the user credentials to be explicitly owned by the same partner.

- (D-101648) **System import/export: Components defined in a service are not exported in the correct order**

  Issue: If you have multiple components of the same type in a service and use the "Move component up" or "Move component down" tools to change the component display order in the UI, the new order is not conserved when you export and then import the service to a new system.

  Workaround: After importing a service with multiple components of the same type, be sure to verify the component order, and manually re-order them if necessary.

- (M-154760) **Failure of FORCE_SYNC command on Solaris 11**

  Issue: In Solaris 11 environments, when running FORCE_SYNC to force the synchronization of maps, the synchronization fails.

  Workaround: Add the following line to `$CORE_ROOT/profile:unset LC_ALL LC_CTYPE`.

- (M-154418) **Sentinel direction reporting: Unexpected values on receipts from partners**

  In the following cases, direction reporting to Sentinel may show unexpected results:

  ○ **MDN sent** – When B2Bi receives a message and sends an MDN, the direction shown in the integration engine is "outbound"; however Sentinel shows "Inbound" for this event.

  ○ **Extra MDN Received** – When B2Bi sends an MDN, there is a redundant "MDN received" event present in Sentinel, with an "Inbound" direction. In this case, the MDN was not really received in this flow, but the direction attribute is reported anyway.

  ○ **MDN Received** – When B2Bi receives an MDN, Sentinel shows the MDN received event as the last event in the flow. This MDN reception event has the "Outbound" direction in Sentinel, but has "Inbound" in the B2Bi Message Tracker UI.

  ○ **External** – The "External" direction is assigned to partner-to-partner exchanges. X12 997 acknowledgements sent for these external messages are also assigned the "External" direction. In this case, the "MDN received" event (MDN received for the 997) has the "External" direction, but the direction of the received MDN (of 997) in B2Bi Message Tracker is "Inbound".

- (M-139276) **Sentinel Tracked Object field type limitation**

  Issue: For Sentinel Tracked Objects, the Sentinel type 'Long String' is not supported in the DML used in Mapping Services. This leads to an attribute length "0" when deploying to a B2Bi integration engine.

Workaround: For B2Bi integration engine processing, the 'Long String' data type is identical to 'String'. In Sentinel Tracked Objects, use the 'String' data type in place of 'Long String' to avoid errors.

- **Sentinel: "Resend" events display as "Delivered"**

When you "Resend" a message from Document Tracker, in Sentinel the event displays unexpectedly as a "Delivered" event within the same CycleID. This incorrect event type labeling will be corrected in a future release of B2Bi.

- **SAN file system hotfix requirement**

Issue: Two SAN 6.2 cluster nodes show different contents of a file on CFS share.

Workaround: In order to run B2Bi on SAN 6.2, you must obtain the **VxFS 6.2.0.003 HotFix** from Symantec Support and apply the HotFix to each Veritas cluster node.

- (M-149162) **Windows failover: Missing Interchange control numbers during a failover**

When configuring an outbound X12 enveloper with the Interchange control number generator specified as `$icid:9$`, in the event of failover the generated control numbers are not consecutive. **Note**: Consecutive control numbers are not guaranteed in the case of failover. This is not considered to be a product defect.

- (M-154673) **Peer Networks: Partner user accounts are not correctly cloned to peers**

Issue: In peer network environments with auto-cloning of trading pickups enabled, when you have communities that include partner user accounts (FTP, SFTP, WebServices, AS4,...) the user accounts are not correctly cloned.

Workaround: If have enabled auto-cloning of trading pickups, you must also enable auto-cloning of partners.

- **Upgrade: Not all Document Tracker "warning" entries are displayed**

When you install B2Bi 2.2.1, the Document Tracker provides an additional search filtering criterion: "warning".

Only "warning" type Document Tracker entries that are generated after installing B2Bi 2.2.1 can be filtered (and optionally displayed) in search results when you use this filtering criterion. "Warning" type entries that were generated in B2Bi 2.2.1 before applying upgrades are not be filtered.

- **Swagger API client: Swagger user can continue to execute operations after logout**

When using Chrome and Firefox browsers, after logging out of a Swagger session, a user can call operations as though they had not logged out. This problem occurs because these browsers remember, and automatically provide, the login credentials. Credentials are cleared from memory when the browser window is closed.

- **Swagger API client: Swagger user cannot log in using the login method**

Issue: The REST login method asks for the authorization header, which is a single string composed of a hash of the username and password. However, in most cases, users only know their username and their password.

Workaround: The user can call directly the desired operation. This triggers the login, causing the browser to display a user-friendly prompt for the username and password.

- **Swagger API client: User cannot import or export certificates**

When a user accesses the import operation, it is not possible to specify the path to the certificate to be imported. For the export operation, it is not possible to specify where the exported file is to be saved. This is because the Swagger client does not support the "application/octet-stream" content-type used by the import/export operations in the B2Bi REST API.

- (M-137103) **B2Bi clustered implementations with X.400 subsystems: Starting any trading engine temporarily stops the X.400 subsystem**

In B2Bi active/active clustered configurations with an X.400 delivery exchange configured, when stopping and then restarting any trading engine in the environment, the X.400 subsystem is temporarily suspended for a period of approximately 15 seconds, which causes a temporary suspension of X.400 services.

The resolution of this defect is being studied for a future release.

- **With ebXML intermediary (SMTP), message cannot be delivered to external SMTP server**

When setting up an ebXML intermediary (SMTP), an embedded SMTP server must be used for the receiver. If the external SMTP server is used, the trading to the receiver fails.

- **FTPS outbound transfer fails when Secure Relay Routing Agent runs on AIX**

Issue: For B2Bi installations with Secure Relay, when the Secure Relay Routing Agent (RA) runs on an AIX machine, FTPS outbound transfers fail when any of the following cipher suites are used as overrides on the partner delivery:

  - SSL_RSA_WITH_DES_CBC_SHA

  - SSL_DHE_RSA_WITH_DES_CBC_SHA

  - SSL_RSA_EXPORT_WITH_RC4_40_MD5

  - SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

  - SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA.

Work around: Select an alternate cipher suite on the partner delivery.

- **Sequential delivery: Trading engine blocks sequential delivery when message-handling timeout threshold is engaged**

For messages that are consumed on exchange pickups with sequential delivery activated, when the message handling time-out threshold for the pickup is reached, the trading engine begins a resend/retry cycle on the sequenced message that blocks the entire sequence until the production of the message is resolved.

- (M-141384) **MQ JAR version conflicts block trading**

You cannot have multiple versions of JMS provider JAR files in the `...Interchange/site/jars` or `...Interchange/corelib` directories. For example, if you already have v7.5 IBM MQ JARs and add V8.0 JARs, you must remove the older JARS to avoid conflicts.

- (M-144653) **Peer Network: Trusted root certificate is not deleted from backup peer**

Issue: In a Peer Network configuration, when a user creates a MLLP with TLS application pickup and adds a trusted root certificate in the MLLP embedded server's "trusted root certificates" tab, the certificate is

correctly cloned to the backup machine. However, if a user then performs an untrust action on the trusted root certificate of the main network, the untrusted status is not propagated to the backup peer network and the certificate is still available.

Workaround: Manually delete the the certificate on the peer machine.

- (M-144708) **Peer Network: When Peer Network messages fail due to transport errors, the messages are resent**

Issue: Peer Messages are an instantaneous snapshot of network status and have no value when resent later.

Work around: Reset Reliable Messaging resend attempts to "0". To do this:

1. In the B2Bi UI, select Trading configuration > Manage trading configuration.

2. Select "Change default collaboration settings".

3. Select the "Reliable messaging" tab.

4. In the "Resend attempts" field enter the value "0".

5. Click "Save changes".

- (M-142813) **Cannot create an embedded WebDAV SSL partner delivery**

When defining a WebDav embedded SSL server to support a WebDav type partner delivery, you cannot successfully add a trusted SSL root certificate linked to the partner. This prevents the creation of a valid WebDav delivery.

- (M-143434) **REST API - Unable to add partner with name that contains non-ASCII character**

Issue: By default, B2Bi does not support the use of non-ASCII characters in partner names when adding partners through the REST API.

Workaround: Go to [B2Bi_install_directory]/Interchange/conf/jvmArguments.xml, and add the property:

<Property key="file.encoding">UTF-8</Property>

- (M-144031) **Installation and upgrades on Windows: Installation directory naming limitation**

Issue: Installing or upgrading to B2Bi 2.2.1 on Windows platforms fails if you install or upgrade to a directory that begins with any of the characters "u", "U" "t" or "T".

Resolution for clean (non-upgrade) installations:

During the installation, do not enter a directory path that begins with any of the following characters: "u", "U", "t", "T"

Resolution for upgrades to existing installation directories that begin with any of the characters "u", "U", "t", "T":

Use the following procedure.

1. Edit the following Integrator environment variables, replacing double backslashes with single backslashes in directory paths:

   ○ %CORE_ROOT%

   ○ %CORE_DATA%

   ○ %CORE_LOCAL%

2. Go to [B2Bi_installation_dir]/Integrator/config, and edit the environment.dat configuration file. Locate the variables listed in step 2 (above), and replace double backslashes with single backslashes in directory paths.

3. Go to the installation directory at [B2Bi_installation_dir]/Configuration, and edit the Install_ Integrator_V3.7.3.properties file. Locate the following variables, and replace double backslashes with single backslashes in directory paths :

InstallDir =

IntegratorLocalDir =

IntegratorDataDir =

IntegratorDMLDirDefault =

IntegratorDMLDirDefault.DefaultValue =

IntegratorDMLDir =

IntegratorRootDir =

4. Install the B2Bi 2.2.1 upgrade.

- (M-136067) **Upgrade: Metadata Profiles with 'equals *' criteria fail in the integration engine**

  After upgrading from B2Bi 1.5.0 to B2Bi 2.2.1, Metadata Profiles with 'equals *' criteria are no longer returned by the integration engine Configuration Adapter Node. To resolve this issue, manually update the Metadata Profile criteria after the upgrade.

- **Upgrade: PostTransfer and Document B2BX Application Components display 1.5.0 values in the 2.2.1 UI**

  After upgrading from B2Bi 1.5.0 to B2Bi 2.2.1, PostTransfer and Document B2BX Application components still display 1.5.0 values. These fields should normally be displayed only on the 2.2.1 Service object that uses the Component. If this occurs, open the affected Component and Service definitions and save the objects. This will resolve the issue.

- **Upgrade: After upgrade, export/import of an Agreement that contains multiple Document Agreements fails**

  This issue occurs only in the following context:

  1. You upgrade from B2Bi 1.5.0 SP11 to B2Bi 2.2.1.

  2. You perform a B2Bi System Configuration Export that includes an Agreement that has multiple Document Agreements, where two or more of the Document Agreements are not unique. One of the Document Agreements is enabled and the non-unique Document Agreements are disabled.

  3. You clean the database and import the exported B2Bi System Configuration.

  The result is that the non-unique Document Agreements are not imported.

- (D-102522) **AS4: Selecting "Synchronous response generated in backend" option on an asynchronous message exchange causes failed receipt status**

When the 'Synchronous response generated in backend' option is enabled on receiver's AS4 HTTP(S) Trading Pickup, and the receiver consumes a negative receipt over a new asynchronous connection, the receiver keeps the connection open for a User Message reply. However, since there is no User Message reply for a negative receipt, the receipt status ends in 'Failed' when all the retries are exhausted.

- (D-101824) **AS4: Synchronous two-way response without RefToMsgId fails**

  In a AS4 synchronous two-way exchange, when the response from the receiver does not include the RefToMsgId, the sender side user message request status changes to "Fail" instead of "Delivered", with a reason that the RefToMsgId was missing. The receipt status on the sender side remains "In process" (instead of "Delivered") because the response message does not include the RefToMsgId.

- (D-101827) **AS4: Synchronous two-way response without ConnectionID causes connection to close prematurely**

  In a AS4 synchronous two-way exchange, when the response does not include the ConnectionId, the sender side stays in the "In Process" status for up to 10 minutes before the message status changes to "Delivered". If the receiver partner tries to resend the response (with correct ConnectionId and RefToMsgId), the message fails because the synchronous connection has been closed after the first response.

- (D-102246) **AS4: In a two-way push/pull exchange, the pull request successfully pulls a receipt when expected to fail**

  The polling client in an AS4 two-way push/pull exchange is able to pull a receipt message in place of a response message. This defect will be corrected in a future release.

- (M-131855) **AS4: Wrong signature generated when using SOAP body with CDATA and MTOM in combination**

  When "Sign Message" and "Use MTOM" are enabled in collaboration settings, and a SOAP body payload has both CDATA and base64 encoded content, the wrong signature value is generated. When the receiver receives this message, it incorrectly fails the message and generates a "The signature or decryption was invalid" SOAP fault.

- (M-133284) **AS4: Unable to configure a partner-specific fragment size in collaboration settings**

  Currently, metadata can be added only in the message attributes section of the polling client and AS4 protocol exchange.

- (M-134139) **AS4: Split compression algorithm is set to "gzip" on first fragment and to "application/gzip" on original message and other fragments**

  When a file is split into multiple fragments, if the MIME/GZIP algorithm was selected for the MIME envelope compression under AS4 collaboration settings/split messages, then on the sender side in Message Tracker "Split Compression Algorithm metadata" is set to "gzip" on the first fragment and to "application/gzip" on original message and other fragments. The expected behavior is for the algorithm to be the same for all fragments and for the original payload.

- (M-134415) **AS4: SoapHeaderAndBody packaging method is not supported**

  Messages that are sent over AS4 can be packaged using the BodyOnly method only. SOAPHeaderAndBody is not currently supported.

- (M-134795) **AS4: Unable to specialize the as4.fragmentSize value for inbound fragments at trading pickup level**

  When consuming split message fragments on an AS4 community trading pickup, it is not possible to specialize the as4.fragmentSize restriction on the trading pickup. Currently as4.fragmentSize is a global system property and applies to both outbound and inbound flows.

- (M-135289) **AS4: No negative response receipt is returned when the splitting fragment numbering is incorrect**

  If the splitting fragment number is set to a valid value, but that value corresponds to to another fragment, no negative response receipt is returned. The reconstructed message fails with the reason: "Failure: java.io.IOException: End of Stream, but boundary not found". No negative response receipt is generated.

- (M-135526) **AS4: Reconstructed (split and rejoined) messages fail if the rejoined packaged size exceeds the maximum configured message size**

  Although the individual elements of a split message do not exceed the "Restrict maximum file size for this transport" setting, if the rejoined message exceeds the maximum size, the message fails.

- (M-135582) **AS4: Incorrectly signed synchronous push receipts are not rejected**

  If an AS4 message push sender is configured to expect synchronous receipts for sent messages that are signed with the SHA 256 algorithm, and the returned receipt is signed with SHA1, then the original push sender does not reject the incorrectly signed receipt.

- **SAP Metadata Browser plugin not supported**

  Issue: B2Bi supports the transfer of IDocs to and from SAP using ALE. However, the use of the B2Bi Metadata Browser to directly view SAP IDOC reports is no longer supported.

  Workaround: To view SAP IDOC reports, export the reports from the SAP system and use them in the Metadata Browser to create ADF files. For details about creating and viewing ADF files, see the B2Bi Operator Guide / Metadata Browser chapter.

- **API Connector and Datamapper ADF Metadata Browser plugins not supported**

  The Metadata Browser plugins for the API Connector and Datamapper ADF should not be used. They will be removed in a future release.

- **Upgrade limitation: Message Tracker fails to display message details**

  After upgrading a B2Bi 1.x implementation to B2Bi 2.2.1, Message Tracker no longer displays message-processing details of messages that were processed prior to the B2Bi 2.2.1 upgrade.

- **Upgrade limitation: Use of trading engine transports on the application side through Message Handler re-routing**

  If you had a B2Bi 1.x implementation in which a "U-turn construct" was employed to enable the use of the Trading Engine transports on the application side, this logic must be manually reconfigured after the upgrade.

- **Upgrade limitation: Alternate party in an agreement is used even when an outbound agreement for enveloping is specified**

  Issue: After upgrading from B2Bi 1.x to B2Bi 2.x, in some cases trading fails due to the way partner routing ID's are selected by the upgrade logic.

This occurs when the upgrade logic creates a document agreement inside an inbound agreement, and where the output in the document agreement refers to an outbound agreement for enveloping and also has the "Use alternate delivery partner" option selected. In this case, the Routing ID that is selected is the one that matches with the Messaging ID of the agreement, which leads to errors. The correct Routing ID should be one that reflects the identity that is used by the communication partner.

Resolution: In the B2Bi UI, manually edit each inbound agreement / document agreement, setting the Partner Routing ID to one that belongs to the community on the remote system.

- **RHEL 6 requirement for X.400 support**

  By default, the Red Hat Enterprise Linux 6 x86_64 operating system installs without installing a 32-bit library (/lib/ld-linux.so.2) needed by the trading engine X.400 subsystem. To enable B2Bi with X.400 installed on RHEL 6, install the package glibc.i686 from the RHEL installation media.

- (M-122568) **System import limitation: Processing fails on messages that were in "Retry Scheduled" state**

  In cases where you stop the trading engine node and import a system backup and then restart the node, any messages that were in "Retry Scheduled" state will fail on send attempts after restart. This is because the system import logic modifies the outbound ID of the target exchange partner. These in-process messages that are failed and any existing messages already in a "Failed" or "Delivered" state are now not possible to Resend or Reprocess.

- **MQSeries server access**

  B2Bi 2.2.1 installs updated MQ Series jars. You may need to modify the MQSeries configuration in order to enable an existing MQ 7.x configuration to work after upgrading to B2Bi 2.2.1.

  In some cases, the MQ jars that are updated in B2Bi 2.2.1 enable additional MQ 7.x security features. Depending on your configuration, you may need to do one or more of the following:

  - Update channel authentication records

  - Add or update authentication or object authorities

  - Add an MQ user to an Interchange MQ exchange point that formerly worked anonymously

  We recommend that you contact your MQ administrator if problems are noted.

- (M-112634) **Web Services provider flow: "check input attributes" and "check output attributes" not persisted on B2Bi server**

  Issue: In Mapping Services, when you create an enumeration in a BusinessDoc leaf (in the Attributes/Enumeration tab), and then use the BusinessDoc in a Flow in which the "check input attributes" and "check output attributes" options are selected, these options are not persisted when you deploy the map to a B2Bi server.

  Resolution: You must manually select the "check input attributes" and "check output attributes" options in the B2Bi user interface (Service/Service details/Component details).

- **MQ/SSL cipher suite selection issues**

  In the B2Bi user interface, when configuring an IBM MQ Series pickup or delivery exchange with SSL, it is necessary to select the SSL cipher suite to use. The cipher suite that you select must correspond to a specific cipher specification that the IBM server supports. The following table indicates correct

relationship between specification and cipher suite. Additionally, cipher suites preceded by an asterisk (*) are used to connect to a FIPS provider and, although they are displayed, they are not currently supported in B2Bi:

Cipher specification (MQSeries name)	B2Bi JSSE cipher suite
DES_SHA_EXPORT1024	*SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
RC4_56_SHA_EXPORT1024	*SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
RC4_MD5_EXPORT	SSL_RSA_EXPORT_WITH_RC4_40_MD5
RC2_MD5_EXPORT	*SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
FIPS_WITH_3DES_EDE_CBC_SHA	*SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	*SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA	*SSL_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA	*SSL_RSA_WITH_AES_256_CBC_SHA
DES_SHA_EXPORT	SSL_RSA_WITH_DES_CBC_SHA
NULL_MD5	SSL_RSA_WITH_NULL_MD5
NULL_SHA	SSL_RSA_WITH_NULL_SHA
RC4_MD5_US	SSL_RSA_WITH_RC4_128_MD5
RC4_SHA_US	SSL_RSA_WITH_RC4_128_SHA

* Not currently supported. Do not select this cipher suite.

- **Failover and sequential delivery**

  The ability to deliver messages in sequence in the case of a failover is not always guaranteed.

- **General Web Services limitations**:

  - B2Bi 2.x supports Web Services on the trading (partner side), but not on the application side.

  - By default, WS-Addressing must be used in provider mode. To disable the need for WS-addressing, refer to the alternate axis2NoWSAddressing.xml file in your WS pickup configuration.

  - The B2Bi WSDL wizard currently only supports the generation of WSDL definitions. These definitions cannot be edited afterwards. To change the WS interface, you must either regenerate a new WSDL using the wizard, or edit the WSDL manually.

- **Web Services provider mode HTTP connection fails to close**

Issue – When configuring Web Services provider mode for one-way communication with faults returned to client, on the Web Service trading pickup you must normally select the option "Synchronous response generated in backend" in order to enable sending of the fault file to the requesting service consumer. However, if the incoming request message does not trigger a fault and is correctly delivered to the back end, the HTTP connection is kept open until timeout on the client side.

Workaround – For a one-way Web Service provider configuration, do not select the option "Synchronous response generated in backend". This prevents the provider from sending a fault message, but allows the connection to close normally after receiving the client request message.

- **Web Services provider mode configuration using Mapping Services RouteTo blocks**

When a Web Services provider flow with attachments is configured that uses a Mapping Services map with a RouteTo block, B2Bi copies the inbound request attachment attributes onto the output response. This results in the inbound attachments being forwarded back to the originator of the Web Service request.

- **PassPort integration issue with integration engine tools**

When configuring the integration engine with PassPort access management, the B2Bi integration engine client tools lose the ability to distinguish between different levels of user privileges (view/modify/execute). Access to individual tools can either be granted or not granted.

Documentation

This section describes documentation enhancements and related documentation.

Documentation enhancements

The following documents have been updated to take into account new product features and enhancements for B2Bi 2.2.1:

- B2Bi Installation Guide
- B2Bi Administrator Guide
- B2Bi online help
- B2Bi Interchange Upgrade Guide
- B2Bi Operations Guide
- B2Bi Support Reference Catalog
- B2Bi Trading Engine Developer Guide

Related documentation

For more information about B2Bi and how it is used in Axway, refer to:

- B2Bi 2.2.1 Installation Guide
- B2Bi 2.2.1 Getting Started Guide
- B2Bi 2.2.1 online help
- B2Bi 2.2.1 Administrator Guide
- B2Bi 2.2.1 Operations Guide
- B2Bi 2.2.1 Support Reference Catalog
- B2Bi 2.2.1 Security Guide
- B2Bi 2.2.1 Interchange Upgrade Guide
- B2Bi 2.2.1 Developer Guide package
- Axway Overview
- Axway Supported Platforms
- Axway Interoperability Matrix
- Axway Concepts Guide
- Axway B2B Reference Solution Implementation Guide

Support services

The Axway Global Support team provides worldwide 24 x 7 support for customers with active support agreements.
Email support@axway.com or visit support.axway.com.