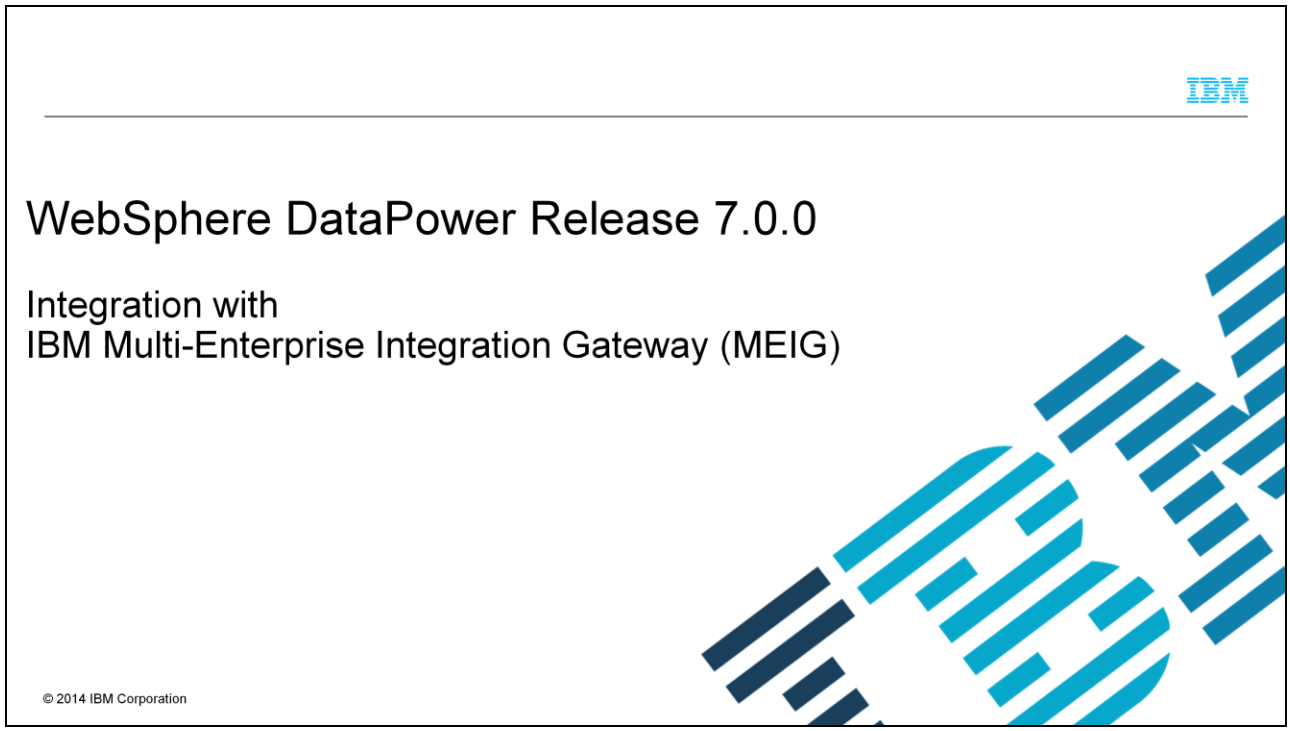


This presentation covers the integration with Multi-Enterprise Integration Gateway, a new feature in WebSphere® DataPower® firmware version 7.0.0.

Table of contents

This presentation gives you an overview of the integration with Multi-Enterprise Integration Gateway, or MEIG, and how to use it. The overview includes the use cases, architectural overview, and differences from existing DataPower XB functions. This presentation will also guide you through the configuration steps at both MEIG and DataPower, and also how to troubleshoot with visibility events.

IBM

Section

Overview of the integration with Multi-Enterprise Integration Gateway

The first section gives you an overview of the integration with Multi-Enterprise Integration Gateway, or MEIG.

Introduction

- What it is
  - An enhancement that enables DataPower Multi-Protocol Gateway to perform security enforcement of incoming AS2 messages in DMZ before forwarding the document to MEIG (MEIG).
    - This function is provided by MEIG AS2 Proxy Front Side Handler, which can be attached to a multi-protocol gateway. It is available on XB, XI, and XG.
    - To perform security enforcement, DataPower retrieves required information (exchange profiles) from MEIG.
  - DataPower generates and send visibility events to MEIG, allowing for troubleshooting.
- Why it is
  - To provide a seamless integration of B2B solutions between DataPower and MEIG, and to enable DataPower to perform security enforcement of incoming AS2 message in DMZ before forwarding the document to enterprise B2B messaging applications
- Who wants it
  - Customers who use both DataPower and MEIG.

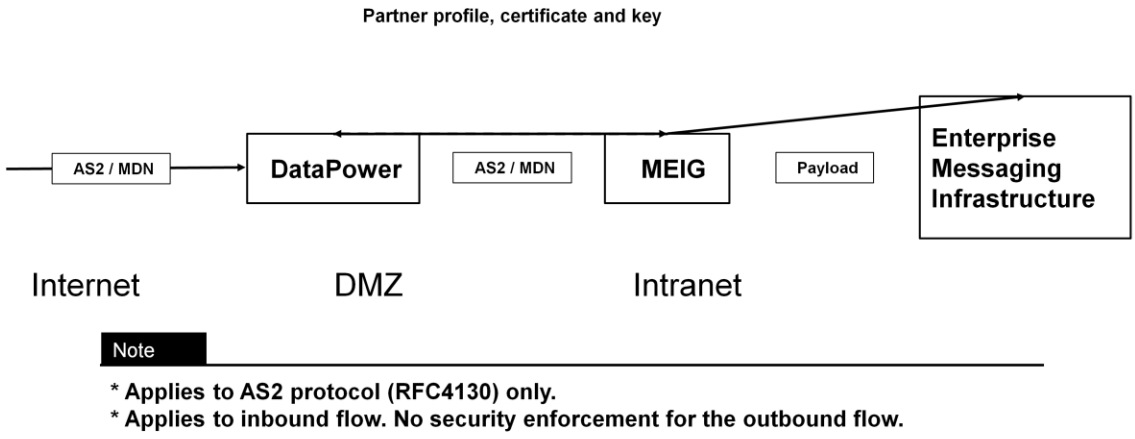
What it is? Integration with MEIG is a new feature added in WebSphere DataPower firmware version 7.0 that enables DataPower to perform security enforcement of incoming AS2 messages in DMZ before forwarding the document to MEIG. This feature is available on XB, XI and XG. The information needed to perform security enforcement, as known as “exchange profiles”, are retrieved from MEIG to DataPower. DataPower also generates and sends visibility events to MEIG for troubleshooting needs at the end of each transaction.

Why it is? With this feature, DataPower can integrate with MEIG regarding B2B solutions and help perform security enforcement of incoming AS2 messages in the DMZ.

Who wants it? Customers who use both DataPower and MEIG will benefit from this new feature.

Use case 1 for DataPower/ MEIG integration

Use DataPower as a DMZ B2B security proxy to decompress, decrypt and/or verify the signature of the incoming AS2 messages or MDNs based on the information provided by MEIG in the intranet. Only verified message will be passed to enterprise messaging infrastructure.



Note

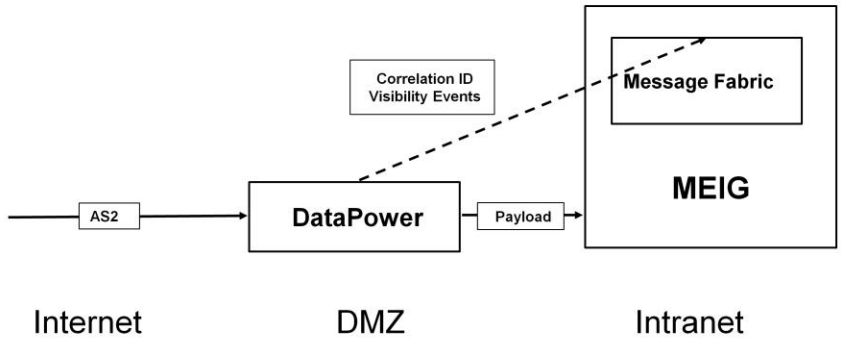
*** Applies to AS2 protocol (RFC4130) only.**
*** Applies to inbound flow. No security enforcement for the outbound flow.**

The first use case illustrates DataPower integration with MEIG. You can use DataPower as a DMZ B2B security proxy to decompress, decrypt and/or verify the signature of incoming AS2 messages or MDNs. The B2B Partner Profiles and required certificates and keys are obtained from MEIG in the Intranet. In this way, only verified messages will be passed to the enterprise messaging infrastructure in the Intranet.

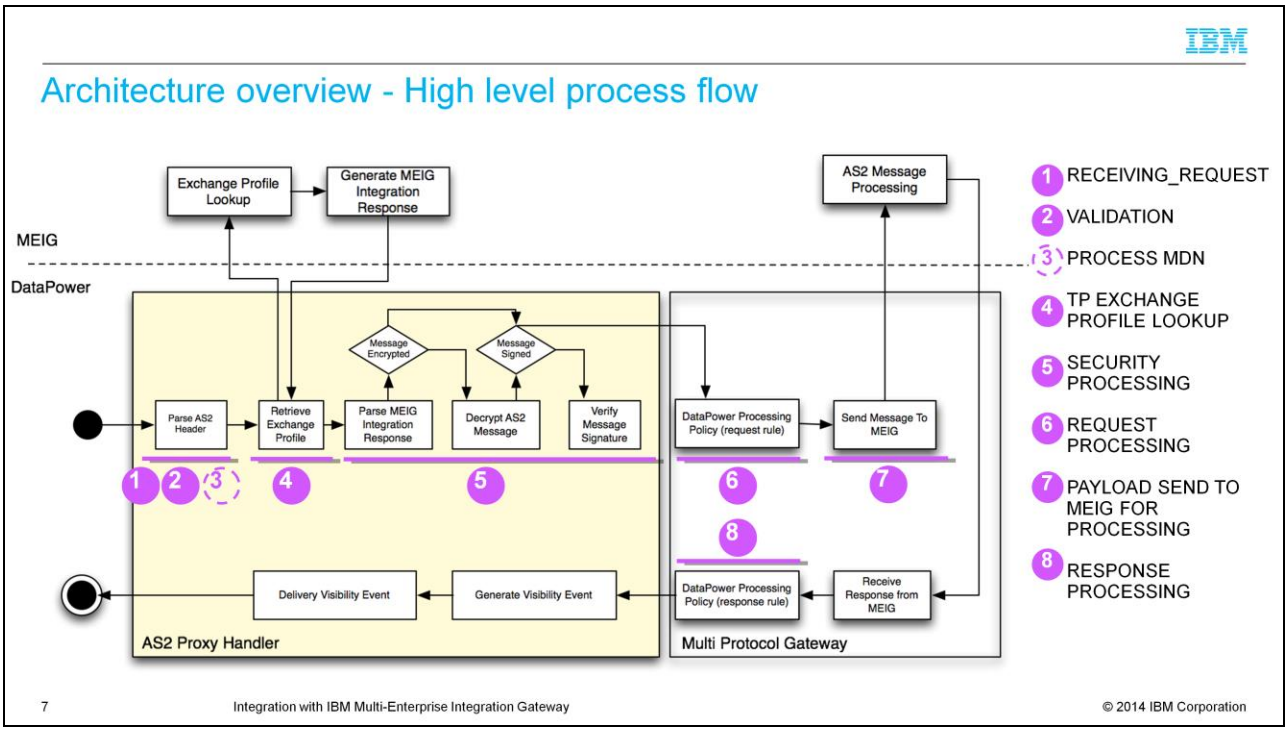
Please note that this feature currently applies to AS2 protocol (RFC4310) only. Also, this feature is performed for inbound flow. There is no security enforcement for the outbound flow.

Use case 2 for DataPower/ MEIG integration

Visibility events (historical transaction status) are available on MEIG so that the root cause of failure transactions can be easily identified.



The second use case for DataPower and MEIG integration is the correlation of transaction life cycle events. For each transaction, DataPower will generate a sequence of state events and send them to MEIG at the end of transaction. These events are associated with a correlation ID that is generated by DataPower to uniquely identify the transaction. When DataPower forward the AS2 message to MEIG, the correlation ID will be passed to MEIG along with the AS2 message. Combined with the events generated by MEIG, this allows administrator to correlate the events and identify the root cause of failure transactions.



This architecture overview illustrates the high level process flow between DataPower and MEIG for an incoming transaction.

When the AS2 Proxy Front Side Handler receives an incoming AS2 message in step 1, it parses the headers and validates the message according to its headers as in step 2.

If the incoming message is an MDN, the MDN is processed in step 3.

After the AS2 Proxy Front Side Handler acquires the required information regarding the transaction, it then asks for a matching exchange profile from MEIG via a RESTful API. MEIG lookups up the exchange profile and returns a response including the information required for security enforcement, as depicted in step 4.

Security enforcement is then performed in step 5, where the message is decrypted and its signature verified.

After the security enforcement, the payload is passed to the processing policy of Multi-Protocol Gateway for processing in step 6. Note that only request rules apply.

In step 7, the processed message is forwarded to MEIG.

In step 8, after the multi-protocol gateway receives response from MEIG, the response is passed into its processing policy for processing as well. Note that only response rules apply.

After steps 1 to 8 are performed, the MEIG AS2 Proxy Handler generates visibility events for the result of each step, and delivers the visibility events to MEIG in batch. This final

step allows users to troubleshoot the transaction at MEIG as well.

Differences from existing DataPower XB functions

- Available on XB, XI, and XG.
- The processing of AS2 messaging is stateless. Better scalability.
- The partner profiles, exchange profiles and crypto credentials are stored on MEIG.
- No AS2 termination by default. This makes DataPower acting as a transparent AS2 proxy to MEIG servers.

This page lists the differences of this new feature from existing DataPower XB functions.

First of all, this new feature is not limited to XB. The new AS2 Proxy Front Side Handler can be attached to multi-protocol gateway and is available on XB, XI, and XG.

In this new feature, the processing of AS2 messaging is stateless. Transaction metadata and message payloads are not persisted, and the AS2 MDNs are not generated on DataPower. This makes it relatively easy to scale.

The partner profiles, exchange profiles and crypto credentials are stored on MEIG, not on DataPower. This prevents partner profile from provisioning and synchronization issues.

Finally, the new AS2 proxy will not perform AS2 termination by default, which means MEIG can receive the original message headers and payload sent by external partner.

IBM

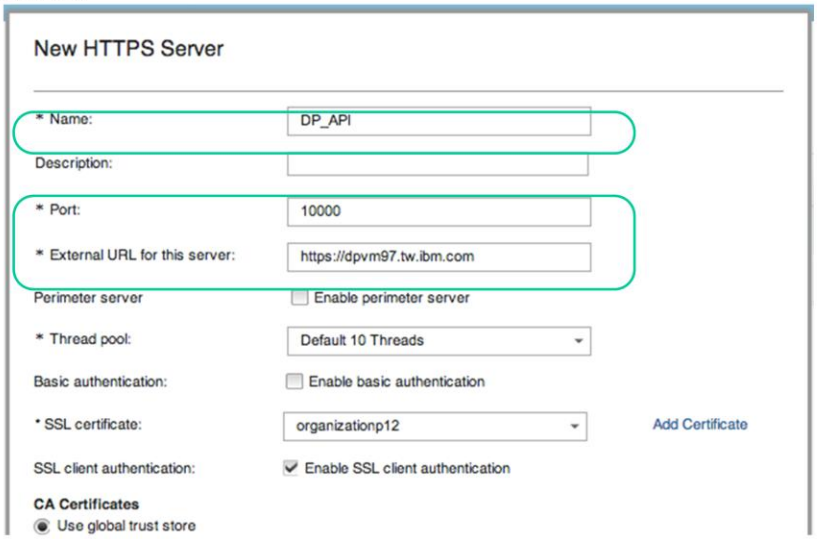
Section

How to use it

This section will tell you how to configure and troubleshoot the DataPower integration with MEIG.

Configure MEIG to integrate with DataPower (1 of 2)

1. Systems Management > HTTP/S Servers
2. New > HTTPS
3. Give it a “Name”
4. Set “Port” and “External URL for this server”



To enable the profile exchange between DataPower and MEIG, you have to setup an HTTPS Server at MEIG. Define the external URL and port here, so that DataPower can communicate with MEIG through RESTful API.

Configure MEIG to integrate with DataPower (2 of 2)

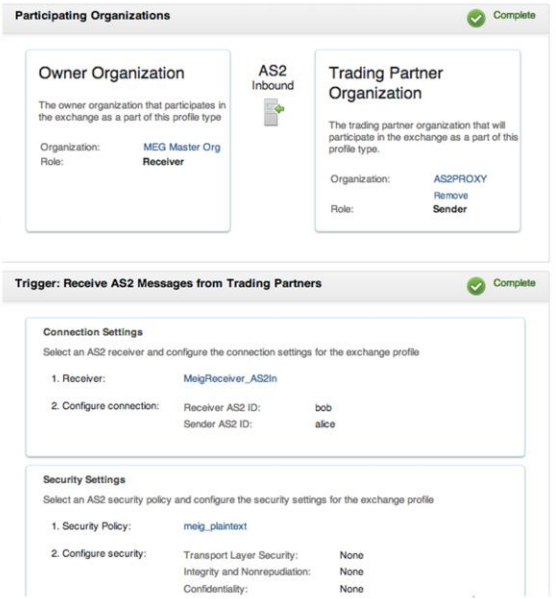
- Exchanges > Exchange Profiles
- New > AS2 Inbound
  - – Participating Organizations
  - – Trigger: Receive AS2 Messages from Trading Partners
    - Connection Settings

      Receiver: set “AS2 service URI” for example, “/meig_as2in"

      AS2 sender/receiver ID
    - Security Settings

      Security Policy

      Sign/Compress/Encrypt
  - – Action: Deliver Message Data
    - Message Destination
  - – Deploy Exchange Profile

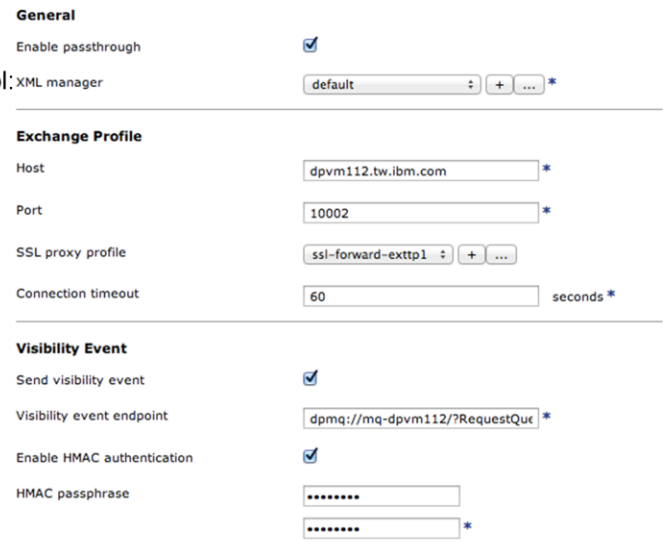


11 Integration with IBM Multi-Enterprise Integration Gateway

After you set up the https server at MEIG, you also have to define the security enforcement rules for trading partners. At the MEIG server, you can create an AS2 inbound exchange profile for a trading partner. In the exchange profile settings, you can define the AS2 sender and receiver ID; the security settings regarding whether the message should be signed, compressed, or encrypted; and where to deliver the message. DataPower will ask for this exchange profile for each incoming AS2 message. The above is an overview of the configuration at MEIG. The next two slides will guide you through the configuration at DataPower.

Configure DataPower to integrate with MEIG - MEIG connection info

- Multi-Protocol Gateway > add front side protocol: "MEIG AS2 Proxy Front Side Handler"
- Select " MEIG Server" tab
- AS2 Proxy Front Side Handler
  - General
    - Enable passthrough (default)
    - XML Manager
  - Exchange Profile
    - set "Local IP address" and "Port"
    - SSL proxy profile
    - Connection timeout
  - Visibility Event
    - Send visibility event (default)
    - Visibility event endpoint
    - HMAC settings



To configure DataPower to integrate with MEIG, you have to define the connection information in an "MEIG AS2 Proxy Front Side Handler" so that you can exchange profiles. You also have to attach this MEIG AS2 Proxy Front Side Handler to a multi-protocol gateway.

In the configuration GUI of AS2 Proxy Front Side Handler, switch to the "Multi-Enterprise Integration Gateway Server" tab. You can find three sections: the "General" section, the "Exchange Profile" section, and the "Visibility Event" section.

In the "General" section, you can decided whether to enable passthrough mode. We will describe this property in details in the next slide. You also have to configure an XML manager for the information exchange between DataPower and MEIG server.

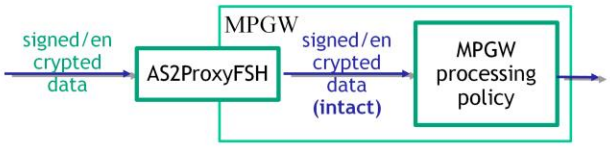
In the "Exchange Profile" section, you must fill in the host name and port of the MEIG server. You also have to specify an SSL proxy profile for securing the communication between DataPower and the MEIG server. And you can define the connection timeout seconds.

In the "Visibility Event" section, you can decided whether to send visibility events to MEIG. If you choose to send them, you will have to specify a URL to a visibility event endpoint. If MEIG sever requires HMAC to secure this communication, you have to enable HMAC authentication, and fill in the corresponding HMAC passphrase.

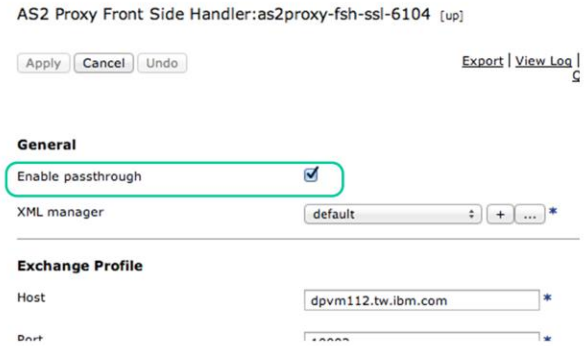
Configure DataPower to integrate with MEIG - Enable passthrough

The "**Enable passthrough**" property controls whether to pass the original AS2 requests to the processing policy of MPGW.

- When **enabled**, the AS2 proxy handler passes the original AS2 requests to MPGW processing policy.



- When **disabled**, the AS2 proxy handler first uses the cryptographic information provided by the exchange profile to decrypt the incoming AS2 requests and verify the signature. The AS2 proxy handler then passes the decrypted request body with signature removed to MPGW for processing.



This slide details the "Enable passthrough" property mentioned in the previous slide.

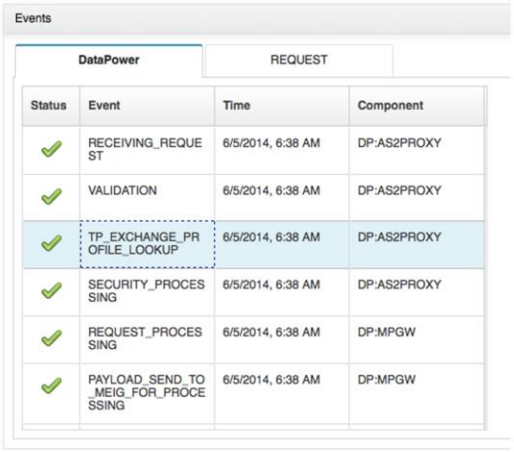
The "Enable passthrough" property controls whether to pass the original AS2 requests to the processing policy of Multi-Protocol Gateway.

When enabled, the MEIG AS2 Proxy Front Side Handler passes the original AS2 requests to Multi-Protocol Gateway processing policy.

When disabled, the MEIG AS2 Proxy Front Side Handler first uses the cryptographic information provided by the exchange profile to decrypt the incoming AS2 requests and verify the signature. The AS2 proxy handler then passes the decrypted request body with signature removed to Multi-Protocol Gateway for processing. For example, you can consider disabling this property if the incoming AS2 transactions do not require signed MDN. This property allows administrator to decide whether AS2 termination is required based on the use case.

Visibility events

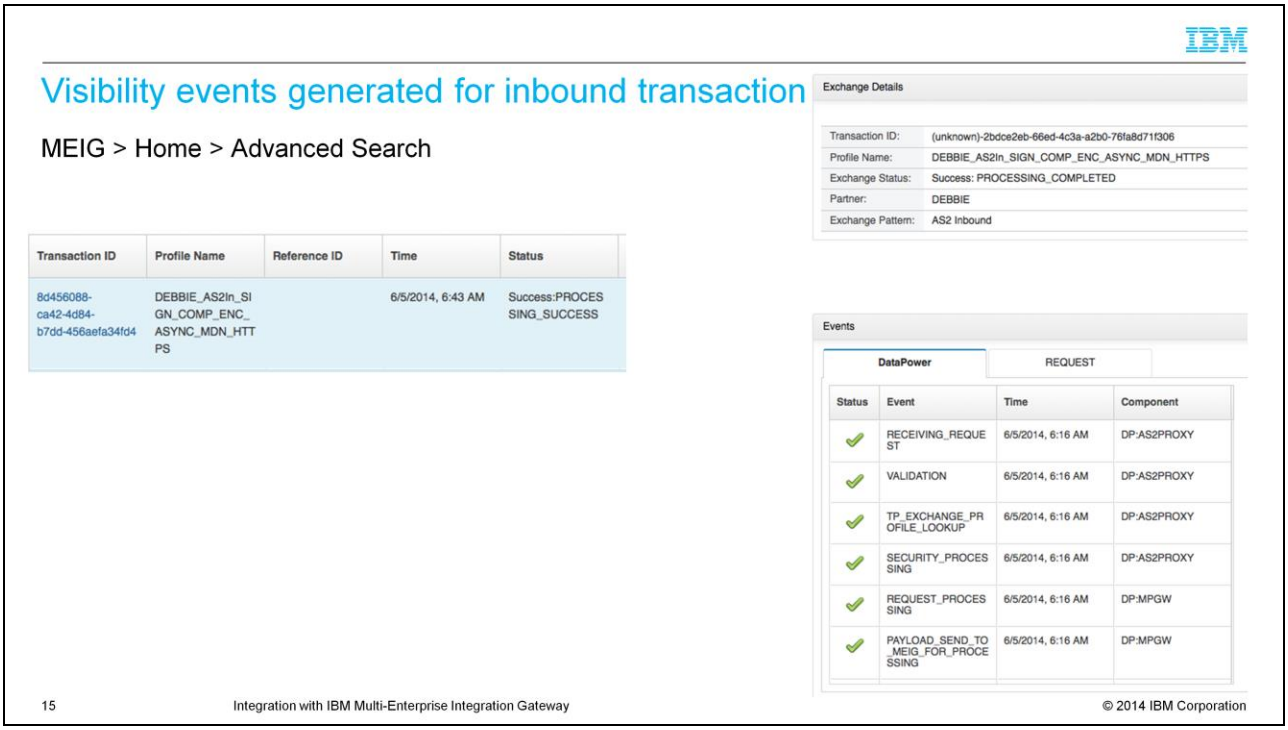
- Visibility events help users to understand and troubleshoot the transaction status for each B2B exchange.
- Users can view the events that take place in an exchange to validate document processing or to determine whether there were problems with the document exchange.
- DataPower generates visibility events to reflect the status of major stages in MEIG AS2 Proxy handler and attaching multi-protocol gateway. These events will then be sent to MEIG to be correlated with those generated by MEIG and to be displayed in one transaction thread.



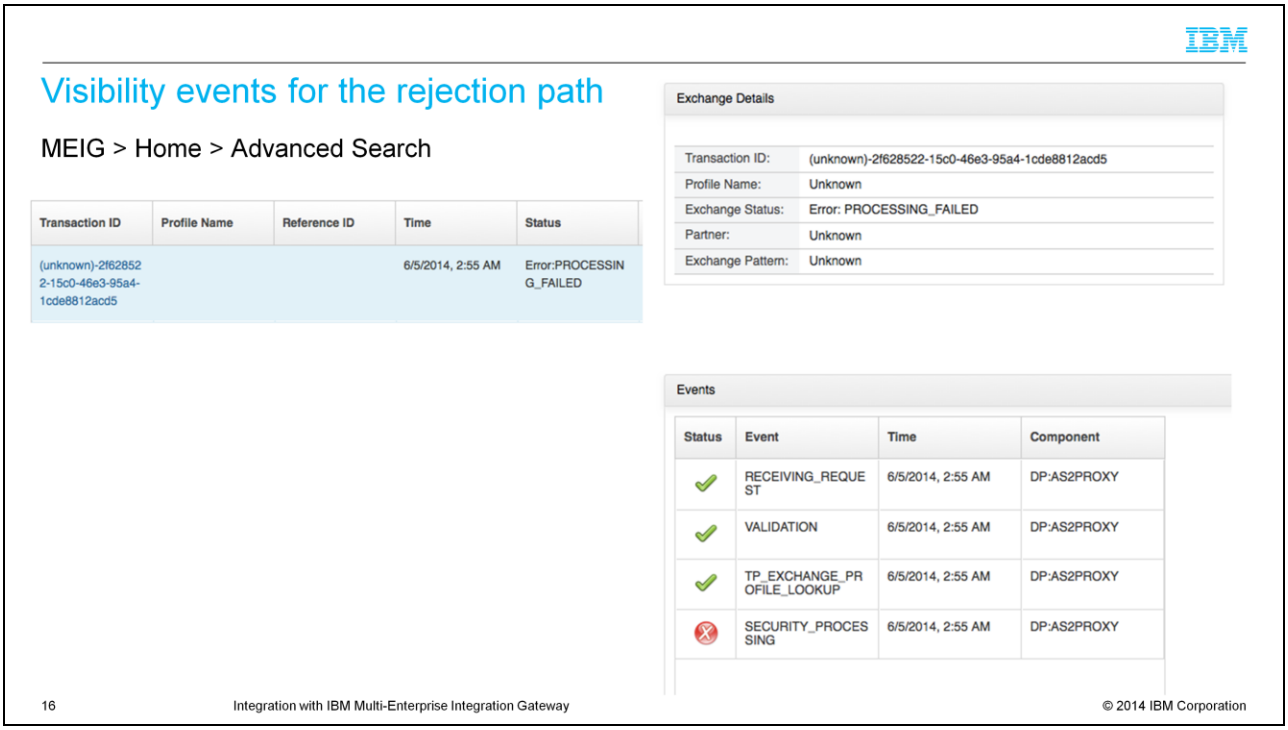
For troubleshooting, you can look at visibility events at MEIG to understand and troubleshoot the transaction status for each B2B exchange.

Users can view the events that take place in an exchange to validate document processing or to determine whether there were problems with the document exchange.

DataPower generates visibility events to reflect the status of major stages in MEIG AS2 Proxy handler and attaching multi-protocol gateway. These events will then be sent to MEIG to be correlated with those generated by MEIG and to be displayed in one transaction thread.



This slide shows the visibility events received at MEIG. You can see visibility events are generated for different stages of each transaction, allowing for troubleshooting.



This slide shows the visibility events received at MEIG for the rejection path. You can see the event fails at security processing stage. This is most likely due to the mismatch of security requirements between incoming message and the partner profile provided by MEIG server.

Trademarks, disclaimer, and copyright information