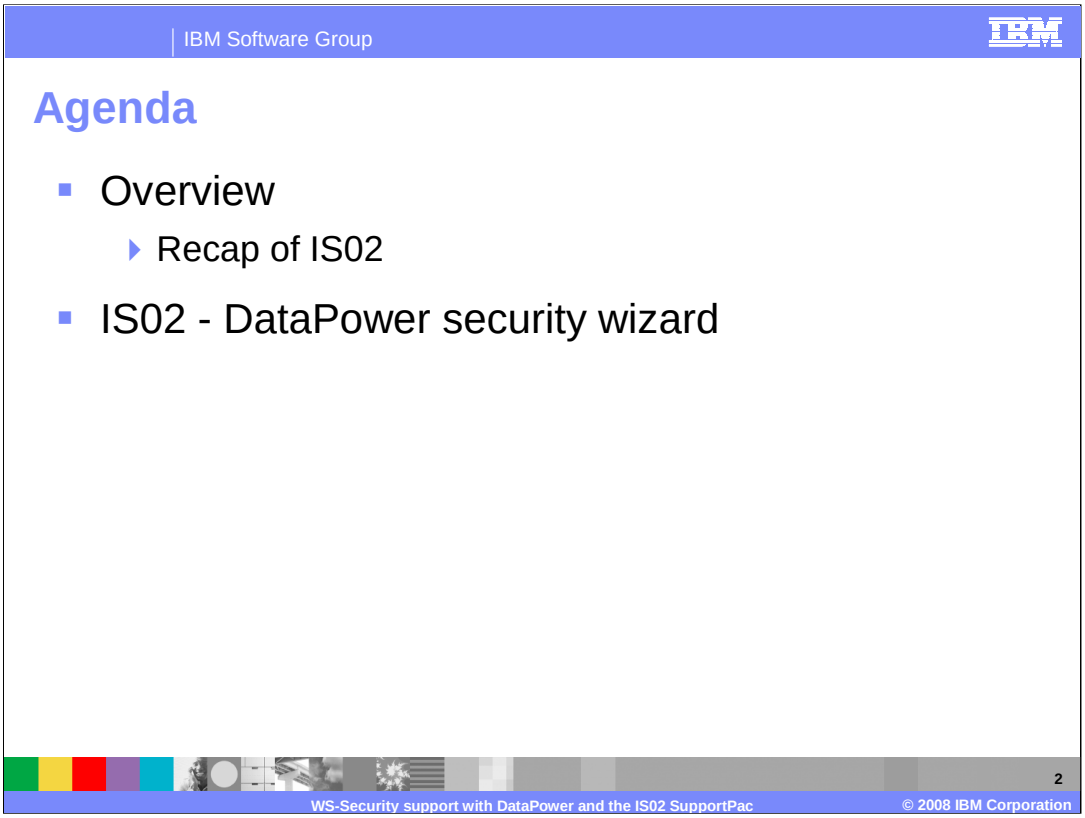
This presentation will discuss the “IS02” support pack, and describe how it can be used to complement the WS-Security function in WebSphere Message Broker Version 6.1 with the addition of the WebSphere DataPower system.

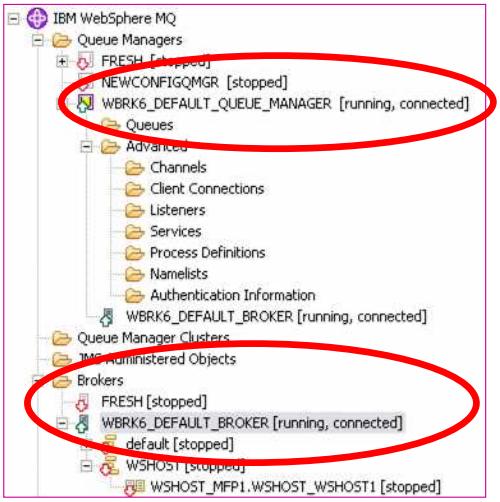


The presentation will first give a recap of the IS02 SupportPac, and how it can be used to administer the Message Broker runtime component.

It will then discuss the new functions in IS02, and show how the wizard has been enhanced to provide the ability to offload the WS-Security processing from the Message Broker.

Integrated WebSphere MQ and Message Broker administration (IS02)

- Automatic discovery of local brokers
- Create, delete, start and stop
  - Local brokers
  - Execution groups
  - Flows
- Multiple deploy of BAR's to execution groups
- Shipped with default configuration wizard from Message Broker version 6
- Shipped with complete Message Broker documentation
- IS02 SupportPac
  - Production ready



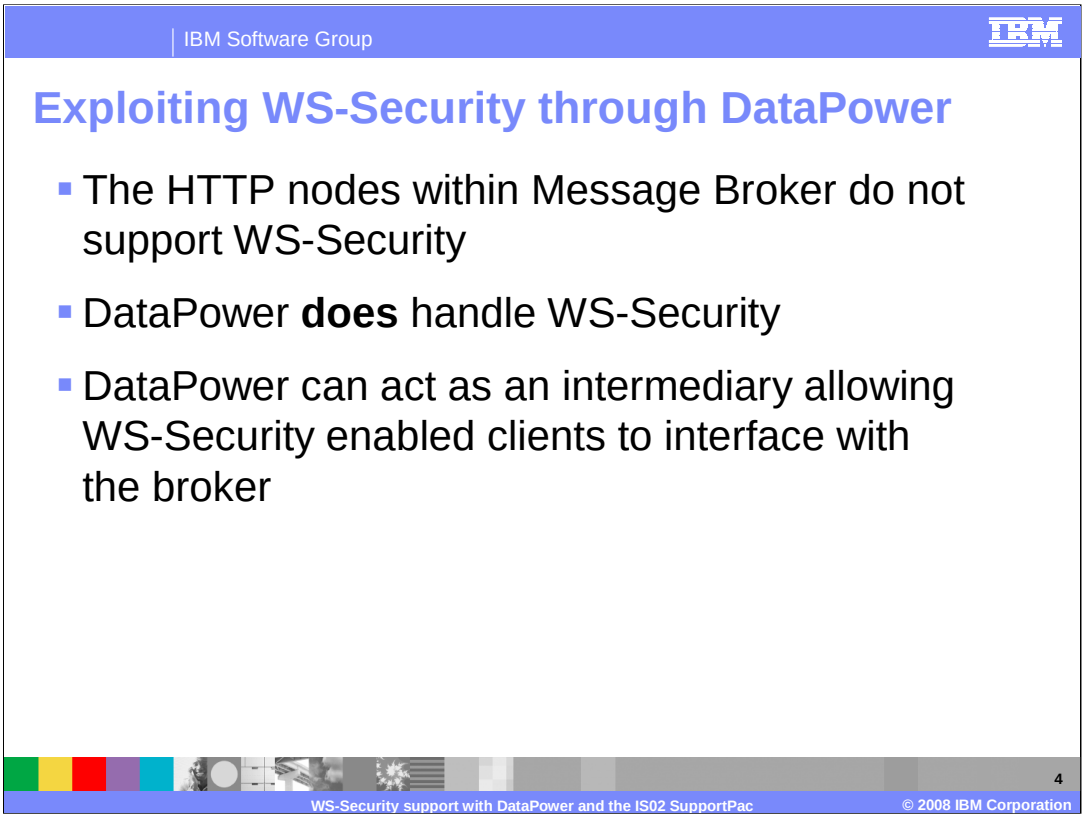
The IS02 SupportPac is a plug-in to the WebSphere MQ Explorer, based on Eclipse. The support pack provides the same capability as the Administration Perspective in the Message Broker Toolkit. Using this plug-in you can perform all administration functions on your Message Broker instances, such as starting and stopping message flow and execution groups, and deploying new instances of broker artifacts.

Since this is a plug-in to the MQ Explorer, the tool therefore provides a single view of all defined queue managers and broker instances.

You can deploy a bar file to multiple execution groups.

The IS02 plug-in understands the relationships between the queue managers and the brokers, and the queue manager display will also show any associated broker or Configuration Manager details. It also understands the resource dependencies, so will prevent deletion of a queue manager used by a broker.

IS02 is a category 3 SupportPac, which means that it is fully supported. You can open PMRs against this support pack in the event of a suspected defect.



This slide explains why it may be appropriate to consider the use of the DataPower system in conjunction with Message Broker.

Although the new SOAP nodes in version 6.1 do support WS-Security, this function is not available if you are using the HTTP nodes. If you are going to use the HTTP nodes for Web services in conjunction with WS-Security, then you will need to handle the security components processing outside the Broker environment. The DataPower system can act in this role, and Web service clients will connect to this intermediary for security processing.

IBM DataPower appliance product line

XML Accelerator XA35

- Accelerates XML processing and transformation
- Increases throughput and reduces latency
- Lowers development costs

XML Security Gateway XS40

- Help secure SOA with XML threat protection and access control
- Combines Web services security, routing and management functions
- Drop-in, centralized policy enforcement
- Easily integrates with exiting infrastructure and processes

Integration Appliance XI50

- Transforms messages (Binary to XML, Binary to Binary, XML to Binary)
- Bridges multiple protocols (MQ, HTTP, JMS)
- Routes messages based on content and policy
- Integrates message-level security and policy functions

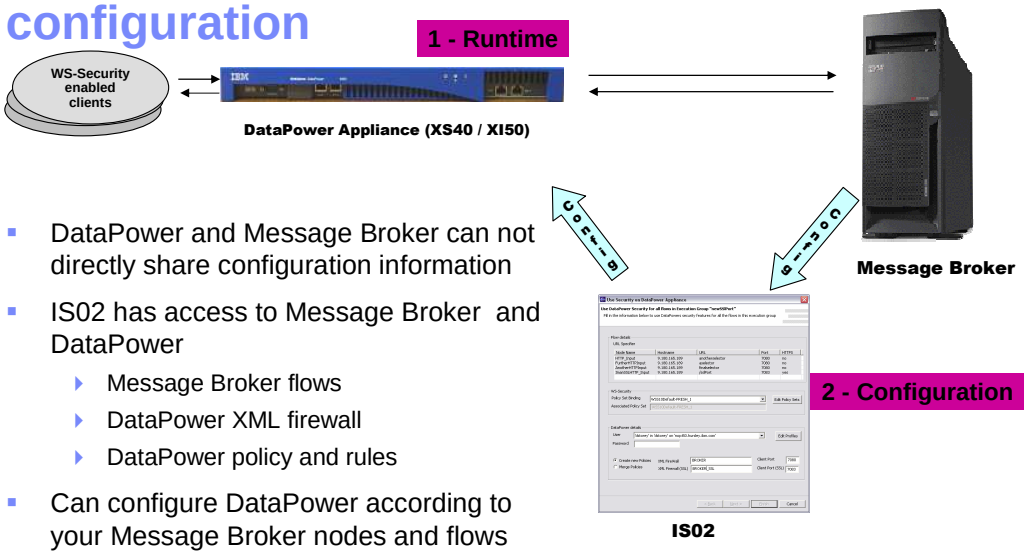
This slide gives a summary of the key DataPower systems.

The XA35 system is used to provide high-capacity XML processing and parsing capability.

The XS40 system provides security capability, including security for Web services, with WS-Security.

The XI50, in addition to providing the capability of the XA35 and XS40, provides the ability to convert between data formats, and to convert between network protocols.

IS02 enhancements for DataPower configuration



- DataPower and Message Broker can not directly share configuration information
- IS02 has access to Message Broker and DataPower
  - Message Broker flows
  - DataPower XML firewall
  - DataPower policy and rules
- Can configure DataPower according to your Message Broker nodes and flows using the DataPower security wizard within IS02

This slide represents the high-level architecture that is appropriate when using the DataPower system in conjunction with Message Broker.

The top part of this slide represents the runtime components, shown as number 1 on the slide. If the Web service client connects directly to the HTTP nodes in Message Broker, then no WS-Security will be possible. Instead, the Web service client connects directly to the DataPower appliance, where security checking is performed. Once the client request has been authenticated, the request is passed through to the Message Broker system. The DataPower system will perform decryption of the SOAP message, and then send the unencrypted message to the Message Broker.

For the reply, Message Broker will send the response message in unencrypted format to the DataPower system. This will encrypt the message and send it on to the originating client.

A typical configuration for this scenario will have the Message Broker system located behind the firewalls. The DataPower system may, however, be located within the DMZ.

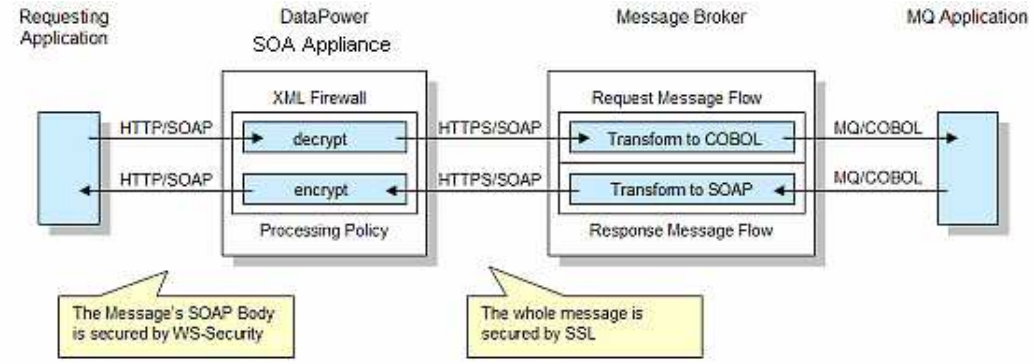
The configuration of this environment is achieved using the IS02 support pack, shown as number 2 on this slide.

The IS02 support pack can communicate with both the Message Broker configuration, and with the DataPower system. It takes information from message broker regarding the Flows and HTTP Nodes, including HTTP/S port numbers and uses this to create a configuration in DataPower to allow the two products to work together.

DataPower can be configured to be used with Message Broker without the need for IS02. However, this is a manual task, and requires specific knowledge of the DataPower system and configuration tools.

This approach can only be used with the XS40 or XI50 models of the DataPower system.

Configuring DataPower for use with Message Broker



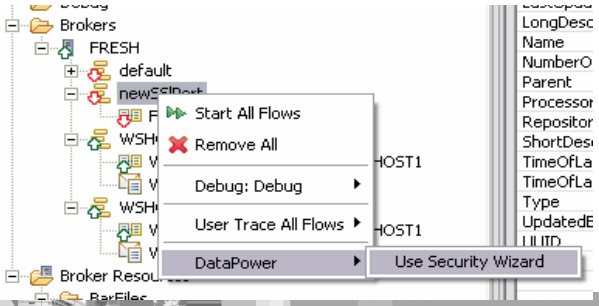
This slide shows the path of a Web service request, secured with WS-Security.

The body of the SOAP message has been secured using WS-Security processing and therefore must be decrypted before it can be processed within the message flow. A DataPower appliance is used as a front-end security gateway to decrypt the body of the SOAP message on the way into the message flow. The DataPower appliance is also used to encrypt the output message from the message flow before the reply is sent to the requesting application.

For a DataPower appliance to perform WS-Security processing, you must first create a firewall within it. This requires administration and information from both the Message Broker message flow and the DataPower appliance. You can perform this administration manually on the DataPower appliance, or you can use the DataPower security wizard, contained in the IS02 Message Broker plug-in.

Use of the IS02 DataPower plug-in

- Requires a user-name, password and domain on their DataPower appliance
- Requires certificates and crypto profiles available on the DataPower appliance in their domain. (For SSL, decryption and encryption)
- Does not need to administer the DataPower appliance directly
  - All configuration done using the DataPower security wizard



Configuration of the DataPower system is started from the IS02 support pack.

Before this is done, you must ensure that you have access to the administration functions of the DataPower system. This means that user-name and password are required, plus knowledge of the DataPower domain.

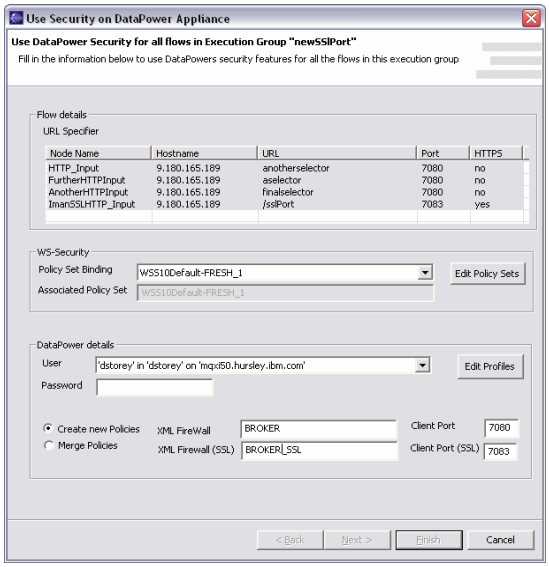
Secondly, if performing encryption and decryption or SSL processing, the DataPower system must be configured with the necessary certificates and crypto profiles.

To start the wizard, open the IS02 Eclipse window, and select the target execution group within the target broker. Right-click the execution group, and select the DataPower action, then start the wizard.

If you cannot see this menu option, select **Windows, Preferences, Broker Explorer, DataPower** and make sure that the **Display DataPower** menu box is checked in the Broker Explorer.

DataPower security wizard – Main window

- Interacts with your Message Broker server
  - Retrieves all HTTP message flow input nodes
  - Shows information about defined policy sets



This screen capture shows the three main categories of information.

First, the Flow Details

This shows information retrieved by the wizard for the selected message flows. The information shown is a list of HTTPS node names, the host name on which they are configured, and the URL which they service. It also includes the port on which the listener is configured, and whether the node supports SSL. In this example a single HTTP input node named HTTP_Input is available in the execution group “WS-HOST”.

Second, the WS-Security information.

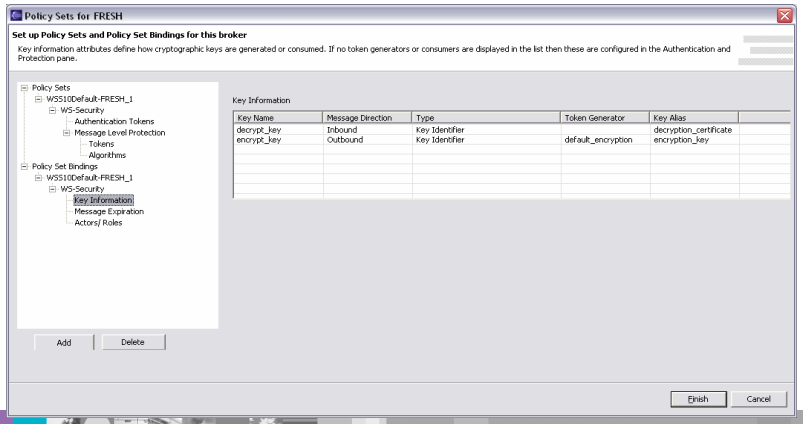
This shows which policy set binding and policy set are to be used. A default policy set and policy set binding are created when the wizard is first used with the name conforming to the template as shown. The name structure is set and cannot be changed. As the broker in this example is called FRESH, the policy set binding name reflects this name. You can edit the policy sets if needed.

Finally the DataPower details

This shows the information needed to use the DataPower appliance, including user-name, domain, and XML firewall name. When the wizard is first invoked, you are prompted to supply the username and domain that you will be using on the DataPower appliance.

DataPower security wizard: Policy sets editor

- A Policy Set is used to configure the WS-Security aspects of your encryption and decryption rules
  - Define the WS-Security for your decryption and encryption actions using the key information table in your policy set bindings
  - Subset of capability provided for the SOAP nodes
  - Supports (whole body) message level encryption and decryption

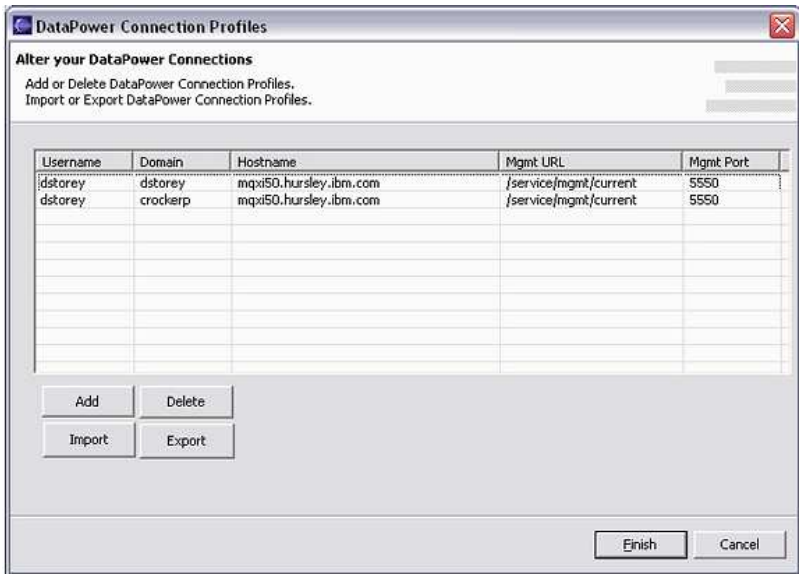


Clicking the “Edit Policy Set” button opens the policy set editor, shown on this screen capture. This is a subset of the Message Broker policy set editor, which is discussed in the IEA presentation covering WS-Security.

You can alter the default policy set and policy set binding pairs or add your own. Each policy set binding has an associated policy set. The important part for encryption and decryption is the key information table specified within the policy set bindings.

The outbound key defines the encryption rules, while the inbound key defines the decryption rules. The Token Generator column points to the message level protection token, which specifies additional WS-Security parameters. After you have created your policy set and binding, click **Finish** to return to the Security wizard.

DataPower connection profiles



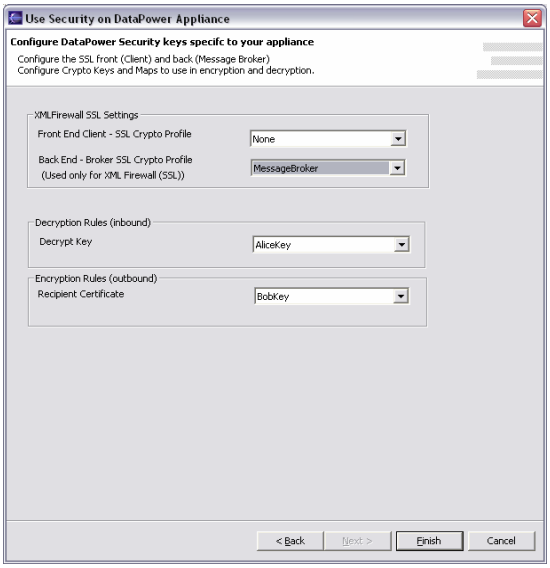
On the main window in the wizard, click the DataPower “edit Profiles” button. This will open a window similar to the screen capture shown on this slide.

You can add, delete, import, and export sets of connection details. Select **Add** to add a new row and then click on the cells in the row to change the values to your connection values. Click **Finish** to save the profile within the IS02 Explorer Toolkit. This will appear in a drop-down list in the Security wizard in subsequent invocations.

Click Finish to return to the main wizard screen.

DataPower security wizard editor

- Interacts with your DataPower appliance
  - Retrieves crypto profiles for SSL communications
  - Retrieves encryption and decryption certificates



From the original IS02 wizard screen, after entering your security credentials, and clicking next, this screen will be shown.

At this point, the wizard has connected to the DataPower system, and has retrieved the Crypto profiles and encryption and decryption certificates, within your DataPower domain.

The SSL Front End Client setting value is used to configure the SSL profile, which client application programs use to connect to the DataPower appliance.

The Back End Broker SSL setting is used to configure your back-end connection for communication from the DataPower appliance to Message Broker. This option is available only if you are using SSL between the broker and the DataPower appliance, which is not used when connecting to Message Broker.

The Decryption and Encryption drop-down boxes are used to configure the decryption and encryption keys in your request and reply rules. Select the required keys for decryption and encryption of the message. In this case, “Alice-Key” is used to decrypt the SOAP message received by the DataPower appliance, and “Bob-Key” is used to encrypt the reply message to the requesting application. These are the names of crypto profiles that have been defined on the DataPower appliance.

On this window, click Finish to transmit the updated configuration to the DataPower system, and then return to the main wizard screen.

DataPower firewall created by security wizard

- Up to two DataPower firewalls created
  - One firewall for HTTP input nodes
  - One firewall for HTTPS input nodes
- Front and back HTTP ports set
- IP address of the Message Broker listener is configured

After you click **Finish** in the main window, several artifacts are created on the DataPower system.

These are:

First, the DataPower XML firewalls -- one for HTTP Input Nodes per broker and one for HTTPS Input Nodes per broker.

Second, a DataPower policy for each DataPower XML firewall.

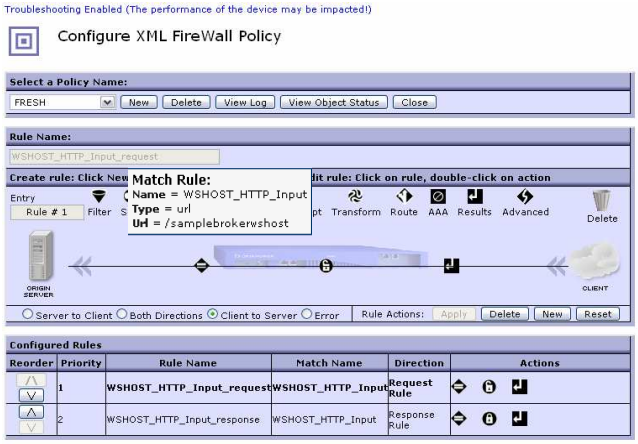
And third, a series of reply and request rules for each HTTPS Input Node that you selected.

In addition, if you have a WS-Security policy set binding selected, each request rule will have a matching action matching the HTTPS Input Node selector and a decryption rule.

Each reply rule will have a matching action matching the HTTPS Input Node selector and an encryption rule.

This screen capture shows an example of the resulting configuration that is created within the DataPower system.

DataPower policy created by security wizard



- Each DataPower firewall has an associated DataPower Policy
- Two rules created per HTTP or HTTPS input node each with the appropriate match rule
  - Request Rule (inbound)
  - Response Rule (outbound)
- Ability to merge rules with existing DataPower Policy and DataPower Firewall
  - Rules are added to the DataPower policy.
  - No changes are made to the DataPower firewall

This example shows a DataPower policy that has been created using the wizard.

The schematic in the center of the screen shows the client to server connection. Note that the client is shown on the right side of this window.

Two rules have been created. A request rule for inbound messages and a response rule for outbound messages. Two rules are created for each HTTP input.

The request rule will decrypt the message, and the response rule will encrypt the message.

At the bottom of the screen capture, the encrypt and decrypt keys are shown.

It is possible to add rules to an existing policy at a later time.

DataPower Message Broker articles available on IBM developerWorks® (circa July 2007)

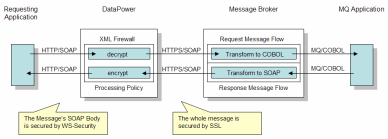
Integrating DataPower with WebSphere Message Broker

Peter Crocker
30/04/07

Integrating

Overview

The following diagram illustrates the scenario that is described within this document.



The requesting application communicates to a DataPower box using SOAP over HTTP where the message body is encrypted with the WS-Security standard. The DataPower box decrypts the body of the message is receives. This content is then passed to Message Broker over a connection secured over HTTPS. Message Broker receieves the SOAP message and transforms this to a COBOL structure for the final MQ application. The responses then flow back in a similar fashion. The Message Broker and MQ Application is an instance of the WSHost sample that is provided with the product.

The initial configuration uses simple HTTP between DataPower and Message Broker. The modifications to use HTTPS are performed as a second stage of the configuration within this document.

Configuration

The following details the configuration of DataPower. The relevant externals that Message Broker presents to DataPower are also detailed.

Integrating DataPower with WebSphere Message Broker using the Broker Explorer (IS02 Support Pac)

Dominic Storey
Peter Crocker
23/05/07

Overview

This article describes how to use the DataPower security wizard within the Broker Explorer support pac to configure your DataPower appliance to handle the WS-Security for your HTTP(S) Input Nodes.

The working scenario here is based on the developerWorks article "Integrating DataPower with WebSphere Message Broker". This article should be seen as a partner to that article and that article should be read as a pre- requisite of this article.

DataPower Setup

To get a complete and working scenario there are several tasks which need to be completed by a DataPower administrator before a Message Broker user can configure the appliance to handle their HTTP(S) Input nodes.

1. You need to have a userid, password and domain configured on the DataPower appliance.

2. If you are using SSL to communicate to the Broker or to a client then the DataPower administrator must make sure that the SSL Crypto Certificates and Validation Credentials are set up and available to your domain. (For further details see the "SSL Enabling HHTP for Message Broker" section in "Integrating DataPower with WebSphere Message Broker")

3. If you want to use the DataPower appliance to encrypt or decrypt then you must have the required Crypto Certificate available on the DataPower appliance in your domain.

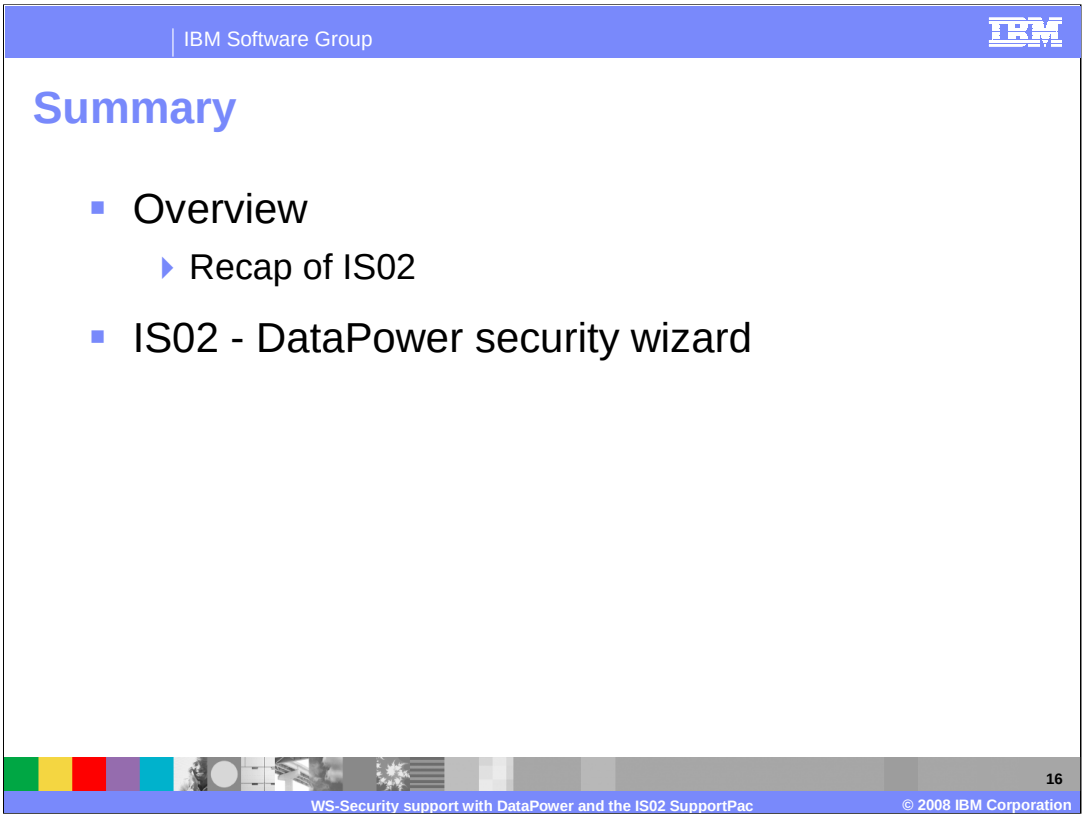
Using the Security Wizard

You run the security wizard by right clicking either an execution group or a message flow in the Brokers tree within the Broker explorer and selecting DataPower -> Security Wizard. If you cannot see this menu option check that you have the "Display DataPower menus" box checked in the "Windows -> Preferences -> Broker Explorer -> DataPower".

http://www.ibm.com/developerworks

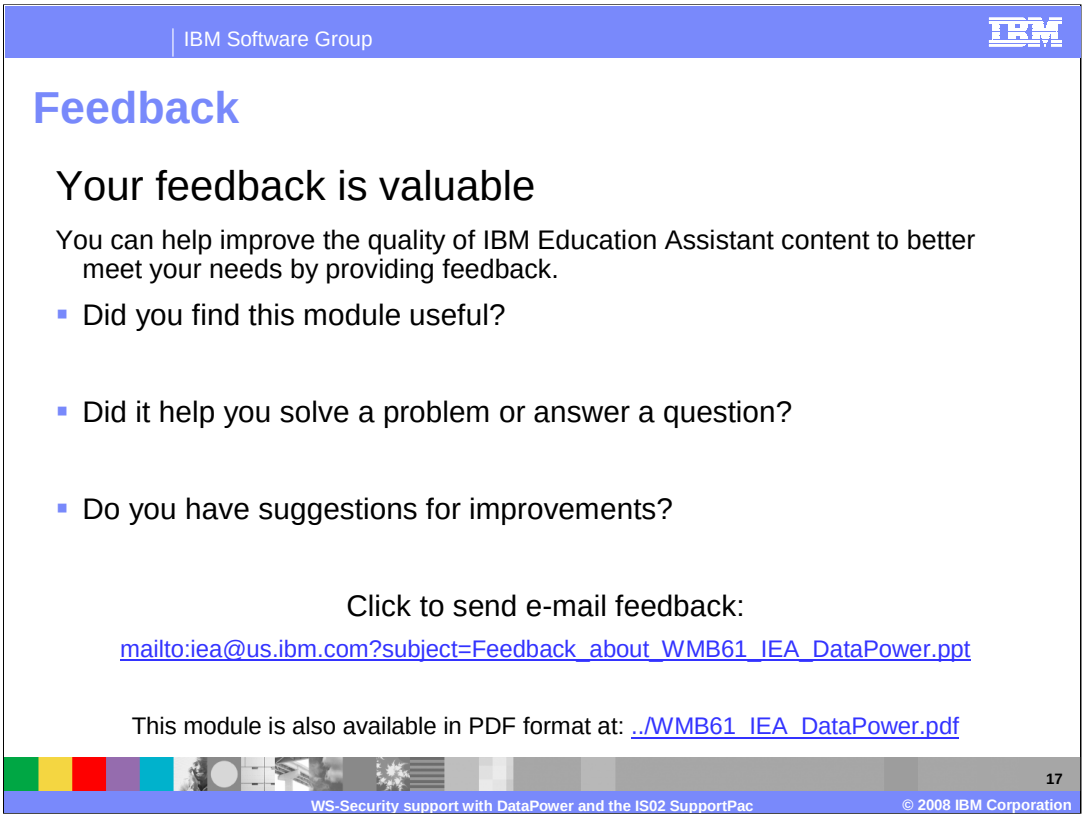
This implementation has been fully described in several articles published on IBM DeveloperWorks. These can be found by using the Web address shown on this slide.

Select the WebSphere category, and use the search criteria "Message Broker DataPower".



In summary, this presentation has given a brief overview of the capabilities of the DataPower system, and how it can be used in conjunction with Message Broker.

It then showed how the IS02 support pack can be used to configure that DataPower system, and showed an example of the wizard used to do this.



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

developerWorks DataPower IBM SupportPac WebSphere

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.