iWay

iWay Adapter for HIPAA for BEA WebLogic User's Guide
Version 5 Release 5

October 15, 2004
DN3501516.1004

Preface

This documentation describes how to use the iWay Adapter for HIPAA for BEA WebLogic. It is intended for developers to enable them to parse, transform, validate, store, and integrate healthcare information into the existing enterprise and pass information electronically, to partners, in HIPAA mandated form.

How This Manual Is Organized

The following table lists the numbers and titles of the chapters for this manual with a brief description of the contents of each chapter.

Chapter/Appendix		Contents
1	HIPAA and the iWay Adapter for HIPAA for BEA WebLogic	Explains the mandate of the Health Insurance Portability and Accountability Act (HIPAA) and describes how the components of the iWay Adapter for HIPAA for BEA WebLogic streamline the flow of information.
2	Creating XML Schemas or Web Services for the iWay Adapter for HIPAA for BEA WebLogic	Describes how to use iWay Servlet Application Explorer to create XML schemas or Web services for the iWay Adapter for HIPAA for BEA WebLogic.
3	Listening for Events in HIPAA	Describes how to use iWay Servlet Application Explorer to listen for events for the iWay Adapter for HIPAA for BEA WebLogic.
4	Using Web Services Policy-Based Security	Describes how to configure Web services policy-based security.
5	Management and Monitoring	Describes how to use managing and monitoring tools provided by iBSE and JCA to gauge the performance of your run-time environment.
A	Using Application Explorer in BEA WebLogic Workshop	Describes how to use iWay Java Swing Application Explorer running in BEA WebLogic Workshop to create XML schemas for HIPAA.

Documentation Conventions

The following table lists the conventions that apply in this manual and a description of each.

Convention	Description
`THIS TYPEFACE` or `this typeface`	Denotes syntax that you must enter exactly as shown.
`this typeface`	Represents a placeholder (or variable) in syntax for a value that you or the system must supply.
`underscore`	Indicates a default setting.
this typeface	Represents a placeholder (or variable) in a text paragraph, a cross-reference, or an important term.
this typeface	Highlights a file name or command in a text paragraph that must be lowercase.
this typeface	Indicates a button, menu item, or dialog box option you can click or select.
Key + Key	Indicates keys that you must press simultaneously.
`{ }`	Indicates two or three choices; type one of them, not the braces.
`|`	Separates mutually exclusive choices in syntax. Type one of them, not the symbol.
`...`	Indicates that you can enter a parameter multiple times. Type only the parameter, not the ellipsis points (…).
`.` `.` `.`	Indicates that there are (or could be) intervening or additional commands.

Related Publications

Visit our World Wide Web site, http://www.iwaysoftware.com, to view a current listing of our publications and to place an order. You can also contact the Publications Order Department at (800) 969-4636.

Customer Support

Do you have questions about the iWay Adapter for HIPAA for BEA WebLogic?

If you bought the product from a vendor other than iWay Software, contact your distributor.

If you bought the product directly from iWay Software, call Information Builders Customer Support Service (CSS) at (800) 736-6130 or (212) 736-6130. Customer Support Consultants are available Monday through Friday between 8:00 a.m. and 8:00 p.m. EST to address all your iWay Adapter for HIPAA for BEA WebLogic questions. Information Builders consultants can also give you general guidance regarding product capabilities and documentation. Please be ready to provide your six-digit site code (*xxxx.xx*) when you call.

You can also access support services electronically, 24 hours a day, with InfoResponse Online. InfoResponse Online is accessible through our World Wide Web site, http://www.informationbuilders.com. It connects you to the tracking system and known-problem database at the Information Builders support center. Registered users can open, update, and view the status of cases in the tracking system and read descriptions of reported software issues. New users can register immediately for this service. The technical support section of www.informationbuilders.com also provides usage techniques, diagnostic tips, and answers to frequently asked questions.

To learn about the full range of available support services, ask your Information Builders representative about InfoResponse Online, or call (800) 969-INFO.

Help Us to Serve You Better

To help our consultants answer your questions effectively when you call, please provide the following information:

- Your six-digit site code number (*xxxx.xx*).
- Your software configuration.

The following table lists the information to provide about your software configuration.

	Version-Build Date	**HF/Service Pack**	**Patches**	**OS**	**Java Version**
iWay Product					
Third-party Application Server					
EIS (adapter target)					

Note: For the EIS, ensure you record the application or database name and release level, including minor versions, for example, 4.6.1.

- The exact nature of the error or problem, specified as follows:
  - Steps to reproduce the problem.
  - Problem description (be as specific as possible).
  - Error message(s).
- To best define the problem, provide the following:
  - Screen captures of the error
  - Error output files
  - Trace files and log files
  - Log transaction
  - XML schemas and/or document instances
  - Other input documents (for example, transformations)

- Configuration files (all are applicable):

  .xch files

  config.xml file

  base.xml file

  repository.xml file

  ibserepo.xml file

  .dic files

  .rules files

- Environment variable settings:

  IWAY55

  IWAY55OEM

  CLASSPATH

  JAVA_HOME

  ACBDIR

  CBDIR (UNIX)

- Has the process, procedure, or query ever worked in its current form? Has it changed recently? If so, how (provide specific details)? How often does the problem occur?
- Can this problem be reproduced? If so, how? Can it be consistently reproduced?
- Have you tried to reproduce your problem in the simplest form possible?
- Do you have a trace file?
- How is the problem affecting your business? Is it halting development or production?
- Do you just have questions about functionality or documentation?

User Feedback

In an effort to produce effective documentation, the Documentation Services staff welcomes your opinions regarding this manual. Please use the Reader Comments form at the end of this manual to communicate suggestions for improving this publication or to alert us to corrections. You also can go to our Web site, http://www.iwaysoftware.com and use the Documentation Feedback form.

Thank you, in advance, for your comments.

iWay Software Training and Professional Services

Interested in training? Our Education Department offers a wide variety of training courses for iWay Software and other Information Builders products.

For information on course descriptions, locations, and dates, or to register for classes, visit our World Wide Web site, http://www.iwaysoftware.com or call (800) 969-INFO to speak to an Education Representative.

Interested in technical assistance for your implementation? Our Professional Services department provides expert design, systems architecture, implementation, and project management services for all your business integration projects. For information, visit our World Wide Web site, http://www.iwaysoftware.com.

Contents

CHAPTER 1

HIPAA and the iWay Adapter for HIPAA for BEA WebLogic

Topics:

- Mandating HIPAA
- Promoting HIPAA Compliance and Integration
- Transforming Data
- Installation Notes for the HIPAA Websphere MQ Integrator Developer Suite
- Introducing the iWay Adapter for HIPAA
- The iWay Adapter for HIPAA Toolkit
- Deployment Information for the iWay Adapter for HIPAA

The US Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) to reform the health insurance market. HIPAA simplifies the healthcare administration and financial processes by adopting national uniform standards for the electronic transmission of health information. The iWay Adapter for HIPAA, which is based on these standards, promotes the comprehensive integration and support of over 200 enterprise data and application systems.

The iWay Adapter for HIPAA streamlines this very complex flow of clinical and administrative information by providing seamless integration and access to data on disparate platforms with differing communication protocols, database structures, APIs, user interfaces, and security frameworks. This protects the investment in legacy applications and databases, as well as packaged customer relationship management (CRM), enterprise resource planning (ERP), and supply chain management (SCM) applications.

Mandating HIPAA

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, known as HIPAA) includes a provision for Administrative Simplification, which requires the Secretary of the Department of Health and Human Services to adopt standards to support the electronic exchange of administrative and financial healthcare transactions, primarily between healthcare providers and plans. HIPAA mandates the adoption of standards for such transactions and specifications for implementing each standard. The iWay Adapter for HIPAA is based on the October 1998 ASC X12 standards, referred to as Version 4, Release 1, Sub-release 0 (004010).

Achieving Administrative Simplification

Administrative Simplification is a method of making business practices (billing, computer systems, and communication) uniform so that providers and payers can easily interact with each other through one another's proprietary systems.

The Administrative Simplification provisions of HIPAA are intended to standardize forms and methods of completing claims, and other payment-related documents, and to use a universal identifier for providers of healthcare. Another goal is to increase the use and efficiency of computer-to-computer methods of exchanging healthcare information.

HIPAA addresses the following areas of Administrative Simplification:

- **Electronic Data Interchange (EDI)** is the electronic transfer of information in a standard format between trading partners. It enables partners to exchange information and transact business in a fast and cost-effective way. The transactions that are included within HIPAA consist of standard electronic formats for enrollment, eligibility, payment and remittance advice, claims, health plan premium payments, health claim status, and referral certification and authorization.
- **Code Sets** include data elements used to uniformly document the reasons why patients are seen and what is done to them during healthcare encounters (procedures).
- **Identifiers** are numbers used in the administration of healthcare to identify healthcare providers, health plans, employers, and individuals (patients). Over time, the use of identifiers is intended to simplify administrative processes, such as referrals and billing, improve accuracy of data, and reduce costs.
- **Security** refers to standards developed and adopted for all health plans, clearing houses, and providers to follow. Compliance is required at all stages of transmission and storage of healthcare information to ensure integrity and confidentiality of the records at all phases of the process (before, during, and after transmission).
- **Privacy** refers to standards defining what are appropriate and inappropriate disclosures of individually identifiable health information and how patient rights are to be protected.

The overall benefits of Administrative Simplification include:

- Lowering administrative costs.
- Enhancing accuracy of data and reports.
- Increasing customer satisfaction.
- Reducing cycle time.
- Improving cash management.

Promoting HIPAA Compliance and Integration

The iWay Adapter for HIPAA enables healthcare providers to integrate internal patient care and financial systems and external trading partner systems, using the HIPAA-mandated format.

The iWay Adapter for HIPAA:

- Transforms HIPAA transactions into any other format including XML, non-XML, EDI, SQL, SAP® IDoc, RPC, COM+®, and J2EE, and interfaces to legacy applications and data sources.
- Rapidly creates and integrates business-to-business transactions using XML or non-XML EDI formats such as ANSI X.12, UN/EDIFACT, and SWIFT™.
- Allows applications to receive and publish HIPAA transactions across TCP/IP, HTTP, and IIOP networks.
- Provides a common development environment inside multiple message brokers and application servers including IBM WebSphere MQ Integrator®, Microsoft® Commerce Server, Microsoft BizTalk® Server, and Oracle® 9iAs.
- Supports complete HIPAA ANSI X12N 4010 transaction sets.
- Defines custom messages and parsing rules through a rich graphical environment and XML rules engine that eliminates custom coding.

Maximum Interoperability With HIPAA

The iWay Adapter for HIPAA is designed to accelerate and simplify the process of HIPAA compliance, facilitating the seamless integration of internal patient care and financial systems, regardless of format. At the same tine, the iWay Adapter for HIPAA allows secure and auditable business-to-business processes and information exchange with external trading partners. The iWay Adapter for HIPAA supports of over 200 enterprise data and application systems, enabling organizations to easily take the fast path to HIPAA compliance, no matter how complex and diverse the back-end environments are. All of this can be done without custom coding.

Seamless Legacy Integration Solution

The real benefit of HIPAA compliance is the ability to integrate legacy applications using different platforms, databases, and operating systems, as well as software used by various ancillary entities such as reference labs and imaging centers. For the most part, these systems are mainframe applications running legacy applications such as CICS®, VSAM, IMS®, and MODEL204. In addition, the move to distributed computing has resulted in disparate applications based on AS/400®, HP3000, and UNIX® systems with applications such as MUMPS, Ingres®, and Informix®.

The iWay Adapter for HIPAA streamlines this very complex flow of clinical and administrative information by providing seamless integration and access to data on disparate platforms with differing communication protocols, database structures, APIs, user interfaces, and security frameworks. This protects the investment in legacy applications and databases, as well as packaged customer relationship management (CRM), enterprise resource planning (ERP), and supply chain management (SCM) applications.

Transforming Data

The iWay Adapter for HIPAA provides a unique graphical workbench for defining integration rules and mapping the transformations and workflows for HIPAA integration with enterprise systems and external trading partners.

Supported HIPAA Transactions

The iWay Adapter for HIPAA provides support for all of the HIPAA ANSI X 12N 4010 transactions:

- 820 Premium Payment
- 835 Claim Payment
- 270 Eligibility Enquiry
- 271 Eligibility Response
- 276 Claim Request
- 277 Claim Response
- 278 Service Review
- 834 Enrollment
- 837 (I) Claim (Institutional)
- 837 (D) Claim (Dental)
- 837 (P) Claim (Professional)
- Embedded HL7 Documents

Installation Notes for the HIPAA Websphere MQ Integrator Developer Suite

The HIPAA Websphere MQ Integrator Developer suite is a configuration of the iWay Enterprise Integration Suite (EIS). It has been tailored to include:

- HIPAA dictionaries.
- Pre-built transformation templates (HIPAA to XML and XML to HIPAA).
- Document type definitions (DTDs) to map transformations.

The iWay Adapter for HIPAA is also configured to exploit the full power of IBM's best integration products from the WebSphere family. The iWay Adapter for HIPAA can be called from a WebSphere MQ Integrator (WMQI) message flow (through the adapter or an adapter plug-in).

The iWay Adapter for HIPAA is installed by using the supplied license code. The procedure for installing the iWay Adapter for HIPAA is explained in the *WebSphere MQ Integration Suite* manual.

The product is configured to work "out of the box." Configuration involves enabling the listeners to react to specific documents, if the listeners are used. When using the iWay Adapter for HIPAA from WMQI, you only need to point the plug-in node to the MQSI listener port.

The nodes supplied are fully documented in the *WebSphere MQ Integration Suite* manual (which is also supplied with this package).

The WMQI must be installed prior to building your HIPAA solutions. By supplying the correct license code, you install the HIPAA version of the iWay Enterprise Integration Broker (EIB). Please see the *WebSphere MQ Integration Suite* manual to proceed.

Introducing the iWay Adapter for HIPAA

The iWay Adapter for HIPAA enables fast integration of HIPAA EDI transactions into your existing environment. The adapter enables developers to parse, transform, validate, store, and integrate healthcare information into the existing enterprise and pass information electronically, to partners, in HIPAA mandated format.

To enable fast integration, the iWay Adapter for HIPAA includes a parser for the EDI documents and pre-built templates that enable developers to convert HIPAA documents to XML format or XML documents to HIPAA format. DTDs for the XML to HIPAA transformation are provided. The adapter also includes dictionaries for all eleven of the EDI transactions to enable you to build custom templates using the Workbench tool set. The adapter consists of three major components that allow integration of HIPAA into your enterprise:

- HIPAA toolkit

- HIPAA 4010 dictionaries
- Rules files
- Code sets
- DTDs
- Transformation templates
- HIPAA plug-in node for WebSphere MQ Integrator (optional)

Document Conversion

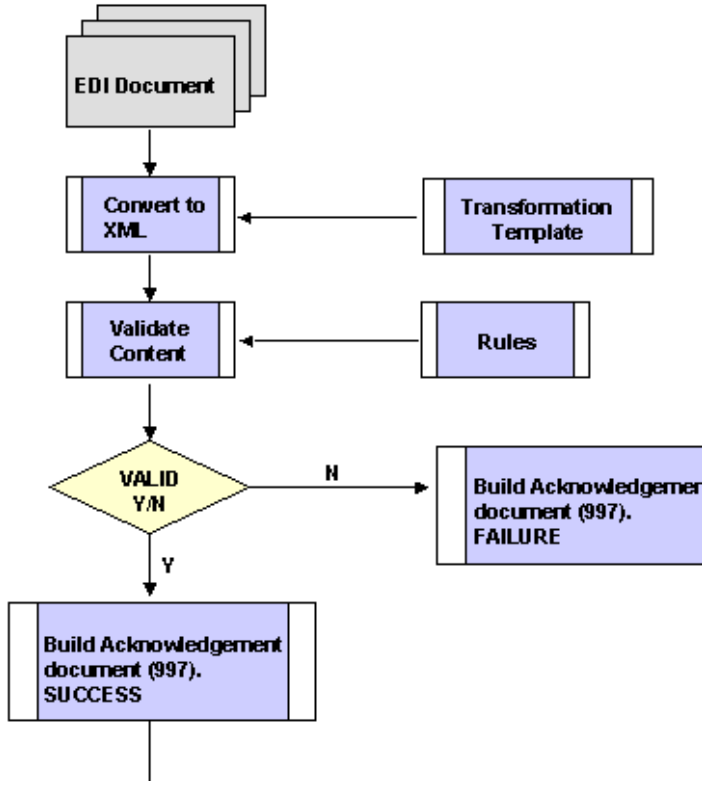
which is configured to transform HIPAA documents to XML documents (and vice versa) and to validate the HIPAA documents (based on the published implementation guides). The process involves the transformation of the incoming EDI document, applying all the mapping rules that have been created at design time using the Workbench.

After the document is transformed to XML, the level 1-5 validation tests are performed. The rules engine uses a rule file (supplied for each transaction), which applies rules as per the implementation guide for each transaction. After validation, a functional acknowledgement is created and can be routed back to the originator of the transaction.

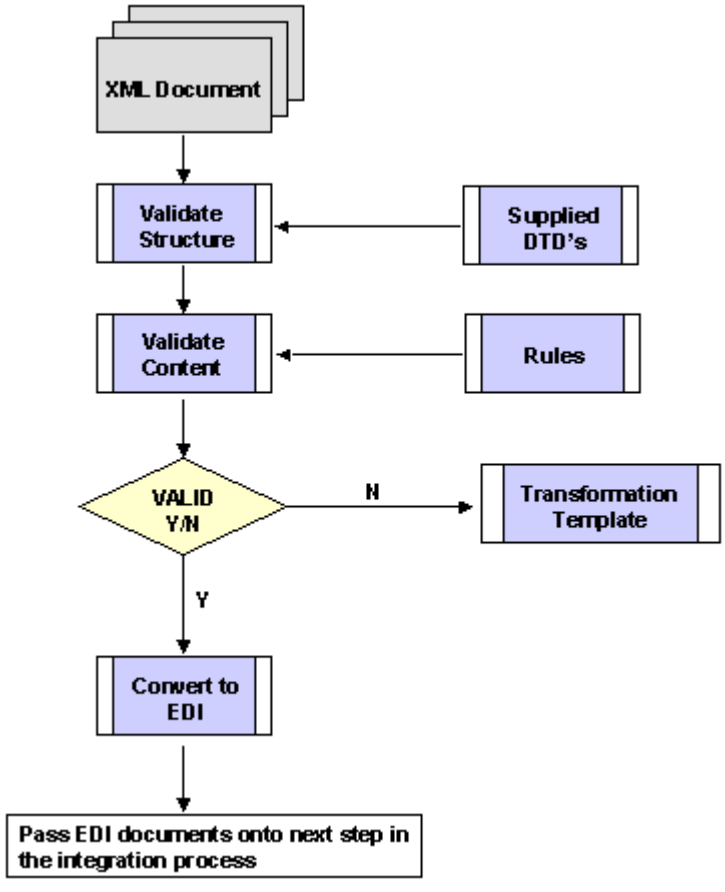
The process of converting XML to HIPAA format is the reverse process, with an exception of cases when the XML document is incorrectly built prior to transformation to EDI format.

The following diagrams show the steps for document conversion from:

- EDI to XML
- XML to EDI



Conversion of a HIPAA Document to an XML Document



Conversion of an XML Document to an EDI Document

The iWay Adapter for HIPAA Toolkit

The iWay Adapter for HIPAA toolkit includes pre-built XML to EDI and EDI to XML templates for all of the 4010 HIPAA transaction sets.

The following list contains the documents supplied for XML to EDI and EDI to XML translation:

Doc #	Description	XML to EDI and EDI to XML templates (.xch)	Sample EDI file	Validation (rule file)	Sample / Structure files (for XML to EDI transformation)	DTDs
270	Health Care Eligibility Inquiry	270_XML_HIPPA.xch 270_HIPPA_XML.xch	_270_eligibility_request.data	HIPAA270rules.xml	270_XMLStruc.xml	270.dtd
271	Health Care Eligibility Response	271_XML_HIPPA.xch 271_HIPPA_XML.xch	_271_eligibility_response.data	HIPAA271rules.xml	271_XMLStruc.xml	271.dtd
276	Health Care Claim Status Request	276_XML_HIPPA.xch 276_HIPPA_XML.xch	_276_ClaimStatus_request.data	HIPAA276rules.xml	276_XMLStruc.xml	276.dtd
277	Health Care Claim Status Response	277_XML_HIPPA.xch 277_HIPPA_XML.xch	_276_ClaimStatus_response.data	HIPAA277rules.xml	277_XMLStruc.xml	277.dtd
278Req	Health Care Services Review—Request for Review	278Req_XML_HIPPA.xch 278Req_HIPPA_XML.xch	_278_review_request.data	HIPAA278Request_rules.xml	278Req_XMLStruc.xml	278Req.dtd
278Res	Health Care Services Review—Response	278Res_XML_HIPPA.xch 278Res_HIPPA_XML.xch	_278_review_response.data	HIPAA278Response_rules.xml	278Res_XMLStruc.xml	278Res.dtd
820	Payroll Deducted and Other Group Premium Payment for Insurance Products	820_XML_HIPPA.xch 820_HIPPA_XML.xch	_820_premiumPayment.data	HIPAA820rules.xml	820_XMLStruc.xml	820.dtd
834	Benefit Enrollment and Maintenance	834_XML_HIPPA.xch 834_HIPPA_XML.xch	_834_benefitEnrollment.data	HIPAA834rules.xml	834_XMLStruc.xml	834.dtd
835	Health Care Claim Payment/Advice	835_XML_HIPPA.xch 835_HIPPA_XML.xch	_835_remittance.data	HIPAA835rules.xml	835_XMLStruc.xml	835.dtd
837I	Health Care Claim - Institutional	837Ins_XML_HIPPA.xch 837Ins_HIPPA_XML.xch	_837_dental.data	HIPAA837Irules.xml	837Ins_XMLStruc.xml	837Ins.dtd
837D	Health Care Claim - Dental	837Den_XML_HIPPA.xch 837Den_HIPPA_XML.xch	_837_inst.data	HIPAA837Drules.xml	837Den_XMLStruc.xml	837Den.dtd
837P	Health Care Claim - Professional	837Pro_XML_HIPPA.xch 837Pro_HIPPA_XML.xch	_837_Professional.data	HIPAA837Prules.xml	837Pro_XMLStruc.xml	837Pro.dtd

Using the iWay Application Explorer With the iWay Adapter for HIPAA for BEA WebLogic

iWay Application Explorer uses an explorer metaphor for browsing the system. The explorer enables you to create XML schemas and Web services for the associated object. External applications that access HIPAA through the iWay Adapter for HIPAA for BEA WebLogic use either XML schemas or Web services to pass data between the external application and the adapter.

The two versions of iWay Application Explorer that are supported for Siebel are Servlet iWay Application Explorer, a Java Web application running within a servlet container that is accessible through a Web browser, and Application Explorer running in BEA WebLogic Workshop.Application Explorer uses interfaces provided by HIPAA and in-depth knowledge of the HIPAA application systems to access and browse business object metadata. After an object is selected, Application Explorer can generate an XML schema or Web service to define the object for use in conjunction with the iWay Adapter for HIPAA for BEA WebLogic.

External applications accessing HIPAA via the iWay Adapter for HIPAA for BEA WebLogic use either the XML schema or Web service to pass data between the external application and the adapter.

The steps required to create XML schemas for Web services are illustrated in *Chapter 2, Creating XML Schemas or Web Services for the iWay Adapter for HIPAA for BEA WebLogic*.

Key Features of iWay Application Explorer

Key features of iWay Application Explorer include:

- The ability to connect to and explore a variety of application systems.
- Access to application system object metadata.
- A point-and-click process for generating XML schemas and Web services.

Installing and Configuring the Servlet iWay Application Explorer

iWay Application Explorer must be deployed through a servlet container or application server (for example, Sun Java System Application Server, BEA WebLogic, Apache Tomcat, SAP J2EE Engine, or IBM WebSphere). If you are using Application Explorer in BEA WebLogic Workshop, you must also have the BEA WebLogic Workshop installed.

Note: To use Application Explorer within the BEA WebLogic Workshop, iBSE must be deployed to the BEA WebLogic server.

In addition, the HIPAA Enterprise Information System (EIS) must be installed, configured, and available for client access. Application Explorer need not reside on the same system as HIPAA, but network access is required.

For more information on installing and configuring the Java Servlet iWay Application Explorer, see the *iWay 5.5 Installation and Configuration* documentation.

Deployment Information for the iWay Adapter for HIPAA

The iWay Adapter for HIPAA for BEA WebLogic works in conjunction with the following components:

- iWay Application Explorer

with either

- iWay Business Services Engine (iBSE)

or

- iWay Enterprise Connector for J2EE™ Connector Architecture (JCA)

Application Explorer, used to configure connections and create Web services and events, can be configured to work in a Web services environment in conjunction with the iWay Business Services Engine or with the iWay Enterprise Connector for J2EE Connector Architecture (JCA). When working in a JCA environment, the connector uses the Common Client Interface (CCI) to provide fast integration services using iWay Adapters instead of using Web services.

Both iBSE and the iWay connector for JCA are deployed to an application server such as BEA WebLogic Server with iWay Application Explorer and the adapters.

Deployment Roadmap

The following table lists the location of deployment information for the iWay Adapter for HIPAA for BEA WebLogic in the three operating environments. A description of each environment follows the table.

Deployment Option	Chapter
iWay Application Explorer	• Chapters 2 and 3 and Appendix A of this guide • i*Way Installation and Configuration for BEA WebLogic* • *iWay Servlet Application Explorer for BEA WebLogicUser's Guide*
iWay Business Services Engine (iBSE)	• *iWay Installation and Configuration for BEA WebLogic*
iWay Enterprise Connector for J2EE Connector Architecture (JCA)	• *iWay Connector for JCA for BEA WebLogic User's Guide* • *iWay Installation and Configuration for BEA WebLogic*

iWay Application Explorer

iWay Application Explorer uses an explorer metaphor to browse the HIPAA system for metadata. The explorer enables you to create XML schemas and Web services for the associated object. In addition, you can create ports and channels to listen for events in HIPAA. External applications that access HIPAA through the iWay Adapter for HIPAA for BEA WebLogic use either XML schemas or Web services to pass data between the external application and the adapter.

The iWay Business Services Engine (iBSE)

The iWay Business Services Engine (iBSE) exposes—as Web services—enterprise assets that are accessible from adapters regardless of the programming language or the particular operating system.

iBSE simplifies the creation and execution of Web services when running:

- Custom and legacy applications
- Database queries and stored procedures
- Packaged applications
- Terminal emulation and screen-based systems
- Transactional systems

Web services is a distributed programming architecture that solves Enterprise Application Integration (EAI) hurdles that other programming models cannot. It enables programs to communicate with one another using a text-based, platform- and language-independent message format called XML.

Coupled with a platform and language independent messaging protocol called SOAP (Simple Object Access Protocol), XML enables application development and integration by assembling previously built components from multiple Web services.

The iWay Enterprise Connector for J2EE Connector Architecture (JCA)

The iWay Enterprise Connector for J2EE Connector Architecture (JCA) enables developers of JCA-compliant applications to deploy iWay adapters as JCA resources. The connector is supported on J2EE-compliant application servers such as the BEA WebLogic Server.

The iWay Connector for JCA is distributed as a standard Resource Adapter Archive (RAR) for deployment to the application server. Thus, the connector can be used in systems that are non-compliant, although services such as pooled connections are not available.

CHAPTER 2

Creating XML Schemas or Web Services for the iWay Adapter for HIPAA for BEA WebLogic

Topics:

- Overview
- Starting iWay Servlet Application Explorer
- Establishing a Target for HIPAA
- Creating a Schema
- Creating a Web Service

This section describes how to use iWay Servlet Application Explorer to create XML schemas or Web services for the iWay Adapter for HIPAA for BEA WebLogic.

Overview

External applications that access HIPAA through the adapter use either XML schemas or Web services to pass data between the external application and the adapter. You can use iWay Servlet Application Explorer to create the required XML schemas and Web services.

Application Explorer is a Web application running within a servlet container that is accessible through a Web browser. For more information on installing and configuring the iWay Servlet Application Explorer, see the *iWay 5.5 Installation and Configuration for BEA WebLogic* documentation.

Starting iWay Servlet Application Explorer

Before you can use iWay Servlet Application Explorer, you must start BEA WebLogic Server. Then, you can open Application Explorer.

Procedure How to Start BEA WebLogic Server on Windows or on UNIX

1. To start the BEA WebLogic Server on Windows:
   a. Click the *Windows Start menu*.
   b. Select *Programs*, *BEA WebLogic Platform 8.1*, *User Projects, your domain for iWay,* and then, click *Start Server.*
2. To start BEA WebLogic Server on UNIX or from a command line, type the following at the prompt:

   ```
   BEA_HOME\user_projects\domains\DOMAIN_NAME\startWebLogic.cmd
   ```

   where:

   BEA_HOME
   Is the directory where BEA WebLogic is installed.

   DOMAIN_NAME
   Is the domain you are using for iWay.

Procedure How to Open iWay Servlet Application Explorer

To open Application Explorer:

1. Enter the following URL in your browser window:

   ```
   http://hostname:port/iwae/index.html
   ```

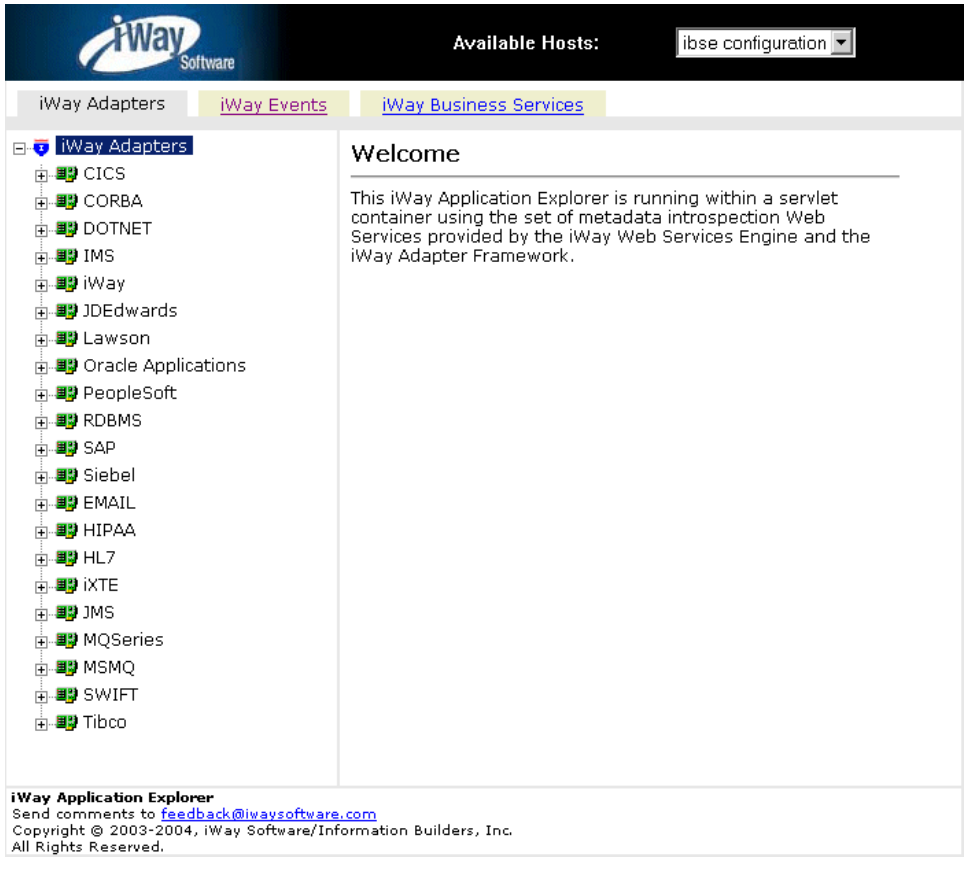
   where:

   hostname
   Is the name of the machine where your application server is running.

port

Is the port where the application server is listening.

After you start Application Explorer, the following Welcome window opens, showing the iWay Adapters, iWay Events, and iWay Business Services tabs. The iWay Adapters node is highlighted in the left pane.



The Available Hosts drop-down menu in the upper right lists the iWay Connector for JCA or Servlet iBSE instance you can access.

For more information on adding instances, see the *iWay 5.5 Installation and Configuration for BEA WebLogic* documentation.

You are now ready to create new targets for HIPAA.

Establishing a Target for HIPAA

A target serves as your connection point and is automatically saved after you create it. You must establish a connection to HIPAA every time you start iWay Application Explorer or after you disconnect from the system.

Creating a New Target

To connect to HIPAA for the first time, you must create a new target.

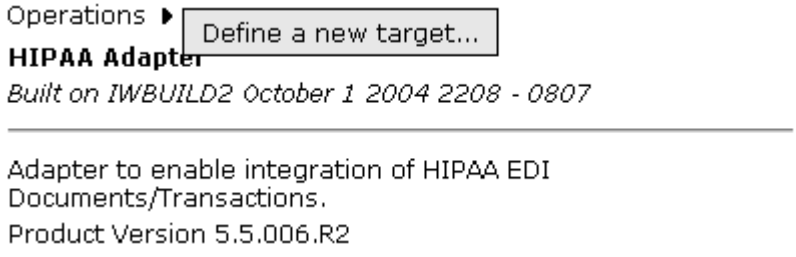
Procedure How to Create a New Target

The following graphic shows the list of supported adapters in the left pane and information about the selected adapter in the right pane.

To create a new target:

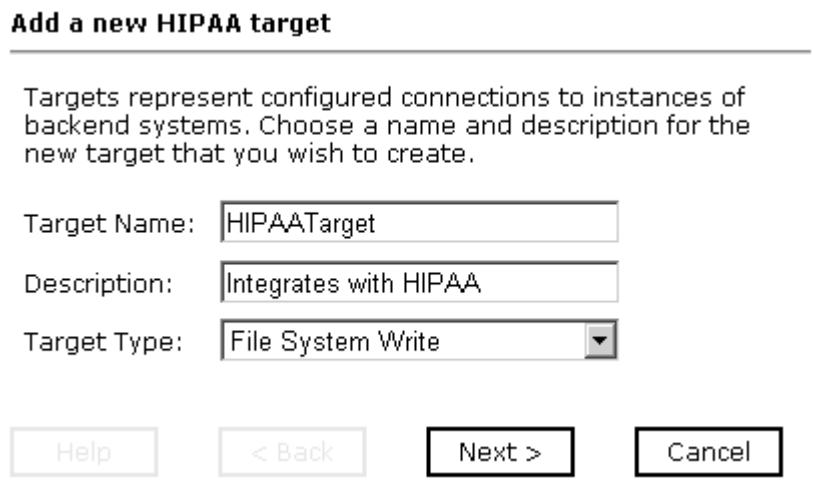
1. In the left pane, click the *HIPAA* node.

Descriptive information (for example, title and product version) regarding the iWay Adapter for HIPAA for BEA WebLogic appears in the right pane.



2. In the right pane, move the pointer over *Operations* and select *Define a new target*.

The Add a new HIPAA target pane opens on the right. The following illustration shows the fields in the right pane where you enter connection information for the target.



3. Specify the following information for the HIPAA target you are defining.

a. Type a descriptive name and a brief description for the new target.

b. From the Target Type drop-down list, select one of the following transports from the drop-down list:

- File System Write.
- File Transfer Protocol (FTP).
- HyperText Transfer Protocol (HTTP).
- IBM MQSeries (MQ).

- TCP Session.

4. Click *Next*.

   The Set connection info pane appears on the right and includes fields that are specific to the type of transport you selected.

5. Provide the appropriate information that is specific to the transport you selected.

   - For more information on File System Write, see *File System Write Properties* on page 2-6.
   - For more information on File Transfer Protocol (FTP), see *File Transfer Protocol Properties* on page 2-7.
   - For more information on HyperText Transfer Protocol (HTTP), see *HyperText Transfer Protocol Properties* on page 2-7.
   - For more information on IBM MQSeries (MQ), see *MQSeries Properties* on page 2-8.
   - For more information on TCP Session, see *TCP Properties* on page 2-8.

6. Click *Finish*.

   The following graphic shows the HIPAA target (HIPAATarget) that appears below the HIPAA node in the left pane.

You are now ready to connect to your HIPAA target.

Reference File System Write Properties

The following table provides definitions for the properties required for the File System Write target type.

Property	Definition
Directory	The directory to which output messages are emitted.
Filename Mask	The output file name (can contain an asterisk), which gets expanded to a timestamp. A pound sign can be used as a mask for a sequence count. Each pound symbol represents a whole number integer value. For example, File## counts up to 99 before restarting at 0, File### counts up to 999 before restarting at 0, and so on.

Reference File Transfer Protocol Properties

The following table provides definitions for the properties required for the File Transfer Protocol target type.

Settings tab

Property	Definition
Host	FTP target system.
Port	FTP target system port.
User	User ID to use when connecting to the FTP host.
Password	Password associated with the user ID.
Directory	The directory to which output messages are emitted.
Filename Mask	The output file name (can contain an asterisk), which gets expanded to a timestamp. A pound sign can be used as a mask for a sequence count. Each pound symbol represents a whole number integer value. For example, File## counts up to 99 before restarting at 0, File### counts up to 999 before restarting at 0, and so on.

Advanced tab

Property	Definition
Retry Interval	The maximum wait interval between retries when a connection fails. Retry interval duration in *xx*H:*xx*M:*xx*S format. For example, 1H:2M:3S is 1 hour 2 minutes and 3 seconds.
Maxtries	Maximum number of retry attempts if a write failure occurs.

Reference HyperText Transfer Protocol Properties

The following table provides definitions for the properties required for the File Transfer Protocol target type.

Property	Definition
HTTP URL	The HTTP URL.

Property	Definition
Header	The HTTP header field.

Reference MQSeries Properties

The following table provides definitions for the properties required for the MQSeries target type.

Settings tab

Property	Definition
Queue Manager	Name of the MQSeries queue manager to be used.
Queue Name	Queue on which request documents are received.
Correlation ID	The correlation ID to set in the MQSeries message header.

MQ Client tab

Property	Definition
Host	Name of the MQSeries queue manager to be used.
Port	Queue on which request documents are received.
Channel	The correlation ID to set in the MQSeries message header.

Reference TCP Properties

The following table provides definitions for the properties required for the TCP target type.

Property	Definition
Host	Host name or host address.
Port	TCP listening port.
Encoding	Document character set.

Connecting to a Target

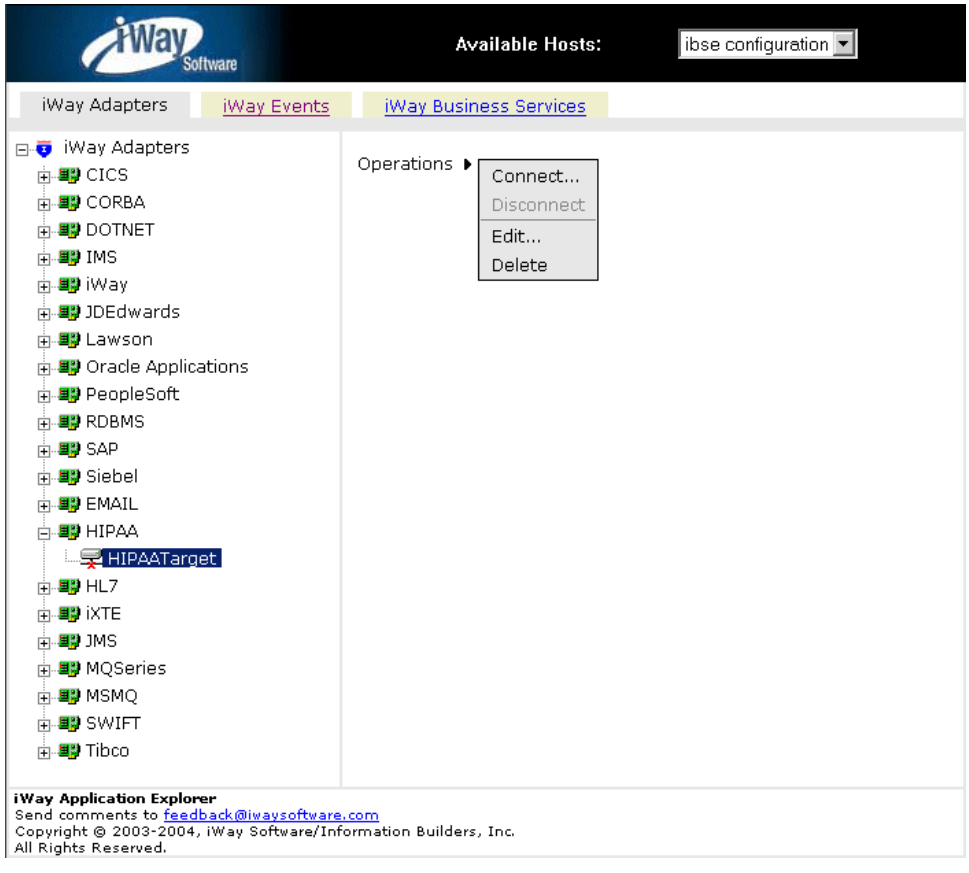
You must use the target you defined to connect to HIPAA.

Procedure How to Connect to a Target

To connect to a target:

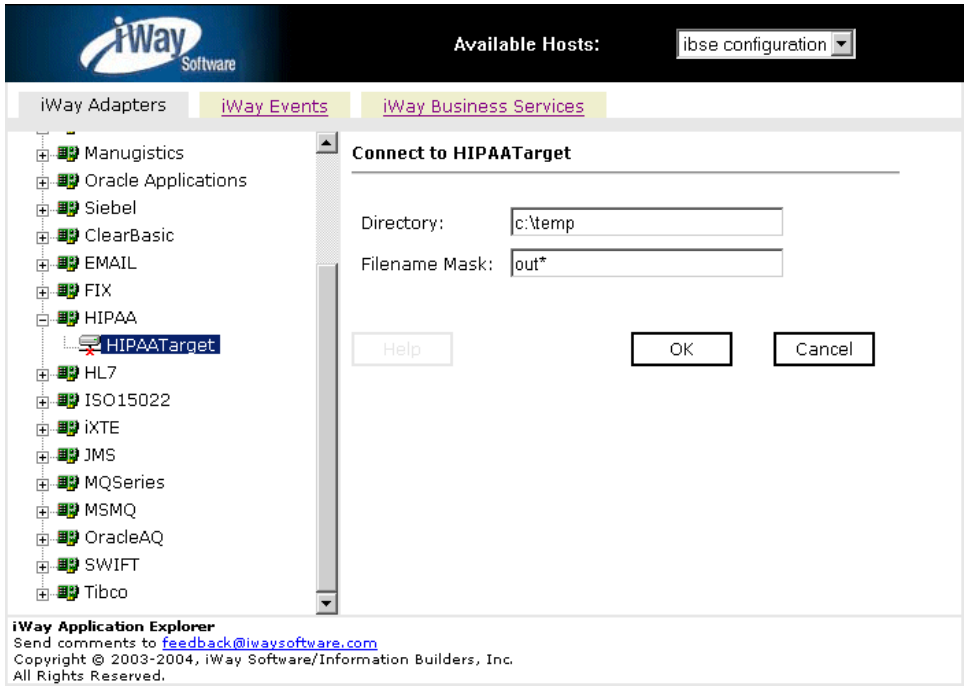
1. In the left pane, expand the *HIPAA* node and select the target you defined, for example, HIPAATarget.

   The following graphic shows the HIPAATarget node selected in the left pane and the Operations menu expanded in the right pane.



2. Move the pointer over *Operations* and select *Connect*.

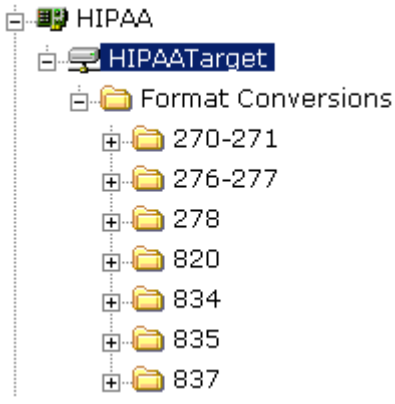
The following graphic shows that the Connect to HIPAATarget pane opens on the right.



3. Click *OK*.

The following graphic shows that the x icon that appeared previously to the left of the HIPAATarget node has disappeared, indicating that the node is now connected.

The following graphic shows the expanded HIPAATarget node.



Disconnecting From a Target

Although you can maintain multiple open connections to different application systems, it is a good practice to close connections when you are not using them.

Procedure How to Disconnect From a Target

To disconnect from a target:

1. From the left pane, click the target, for example, HIPAATarget, to which you are connected.
2. Move the pointer over *Operation* and select *Disconnect*.

   Disconnecting from the application system drops the connection, but the node remains.

Modifying a Target

After you create a target for HIPAA using iWay Servlet Application Explorer, you can edit any of the information that you provided previously.

Procedure How to Edit a Target

To edit a target:

1. In the left pane, click the target, for example, HIPAATarget.
2. Move the pointer over *Operations* and select *Edit*.
3. Modify the connection information.
4. Click *Next* to continue editing additional fields.
5. When you have completed your edits, click *Finish*.

Deleting a Target

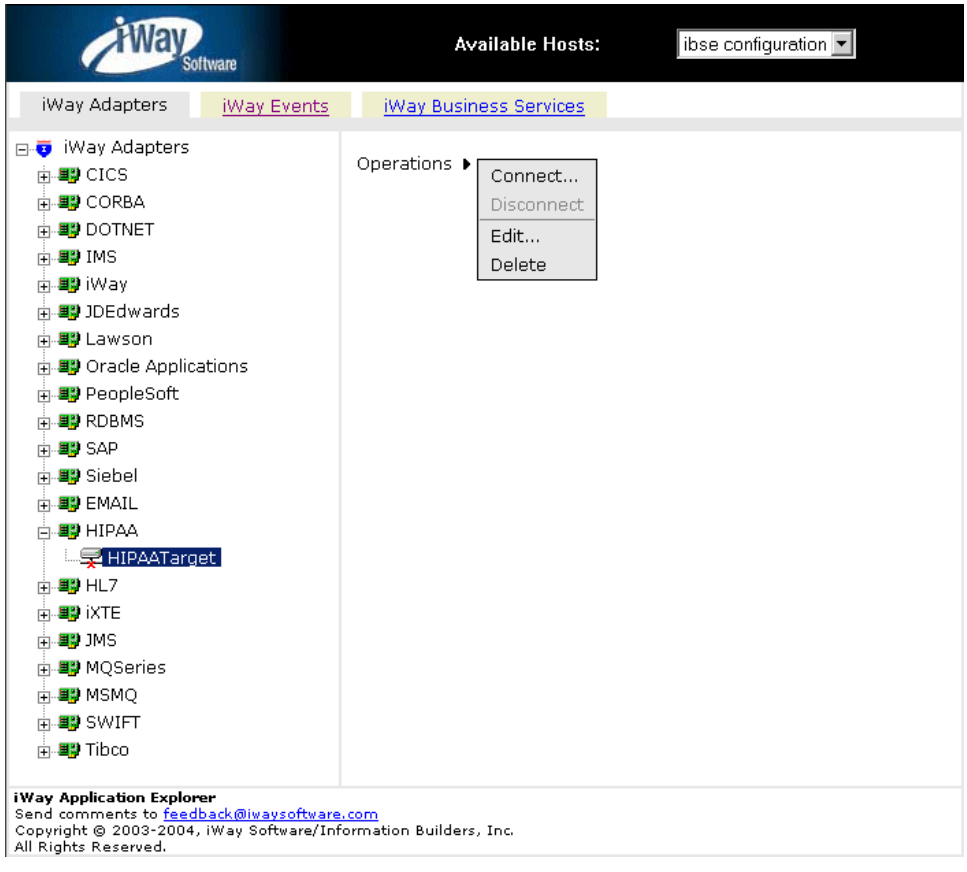
In addition to closing a target, you can delete a target that is no longer required. You can delete it whether or not it is closed. If open, the target automatically closes before it is deleted.

Procedure How to Delete a Target

To delete a target:

1. In the left pane, click the target, for example, HIPAATarget.

   The following graphic shows the target selected in the left pane, and the operations menu expanded in the right pane.



2. Move the pointer over *Operations* and select *Delete*.
3. To delete the target you selected, click *OK*.

The HIPAATarget node disappears from the left pane.

Creating a Schema

You can create service schemas for Business Services and Business Components using iWay Application Explorer.

The following topic, *Creating an XML Schema*, describes how to create schemas for the adapter when you deploy the iWay Adapter for HIPAA for BEA WebLogic for use either in a JCA (iWay Enterprise Connector for J2EE Connector Architecture) environment or a Web services environment.

If you plan to deploy the iWay Adapter for HIPAA for BEA WebLogic in a Web services environment, see also *Creating a Web Service* on page 2-17.

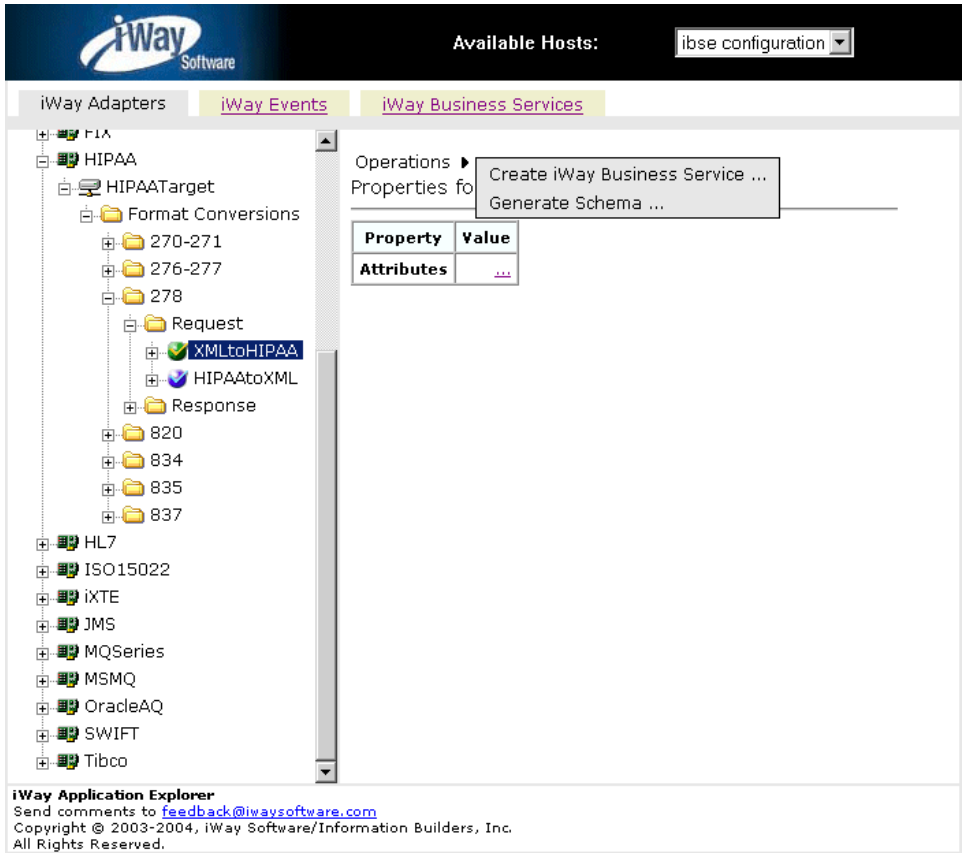
Creating an XML Schema

You create schemas for HIPAA using iWay Application Explorer.

Procedure How to Create an XML Schema

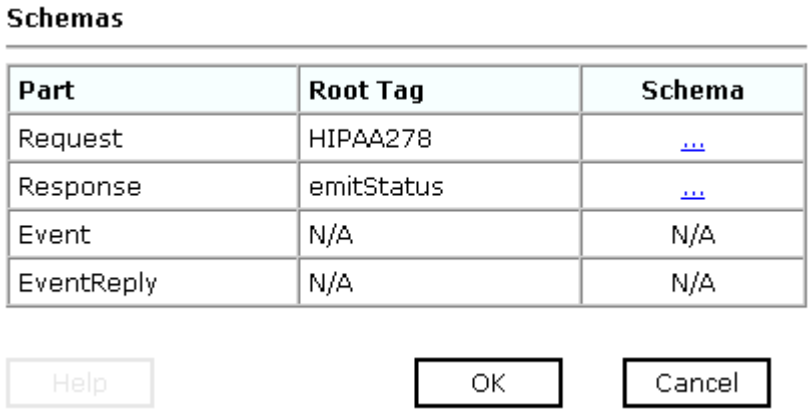
To generate service request and response schemas:

1. If you have not started the explorer, start Application Explorer and connect to your HIPAA system.
2. In the left pane, expand the HIPAATarget node.
3. Continue expanding nodes to get to the HIPAA document level.



4. In the right pane, move the cursor over *Operations* and select *Generate Schema*.

Application Explorer builds schemas. A schemas table similar to the following appears in the right pane. This table contains three columns labeled Part, Root Tag, and Schema. The Schema column provides hyperlinks to the different schemas.



5. To view a schema, click the ellipsis (…) in the row corresponding to the schema you want to view.

The following is an example of a request schema:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--  Generated by the iBSE 2004-10-05T22:13:16Z
  -->
- <xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema">
  - <xs:element name="HIPAA278">
    - <xs:complexType>
      - <xs:sequence>
        - <xs:element maxOccurs="1"
            minOccurs="1" name="ISA">
          - <xs:complexType>
            - <xs:sequence>
              - <xs:element minOccurs="0"
                  name="_01_Authorization_Information_Qu
                - <xs:simpleType>
                  - <xs:restriction
                      base="xs:string">
                      <xs:minLength
                        value="0" />
                      <xs:maxLength
                        value="2" />
                    </xs:restriction>
                  </xs:simpleType>
                </xs:element>
              - <xs:element minOccurs="0"
                  name="_02_Authorization_Information_">
```

For more information on where the schemas are stored, see the following topic, *Schema Location*.

Reference Schema Location

Application Explorer stores the schemas it creates in subdirectories under the iWay home directory of the machine where it is installed. The exact location of the schemas differs depending on whether you deploy Application Explorer with an iBSE or a JCA configuration.

- When using the adapter with an iBSE configuration, the schemas are stored under a \schemas subdirectory of the iWay home directory, for example,

  ```
  C:\Program
  Files\iway55\bea\ibse\wsdl\schemas\service\HIPAA\HIPAATarget
  ```

  where:

  HIPAATarget

  Is the name of the connection to HIPAA as defined in Application Explorer. Under this directory, Application Explorer creates subdirectories containing schemas.

- When using the adapter with a JCA configuration, the schemas are stored under a \schemas subdirectory of the iWay home directory, for example,

  ```
  C:\Program Files\iWay55\config\base\schemas\HIPAA\HIPAATarget
  ```

  where:

  HIPAATarget

  Is the name of the connection to HIPAA as defined in Application Explorer. Application Explorer stores the schemas in this directory.

Creating a Web Service

You can generate a business service (also known as a Web service) for HIPAA operations.

Ensure you properly configure the servlet iBSE. For more information on installing and deploying iWay components, see the *iWay Installation and Configuration for BEA WebLogic* manual.

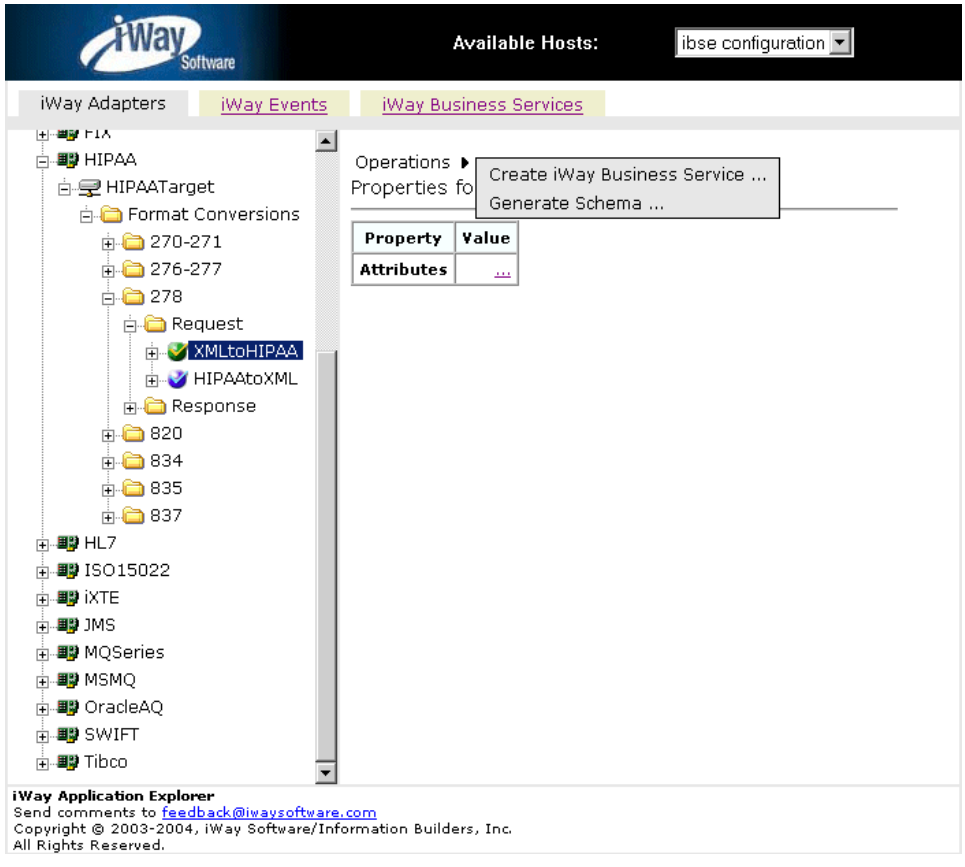
Note: In a J2EE Connector Architecture (JCA) implementation of iWay adapters, Web services are not available. When the adapters are deployed to use the iWay Connector for JCA, the Common Client Interface provides integration services using the iWay adapters. For more information, see the *iWay Installation and Configuration for BEA WebLogic* manual and the i*Way Connector for JCA for BEA WebLogic Server User's Guide*.

Procedure How to Generate a Web Service

To generate a Web service:

1. If you have not already connected, connect to HIPAA.
2. Expand the *HIPAA* node.
3. Continue expanding nodes down to the *Service* level.

   The following graphic shows the left pane with the Service node selected.



4. In the right pane, move the pointer over *Operations* and select *Create iWay Business Service*.

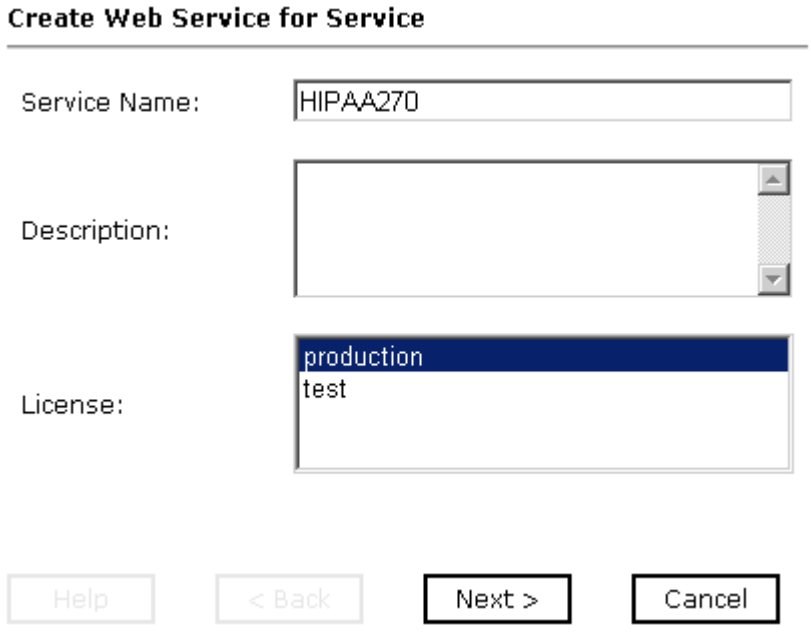
- If this is not the first Web service you want to create and use, choose whether to create a new service or use an existing service.

a. To use a previously created service, select the option to use an existing service and click *Next*.

A drop-down list appears.

b. Select the business service to which you want to add the new service and click *Next*.

- If this is the first Web service you are creating or if you select to create a new service, the Create Web Service pane appears. This pane provides three fields followed by a help button and three action buttons.



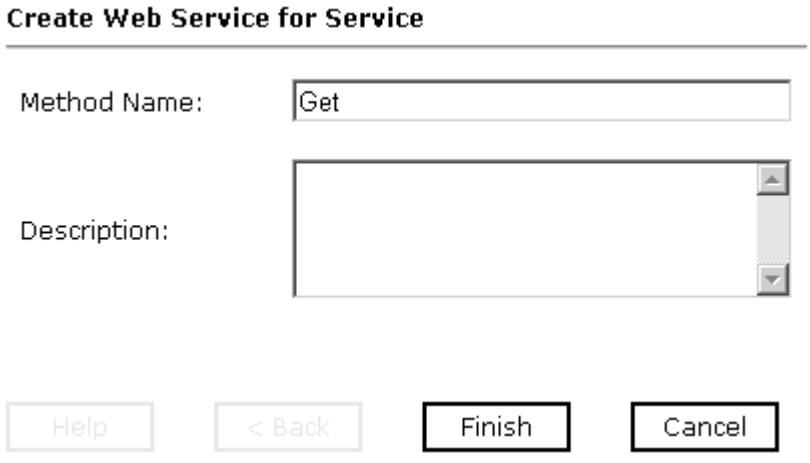
a. In the Service Name field, type a name to identify the Web service (under the Service node in the left pane of the iWay Business Services tab).

b. In the Description field, type a brief description of the Web service.

c. In the License field, select the license(s) with which you want to associate this business service. To select more than one, hold down the *Ctrl* key and click the licenses.

5. Click *Next*.

The right pane displays the next Create Web Service pane, which prompts you for information about the method of the service. It includes two fields, a help button, and three action buttons.

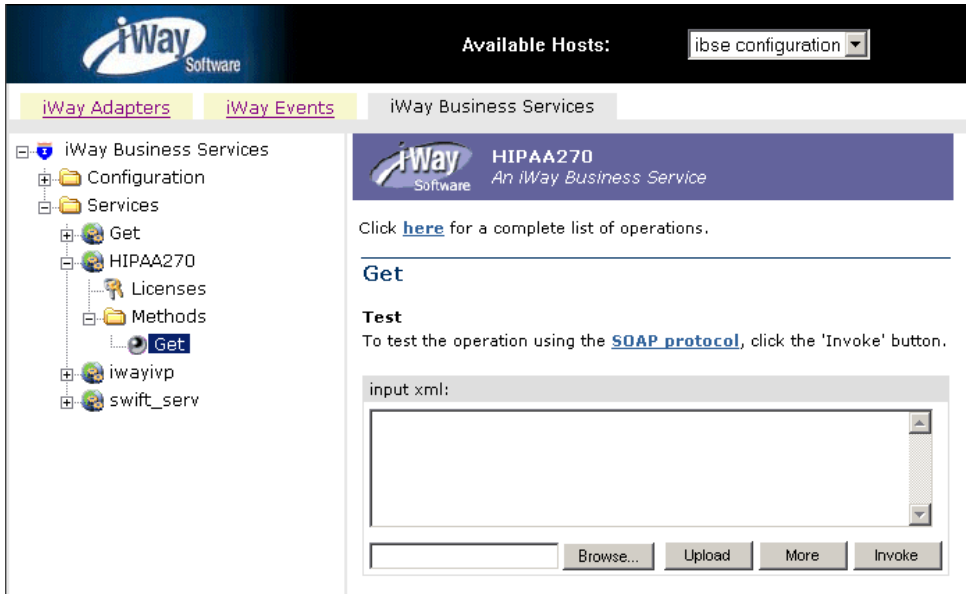


a. In the Method Name field, type a name to specify the name of the method to be added to the business service.

b. In the Description field, type a brief description of the method.

6. Click *Finish*.

Application Explorer switches the view to the iWay Business Services tab, and the new business service appears in the left pane.



Testing a Web Service for a Business Object

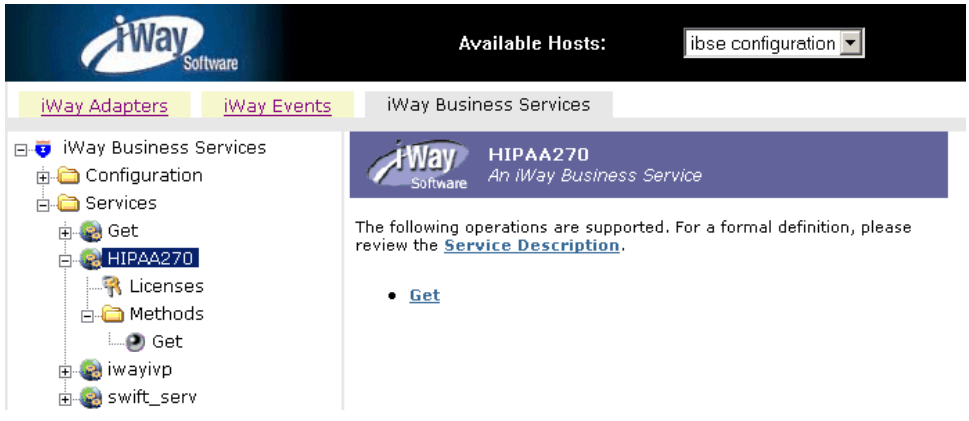
After you create a Web service, test it to ensure it functions properly. Application Explorer includes a test tool for testing a Web service.

Procedure How to Test a Web Service for a Business Object

To test a Web service:

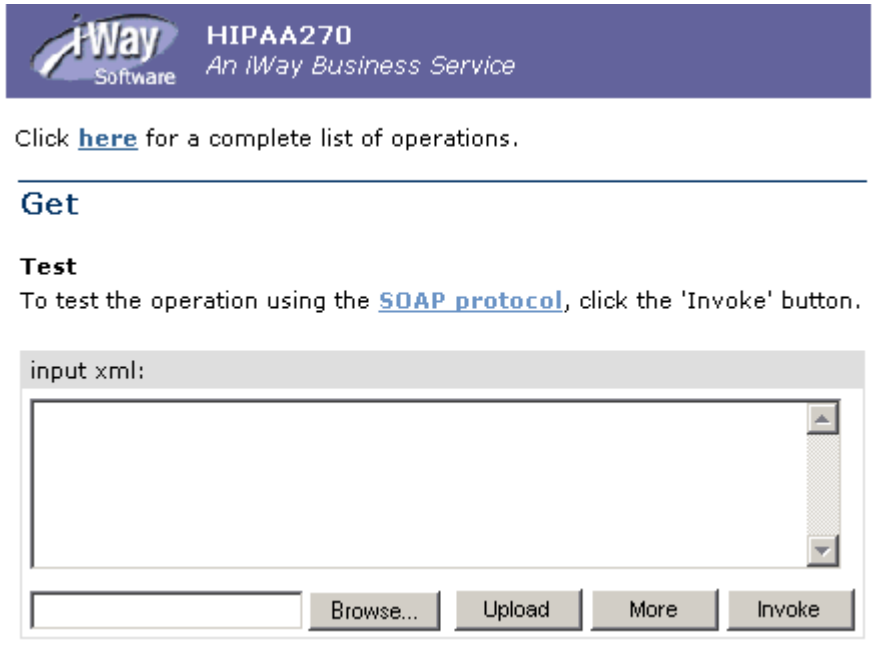
1. If you are not on the iWay Business Services tab of Application Explorer, click the tab to access business services.
2. If it is not expanded, expand the *iWay Business Services* node.
3. Expand the *Services* node.
4. Select the name of the business service you want to test.

   The business service name appears as a link in the right pane, as shown in the following graphic.



5. In the right pane, click the named business services link, for example, *post*.

   The test option appears in the right pane. This pane provides a text field in which to paste the XML input or browse to a file that can be uploaded.



6. Provide the appropriate XML input.
7. Click *Invoke*.

   Application Explorer displays the results in the results pane on the right.

Credential Mapping

For each SOAP request that is received, iBSE checks to see if a user name and password is included in the SOAP header. If a user name and password is available, iBSE acquires this information and replaces the values retrieved from the repository when pushing the request to the iWay Adapter.

CHAPTER 3

Listening for Events in HIPAA

Topics:

- Understanding iWay Event Functionality
- Creating an Event Port
- Creating a Channel

iWay Servlet Application Explorer deployed to a BEA WebLogic Server enables you to listen for events.

Although this section describes the Java™ servlet implementation of Application Explorer, other implementations provide the same functionality by means of similar graphical user interfaces.

Understanding iWay Event Functionality

Events are generated as a result of a HIPAA document arriving at a particular queue. You can use documents arriving at a queue to trigger an action in your application. For example, information in a message arriving at a queue can be used to update customer information in a database. If your application must perform an action when this happens, your application is a consumer of this event.

After you create a connection to your application system, you can add events using iWay Servlet Application Explorer. To create an iWay event, you must create a port and a channel.

- Port

  A port associates a particular business object exposed by an adapter with a particular disposition. A disposition defines the protocol and location of the event data. The port defines the end point of the event consumption. For more information, see *Creating an Event Port* on page 3-2.

- Channel

  A channel represents configured connections to particular instances of back-end or other types of systems. A channel binds one or more event ports to a particular listener managed by an adapter. For more information, see *Creating a Channel* on page 3-14.

Creating an Event Port

The following procedures describe how to create an event port from the iWay Event Adapters tab for various dispositions using Application Explorer.

The following dispositions are available when using the servlet Application Explorer in conjunction with an iBSE implementation. You can switch between an iBSE and a JCA implementation by choosing one or the other from the drop-down menu in the upper right of the Application Explorer.

- File
- iBSE
- MSMQ
- JMS queue
- SOAP
- HTTP
- MQ Series
- MAIL

Note: The MAIL disposition option will be supported in a future release.

The following dispositions are available when using Application Explorer in conjunction with a JCA connector implementation.

- File
- HTTP
- JMS queue
- MQ Series

Procedure How to Create an Event Port for the File Disposition

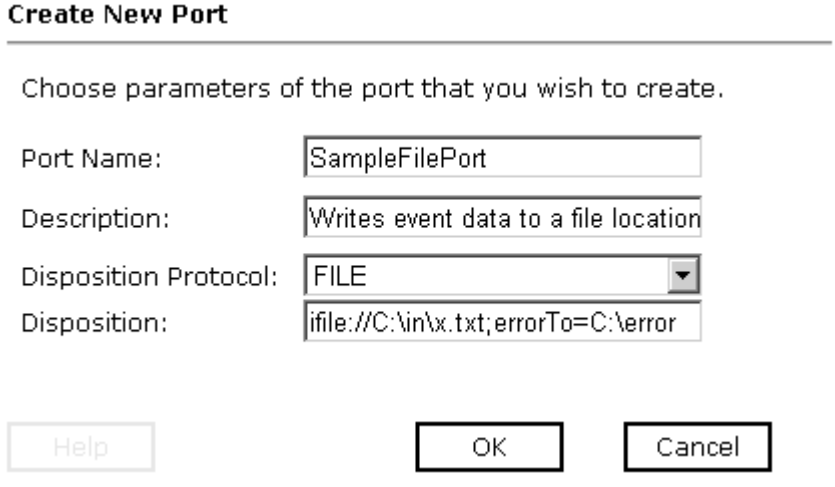
To create a specific event port for the File disposition:

1. Click the *iWay Events* tab.

   The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.
3. Select the *ports* node.
4. Move the pointer over *Operations* and select *Add a new port*.

   The Create New Port fields appear on the right, as shown in the following graphic. This pane provides four fields to define the new port, a help button, and two action buttons.



   a. Type a name for the event port and provide a brief description.

   b. From the Disposition Protocol drop-down list, select *FILE*.

c. In the Disposition field, provide a destination where the event data is written.

When pointing Application Explorer to an **iBSE** deployment, use the following format:

```
ifile://[location];errorTo=[pre-defined port name or another disposition url]
```

For example:

```
ifile://D:\in\x.txt;errorTo=ifile://D:\error
```

When pointing Application Explorer to a **JCA** deployment, provide the full path to the directory.

The following table defines the parameters for the File disposition.

Parameter	Description
location	The destination and filename of the document where event data is written. For example, C:\in\x.txt.
errorTo	Predefined port name or another disposition URL to which error logs are sent. Optional.

5. Click *OK*.

The event port appears under the ports node in the left pane. In the right pane, a table appears that summarizes the information associated with the event port you created. The summary is shown in the following graphic.

Operations ▸

Port Name	SampleFilePort
Description	Writes event data to a file location.
Disposition	ifile://C:\in\x.txt;errorTo=C:\error
Target	MQSeries

You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page 3-14.

Procedure How to Create an Event Port for iBSE

You can call a Web Service created through iWay Business Services Engine (iBSE).

To create an event port for iBSE:

1. Click the *iWay Events* tab.

The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.
3. Select the *ports* node.
4. Move the pointer over *Operations* and select *Add a new port*.

   The Create Event Port pane opens on the right.

   a. In the Port Name field, type a name for the connection.

      The name is used to build a repository entry as well as to identify the connection.

   b. In the Description field, type a description for the target name you just created.

   c. From the Disposition Protocol drop-down list, select *iBSE*.

   d. In the Disposition field, enter an iBSE destination in the form of:

```
ibse:svcName.mthName;responseTo=[pre-defined port name or another
disposition url];errorTo=[pre-defined port name or another
disposition url]
```

   The following table defines the parameters for the disposition.

Parameter	Description
svcName	Name of the service created with iBSE.
mthName	Name of the method created for the Web service.
responseTo	Location where responses to the Web service are posted. A predefined port name or another full URL. Optional.
errorTo	Location where error documents are sent. A predefined port name or another full URL. Optional.

5. Click *OK*.

   In the right pane, a table appears that summarizes the information associated with the event port you created. The event port also appears under the ports node in the left pane.

   You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page 3-14.

Procedure How to Create an Event Port for a JMS Queue

To create an event port for a JMS queue:

1. Click the *iWay Events* tab.

   The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.
3. Select the *ports* node.
4. Move the pointer over *Operations* and select *Add a new port*.

   The Create Event Port pane opens on the right.

   a. Type a name for the event port and provide a brief description.

   b. From the Disposition Protocol drop-down list, select *JMSQ*.

   c. In the Disposition field, enter a JMS destination.

      When pointing Application Explorer to an **iBSE** deployment, use the following format:

      ```
      jmsq:myQueueName@myQueueFac;jndiurl=[myurl];jndifactory=[myfactory
      ];user=[user];password=[xxx];errorTo=[pre-defined port name or
      another disposition url]
      ```

      When pointing Application Explorer to a **JCA** deployment, use the following format:

      ```
      jms:jmsqueue@jmsfactory;jndiurl=;jndifactory=;
      ```

      The following table defines the parameters for the disposition.

Parameter	Description
queue	JNDI name of a queue to which events are emitted.
Connection Factory	A resource that contains information about the JMS Server. The WebLogic connection factory is: `javax.jms.QueueConnectionFactory`

Parameter	Description
jndiurl	The URL to use to contact the JNDI provider. The syntax of this URL depends on which JNDI provider is being used. This value corresponds to the standard JNDI property, `java.naming.provider.url` For BEA WebLogic Server this is `t3://host:port` where: *host* Is the machine name where WebLogic Server is installed. *port* Is the port on which WebLogic server is listening. The default port if not changed at installation is 7001.
jndifactory	Is JNDI context.INITIAL_CONTEXT_FACTORY and is provided by the JNDI service provider. For WebLogic Server, the WebLogic factory is `weblogic.jndi.WLInitialContextFactory`
user	A valid user name required to access a JMS server.
password	A valid password required to access a JMS server.
errorTo	Location where error documents are sent. A predefined port name or another full URL. Optional.

5. Click *OK*.

   The event port appears under the ports node in the left pane. In the right pane, a table appears that summarizes the information associated with the event port you created. The port listing and summary are shown in the following graphic.

   You are now ready to associate the event port with a channel. For more information, see *Creating a Channel* on page 3-14.

Procedure How to Create an Event Port for MSMQ

To create an event port for MSMQ:

1. Click the *iWay Events* tab.

   The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.
3. Select the *ports* node.
4. Move the pointer over *Operations* and select *Add a new port*.

   The Create Event Port pane opens on the right.

   a. In the Port Name field, type a name for the connection, for example, Queue1_on_NTK.

      The name is used to build a repository entry as well as to identify the connection.

   b. In the Description field, type a description for the target name you just created.

   c. From the Disposition Protocol drop-down list, select *MSMQ*.

   d. In the Disposition field, enter a MSMQ destination in the form of:

      ```
      msmq:/host/private$/qName;errorTo=[pre-defined port name or another disposition url]
      ```

   The following table defines the parameters for the disposition.

Parameter	Description
host	Machine name where the Microsoft Queuing system is running.
Queue Type	Private queues are queues that are not published in Active Directory. They appear only on the local computer that contains them. Private queues are accessible only by Message Queuing applications that recognize the full path name or format name of the queue. For private queues, enter *Private$*.
qName	Name of the private queue where messages are placed.
errorTo	Location where error documents are sent. A predefined port name or another full URL. Optional.

5. Click *OK*.

   The event port appears under the ports node in the left pane. In the right pane, a table appears that summarizes the information associated with the event port you created. The summary is shown in the following graphic.

   You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page 3-14.

Procedure How to Create a Port for the SOAP Disposition

To create a port for a SOAP disposition:

1. Click the *iWay Events* tab.

   The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.

3. Select the *ports* node.

4. Move the pointer over *Operations* and select *Add a new port*.

   The Create Event Port window opens in the right pane.

   a. Type a name for the event port and provide a brief description.

   b. From the Disposition Protocol drop-down list, select *SOAP*.

   c. In the Disposition field, enter an SOAP destination, using the following format:

   ```
   soap:[wsdl-url];soapaction=[myaction];responseTo=[pre-defined port
   name or another disposition URL];errorTo=[pre-defined port name or
   another disposition url]
   ```

   The following table defines the parameters for the disposition.

Parameter	Description
wsdl-url	The URL to the WSDL file that is required to create the SOAP message. For example: `http://localhost:7001/ibse/IBSEServlet/test/sw2xml2003MQ.ibs?wsdl` This value can be found by navigating to the iWay Business Services tab and opening the *Service Description* link in a new window. The WSDL URL appears in the Address field. You can also open the WSDL file in a third party XML editor (for example, XMLSPY) and view the SOAP request settings to find this value.

Parameter	Description

soapaction	The method that will be called by the disposition. For example:
	`HIPAA.mt200Request@test@@`
	where
	`HIPAA`
	Is the name of the Web service you created using Application Explorer.
	`mt200`
	Is the method being used.
	`test`
	Is the license that is being used by the Web service.
	This value can be found by navigating to the iWay Business Services tab and opening the *Service Description* link in a new window. Perform a search for *soapAction*.
	You can also open the WSDL file in a third party XML editor (for example, XMLSPY) and view the SOAP request settings to find this value.

responseTo	The location to which responses are posted. A predefined port name or another full URL. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.
errorTo	The location to which error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

5. Click *OK*.

   The event port appears under the ports node in the left pane. In the right pane, a table appears that summarizes the information associated with the event port you created.

Procedure **How to Create an Event Port for an HTTP Disposition**

To create an event port for an HTTP disposition:

1. Click the *iWay Events* tab.

   The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.

3. Select the *ports* node.
4. Move the pointer over *Operations* and select *Add a new port*.

   The Create iWay Event Port pane opens on the right.

   a. Type an event port name and a brief description.

   b. From the disposition protocol drop-down list, select *HTTP*.

   c. From the Disposition field, enter an HTTP destination.

      When pointing Application Explorer to an **iBSE** deployment, use the following format:

```
ihttp://[myurl];responseTo=[pre-defined port name or another
disposition url];
```

   where:

   url

   Is the URL target for the post operation, for example,

   `http://myhost:1234/docroot`

   responseTo

   Is the location where responses are posted (optional).

   When pointing Application Explorer to a **JCA** deployment, use the following format:

```
http://host:port/uri
```

   where:

   host:port

   Is the combination of the name of the host on which the Web server resides and the port on which the server is listening for the post operation.

   uri

   Is the universal resource identifier that completes the url specification.

5. Click *OK*.

   The port appears under the ports node in the left pane.

Procedure How to Create an Event Port for MQ Series Disposition

To create an event port for MQ Series using Application Explorer:

1. Click the *iWay Events* tab.

   The iWay Event Adapters window opens.

2. In the left pane, expand the *HIPAA* node.

3. Select the *ports* node.
4. Move the pointer over *Operations* and select *Add a new port*.

   The Create iWay Event Port pane opens on the right.

   a. Type an event port name and a brief description.

   b. From the disposition protocol drop-down list, select *MQ Series*.

   c. In the Disposition field, enter an MQ Series destination.

      When pointing Application Explorer to an **iBSE** deployment, use the following format:

      ```
      mqseries:/qManager/
      qName;host=[hostname];port=[port];channel=[channnelname];errorTo=[
      pre-defined port name or another disposition url]
      ```

      When pointing Application Explorer to a **JCA** deployment, use the following format:

      ```
      mq:qmanager@respqueue;host=;port=;channel=
      ```

   The following table defines the parameters for the disposition.

:

Parameter	Description
qManager	Is the name of the queue manager to which the server must connect.
qName or respqueue	Name of the queue where messages are placed.
host	The host on which the MQ Server is located (for the MQ Client only).
port	The number to connect to an MQ Server queue manager (for the MQ client only).
channel	The case-sensitive name of the channel that connects with the remote MQ Server queue manager (for the MQ client only). The default channel name for MQSeries is SYSTEM.DEF.SVRCONN.
errorTo	Location where error documents are sent. This can be a predefined port name or another full URL. Optional.

5. Click *OK*.

   The newly created event port appears under the port section of the event adapter in the left pane.

Editing or Deleting an Event Port

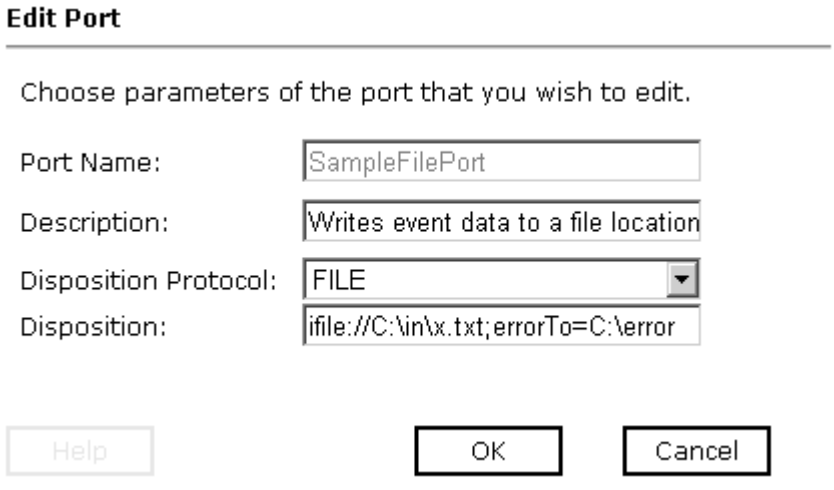
The following procedures provide information on how to modify and delete an event port.

Procedure How to Edit an Event Port

To edit an existing event port:

1. In the left pane, select the event port you want to edit.
2. In the right pane, move the pointer over *Operations* and select *Edit*.

   The Edit Port window opens. This pane provides four fields, a help button, and two action buttons.



3. Make the required changes to the Description, Disposition Protocol, or Disposition fields, and click *OK*.

   Note: The Edit Port pane does not allow you to change the name of the port, only the parameters.

Procedure How to Delete an Event Port

To delete an existing event port:

1. Select the event port you want to delete.
2. In the right pane, move the pointer over *Operations* and select *Delete*.

   A confirmation dialog box opens.

3. To delete the event port you selected, click *OK*.

The event port disappears from the list in the left pane.

Creating a Channel

The following procedure describes how to create a HIPAA channel for your iWay Event. You must associate a port to a channel before you can make the channel active.

Procedure How to Create a HIPAA Channel

To create a channel using iWay Application Explorer:

1. Click the *iWay Events* tab.

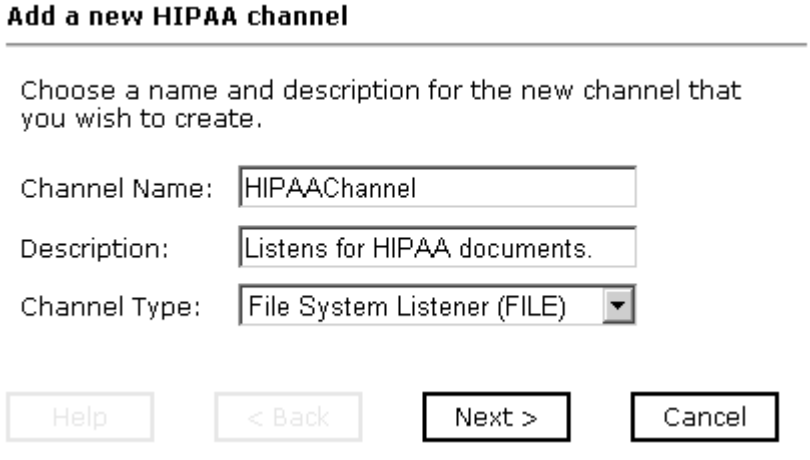
   The iWay Event Adapters window opens. The adapters that appear in the left pane support events.

2. Expand the *HIPAA* node.

   The ports and channels nodes appear in the left pane.

3. Click the *channels* node.
4. In the right pane, move the pointer over *Operations* and select *Add a new channel*.

   The Add a new channel window opens.



   a. Type a name for the channel, for example, HIPAAChannel.

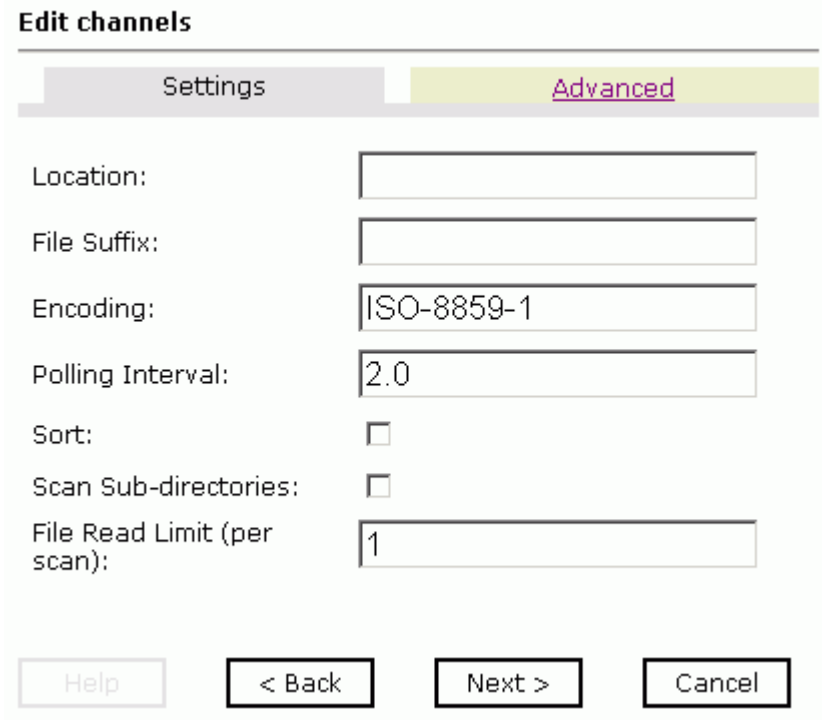
   b. Type a brief description.

c. From the drop-down list, select a type of listener:

- File System Listener (FILE)
- HyperText Transfer Protocol
- TCP Listener (TCP)
- IBM MQ Series (MQ)
- File Transfer Protocol (FTP)

5. Click *Next*.

The Edit Channels window opens in the right pane and includes fields that are specific to the type of listener you selected.



6. Provide the appropriate information that is specific to the listener you selected:

For information on the parameters for a File System Listener (FILE) listener, see *File System Listener (FILE) listener Configuration Parameters* on page 3-17.

For information on the parameters for a HyperText Transfer Protocol listener, see *HyperText Transfer Protocol Listener Configuration Parameters* on page 3-18.

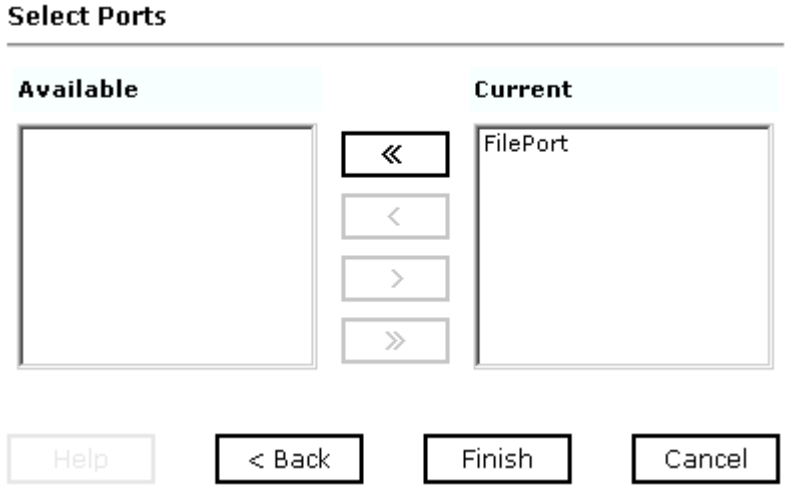
For information on the parameters for a TCP Listener, see *TCP Listener Configuration Parameters* on page 3-19.

For information on the parameters for an IBM MQ Series (MQ) listener, see *IBM MQ Series (MQ) Listener Configuration Parameters* on page 3-20.

For information on the parameters for a File Transfer Protocol (FTP) listener, see *File Transfer Protocol (FTP) Listener Configuration Parameters* on page 3-21.

7. Click *Next*.

The Select Ports pane opens, as shown in the following graphic. A list of available ports appear in Available field on the left, and the ports that are currently associated appear in the Current field on the right. This pane also contains a help button and three action buttons.



a. Select an event port from the list of current ports.

b. Click the single right (>) arrow button to transfer the port to the list of available ports. To associate all the event ports, click the double right (>>) arrow button.

8. Click *Finish*.

A summary window opens in the right pane, showing the channel description, channel status, and available ports.

All the information in the summary is associated with the channel you created.

The channel also appears under the channels node in the left pane. The following graphic shows a sample listing of a channel. An X over the icon, also shown in this graphic, indicates that the channel is currently disconnected. You must start the channel to activate your event configuration.

9. In the right pane, move the pointer over *Operations* and select *Start the channel*.

The channel you created becomes active.

The X that was over the icon disappears.

10. To stop the channel, move the pointer over *Operations* and select *Stop the channel*.

Reference **File System Listener (FILE) listener Configuration Parameters**

On the Settings tab:

Parameter	Description
Location	The directory where messages are received. DOS-style file patterns are valid for this parameter. You can specify a file pattern as well as a directory. For example, c:\xyz\ab*cd (without a file suffix) takes the file suffix from that parameter. If you use a pattern, files are selected based on the suffix and then the pattern. AB?CD selects ABxCD. AB*CD selects ABxxxCD.
File Suffix	File extension for the file event. This limits input files to those with the specified extensions. The "." is not required. The minus sign ("-") indicated that there is no extension. If the file extension is zip, the unzipped files must conform to the event schema, or they will fail. This function also works with transform configured.
Encoding	The host on which the MQ Server is located (for the MQ Client only).
Polling Interval	This is a time, expressed as xxH:xxM:xxS For example 1 hour, 2 minutes, and 3 seconds is: 1H:2M:3S The maximum interval between checks for new documents. The higher this value, the longer the interval, and the fewer system resources that are used. The side-effect of a high value is that a worker thread cannot respond to a stop command. If this value is set to 0, the listener runs once and terminates. The default value is 2 seconds.
Sort	The case-sensitive name of the channel that connects with the remote MQ Server queue manager (for the MQ client only). The default channel name for MQSeries is SYSTEM.DEF.SVRCONN.

Parameter	Description
Scan Sub-directories	Location where error documents are sent. This can be a predefined port name or another full URL. Optional.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference **HyperText Transfer Protocol Listener Configuration Parameters**

On the Settings tab:

Parameter	Description
Port	The port where the adapter listens for the HTTP transfer.
Encoding	The character set encoding for inbound documents. For example, UTF-8. The default is ISO-8859-1 US and Western Europe.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference

TCP Listener Configuration Parameters

On the Settings tab:

Parameter	Description
Port	The port where the adapter listens for the TCP transfer.
Encoding	The character set encoding for inbound documents. For example, UTF-8. The default is ISO-8859-1 US and Western Europe.
Allowable Client Host	The name or address of the client restricted to accessing this adapter.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.

Parameter	Description
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference IBM MQ Series (MQ) Listener Configuration Parameters

On the Settings tab:

Parameter	Description
Queue Manager	The name of the MQ queue manager to be used.
Queue Name	The name of the MQ Series or WebSphere MQ queue that the HIPAA system polls.
Polling Interval	The maximum wait interval (in the format *nn*H:*nn*M:*nn*S) between checks for new documents. The higher this value, the longer the interval, and the fewer system resources that are used. However, with a high value, the worker thread cannot respond to a stop command. If timeout is set to 0, the listener runs once and terminates. The default is 2 seconds.

On the MQ Client tab:

Parameter	Description
Host	The host where the MQ Server is located.
Port	The port number used to connect to an MQ Server.
Channel	The channel between an MQ Client and an MQ Server.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.

Parameter	Description
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference

File Transfer Protocol (FTP) Listener Configuration Parameters

On the Settings tab:

Parameter	Description
Host	The name of the FTP host.
Port	The port where the adapter listens on the FTP transfer.
User	The user name to log onto the FTP Server.
Password	The password for the FTP user.
Location	The directory where messages are received. DOS-style file patterns are available for this parameter. You can specify a file pattern as well as a directory. For example, c:\xyz\ab*cd (without a file suffix) takes the file suffix from that parameter. If you use a pattern, files are selected based on the suffix and then the pattern. AB?CD selects ABxCD. AB*CD selects ABxxxCD.
Encoding	The character set encoding for inbound documents. For example, UTF-8. The default is ISO-8859-1 US and Western Europe.
Polling Interval	The maximum wait interval (in the format *nn*H:*nn*M:*nn*S) between checks for new documents. The higher this value, the longer the interval, and the fewer system resources that are used. However, with a high value, the worker thread cannot respond to a stop command. If timeout is set to 0, the listener runs once and terminates. The default is 2 seconds.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Procedure How to Edit a Channel

To edit an existing channel:

1. In the left pane, select the channel you want to edit.
2. In the right pane, move the pointer over *Operations* and select *Edit*.

   The Edit channels window opens.
3. Make the required changes to the channel configuration and click *Finish*.

Procedure How to Delete a Channel

To delete an existing channel:

1. In the left pane, select the channel you want to delete.
2. In the right pane, move the pointer over *Operations* and select *Delete*.

   A confirmation dialog box opens.
3. To delete the channel you selected, click *OK*.

   The channel disappears from the list in the left pane.

CHAPTER 4

Using Web Services Policy-Based Security

Topics:

- Web Services Policy-Based Security
- Configuring Web Services Policy-Based Security

iWay Servlet Application Explorer provides a security feature called Web services policy-based security. The following topics describe how this feature works and how to configure it.

Web Services Policy-Based Security

Web services provide a layer of abstraction between the back-end business logic they invoke and the user or application running the Web service. This enables easy application integration but raises the issue of controlling the use and execution of critical and sensitive business logic that is run as a Web service.

iWay Servlet Application Explorer controls the use of Web services that use iWay adapters using a feature called policy-based security. This feature enables an administrator to apply "policies" to iWay Business Services (Web services) to deny or permit their execution.

A policy is a set of privileges dealing with the execution of an iWay Business Service (iBS) that can be applied to an existing or new iBS. When you set specific rights or privileges inside a policy, you do not have to recreate privileges for every iBS that has security concerns in common with other iWay Business Services. Instead, you can use one policy for many iWay Business Services.

The goal of the feature is to secure requests at both the transport and the SOAP request level transmitted on the wire. Some policies do not deal with security issues directly but do effect the run-time behavior of the Web services to which they are applied.

The iBS administrator creates an "instance" of a policy type, names it, associates individual users and/or groups (a collection of users), and then applies that policy to one or more iWay Business Services.

You can assign a policy to an iBS, or to a method within an iBS. If a policy is applied only to a method, other methods in that iBS are not governed by it. However, if a policy is applied to the iBS, all methods are governed by it. At run time, the user ID and password that are sent to iBSE in the SOAP request message are checked against the list of users for all policies applied to that specific iBS. The policy type that is supported is Resource Execution, which dictates who can or cannot execute the iBS.

When a policy is not applied, the default value for an iBS is to "grant all". For example, anybody can execute the iBS, until the Resource Execution policy is associated to the iBS. At that time, only those granted execution permission, or users who are not part of a group that was denied execution permissions, have access to the iBS.

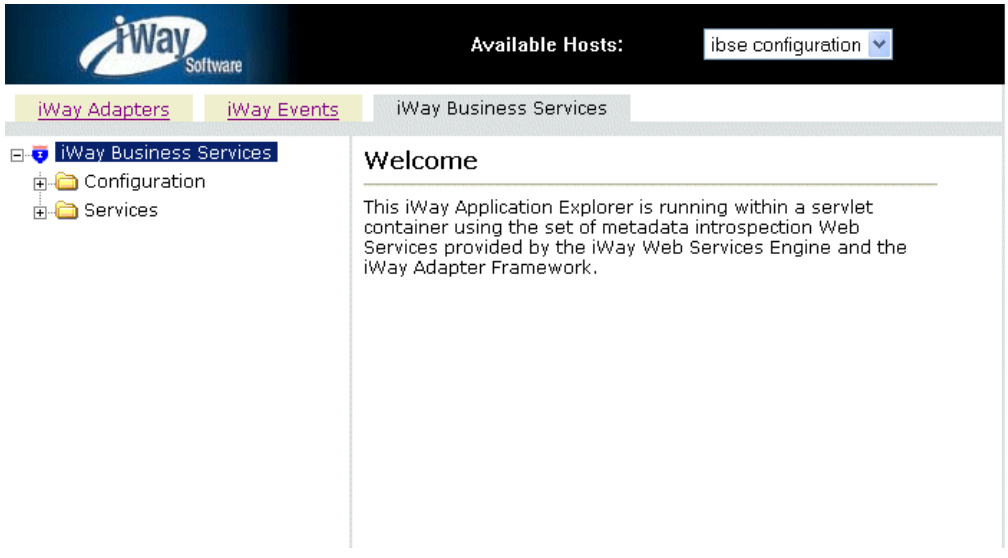
Configuring Web Services Policy-Based Security

The following procedure describes how to configure iBSE policy-based security.

Procedure How to Create and Associate a User With a Policy

Before you create instances of policies, you must have a minimum of one user or one group to associate to an instance. You can create users and groups using iWay Servlet Application Explorer.

1. Open *iWay Servlet Application Explorer*.



   a. Select the *iWay Business Services* tab.

   b. Expand the *Configuration* node.

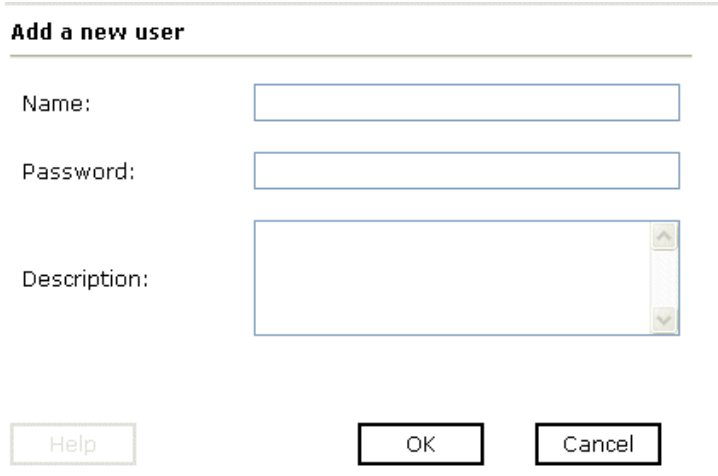
   c. Expand the *Security* node.

   d. Expand the *Users and Groups* node.

   e. Select *Users*.

2. In the right pane, move the pointer over *Operations* and select *Add*.

The Add a new user pane opens.



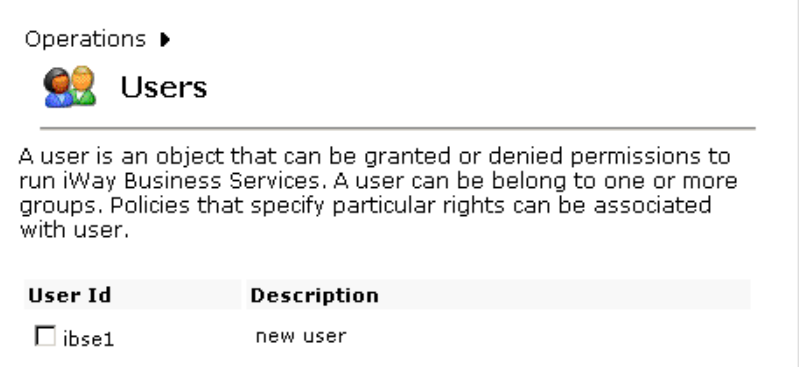
a. In the Name field, type a user ID.

b. In the Password field, type the password associated with the user ID.

c. In the Description field, type a description of the user (optional).

3. Click *OK*.

The new user is added to the configuration.

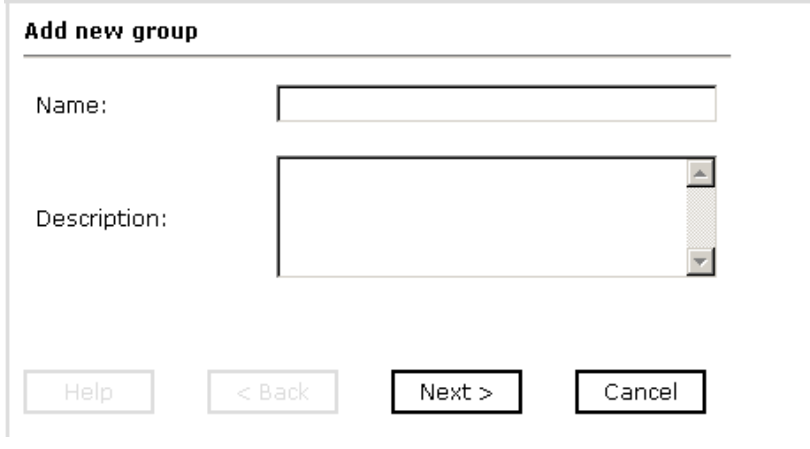


Procedure How to Create a Group to Use With a Policy

To create a group to use with a policy:

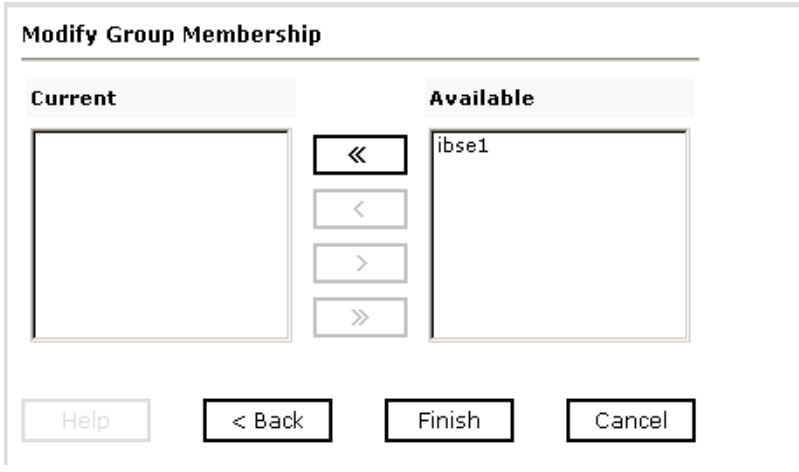
1. Open *iWay Servlet Application Explorer*.
   a. Select the *iWay Business Services* tab.
   b. Expand the *Configuration* node.
   c. Expand the *Security* node.
   d. Expand the *Users and Groups* node.
   e. Select *Groups*.
2. In the right pane, move the pointer over *Operations* and click *Add*.

   The Add new group pane opens.



   a. In the Name field, type a a name for the group.
   b. In the Description field, type a description for the group (optional).
3. Click *Next*.

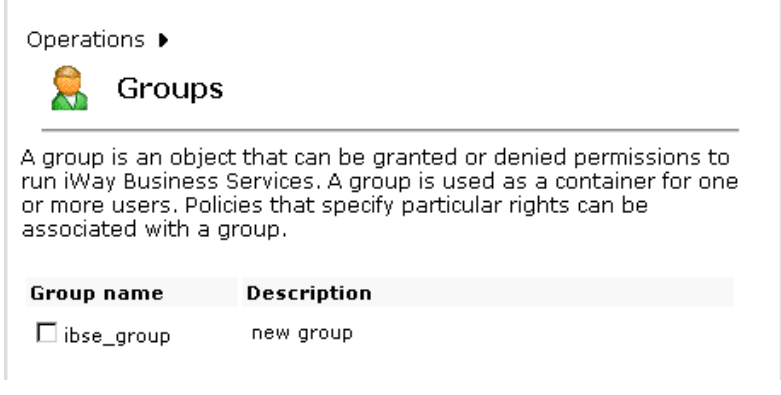
The Modify Group Membership pane opens.



You can either highlight a single user in the list of available users and add it by clicking the left arrow, or you can click the double left arrow to add all users in the list of available users to the group.

4. After you select a minimum of one user, click *Finish*.

   The new group is added to the configuration.



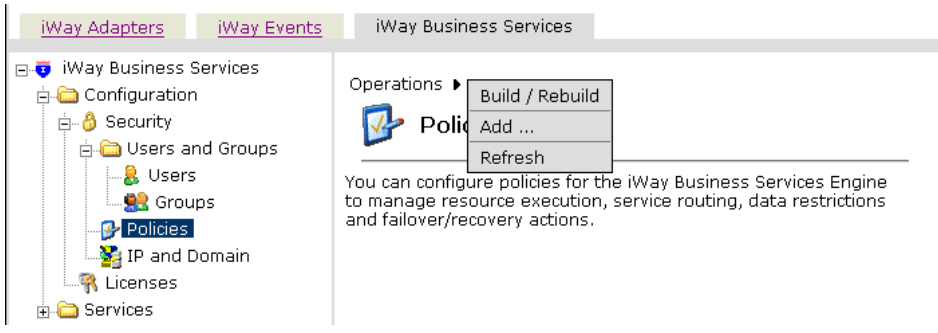
Procedure How to Create an Execution Policy

An execution policy governs who can execute the iBS to which the policy is applied.

To create a group to use with a policy:

1. Open *iWay Servlet Application Explorer*.
   a. Select the *iWay Business Services* tab.

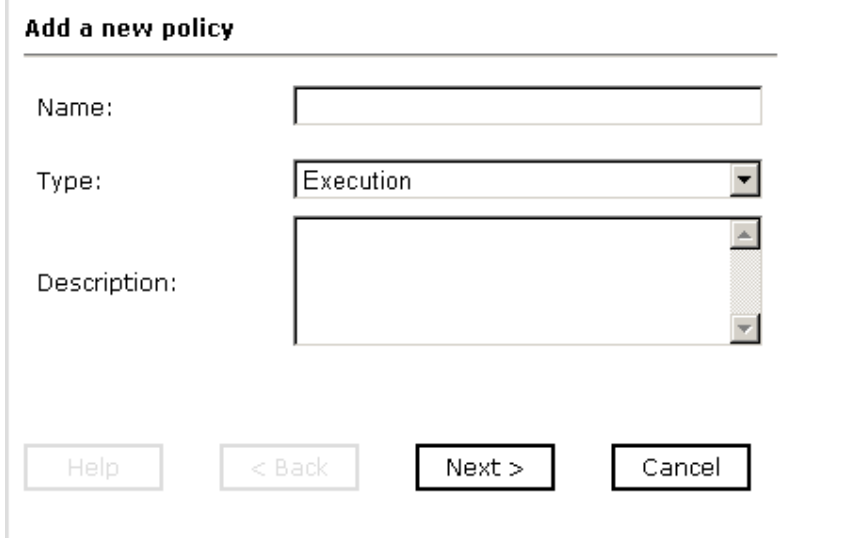
b. Expand the *Configuration* node.



c. Select *Policies*.

2. In the right pane, move the pointer over *Operations* and click *Add*.

The Add a new policy pane opens.



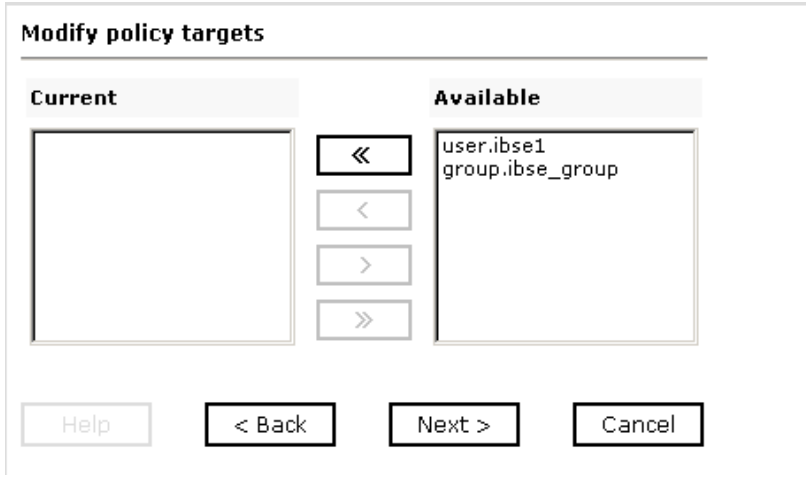
a. In the Name field, type a a name for the policy.

b. From the Type drop-down list, select *Execution*.

c. In the Description field, type a description for the policy (optional).

3. Click *Next*.

The Modify policy targets pane opens.

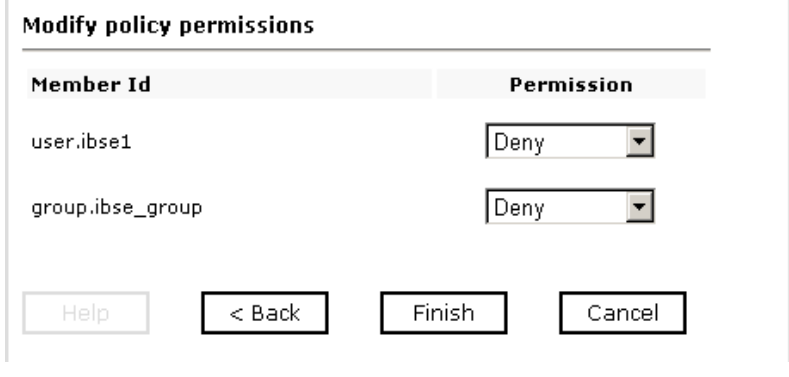


4. Select a minimum of one user or group from the Available pane.

   Note: This user ID is checked against the value in the user ID element of the SOAP header sent to iBSE in a SOAP request.

5. Click *Next*.

   The Modify policy permissions pane opens.

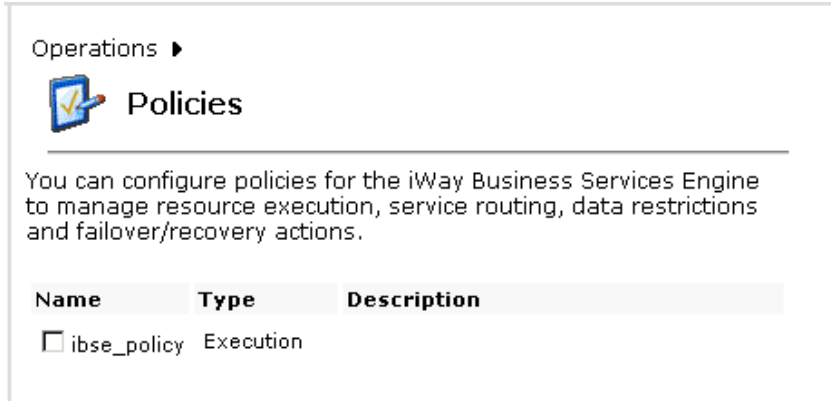


   You select whether users or groups may execute the iBS.

6. From the Permission drop-down lists, select *Grant* to permit execution or *Deny* to restrict execution.

7. Click *Finish*.

The following pane summarizes your configuration.



Configuring the IP and Domain Restrictions Policy Type

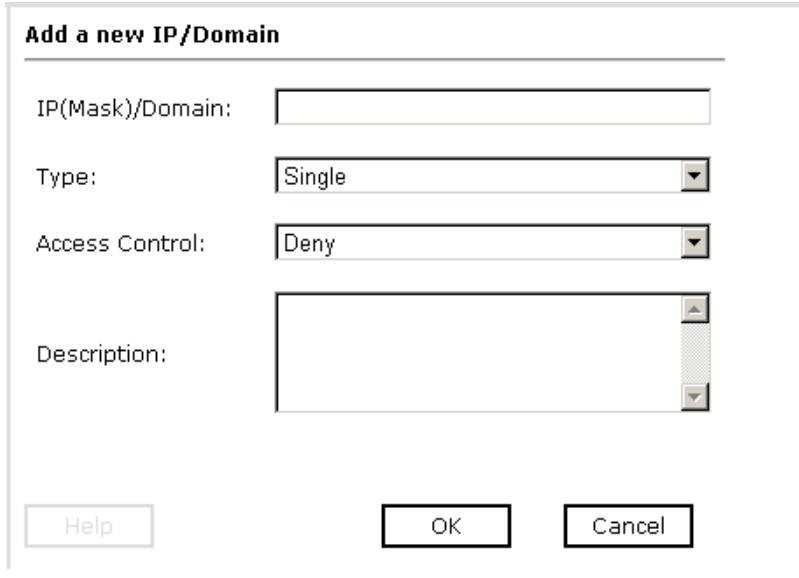
You configure the IP and Domain Restriction policy type slightly differently from other policy types. The IP and Domain Restriction policy type controls connection access to iBSE and therefore need not be applied to individual Web services. You need not create a policy, however, you must enable the Security Policy option in iWay Servlet Application Explorer.

Procedure How to Configure IP and Domain Restrictions

1. Open *iWay Servlet Application Explorer*.
   a. Select the *iWay Business Services* tab.
   b. Expand the *Configuration* node.
   c. Expand the *Security* node.

   d. Select *IP and Domain*.
2. In the right pane, move the pointer over *Operations* and click *Add*.

The Add a new IP/Domain pane opens.



a. From the Type drop-down list, select the type of restriction.

b. In the IP(Mask)/Domain field, type the IP or domain name using the following guidelines.

If you select Single (Computer) from the Type drop-down list, you must provide the IP address for that computer. If you only know the DNS name for the computer, click *DNS Lookup* to obtain the IP Address based on the DNS name.

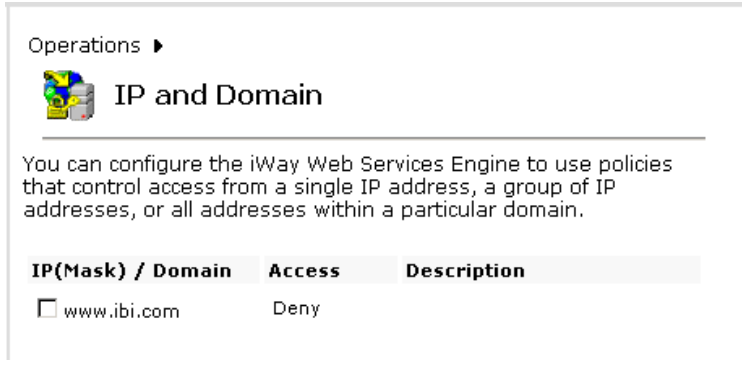
If you select Group (of Computers), you must provide the IP address and subnet mask for the computer group.

If you select Domain, you must provide the domain name, for example, yahoo.com.

3. From the Access Control drop-down list, select *Grant* to permit access or *Deny* to restrict access for the IP addresses and domain names you are adding.

4. Click *OK*.

The following pane summarizes your configuration.



CHAPTER 5

Management and Monitoring

Topics:

- Managing and Monitoring Services and Events Using iBSE
- Managing and Monitoring Services and Events Using iWay JCA
- Setting Engine Log Levels
- Configuring Connection Pool Sizes

Once you have created services and events using iWay Application Explorer, you can use managing and monitoring tools provided by iBSE and JCA to gauge the performance of your run-time environment. The following section describe how to configure and use these features.

Managing and Monitoring Services and Events Using iBSE

iBSE provides a console to manage and monitor services and events currently in use and display resource usage and invocation statistics. These indicators can help you adjust your environment for optimum efficiency.

The following monitoring levels are available for services:

- System
- Service
- Method

The following monitoring levels are available for events:

- System
- Channel
- Port

Procedure How to Access the Monitoring Console

To access the monitoring console:

1. Ensure that BEA WebLogic Server is started.
2. Enter the following URL in your Web browser:

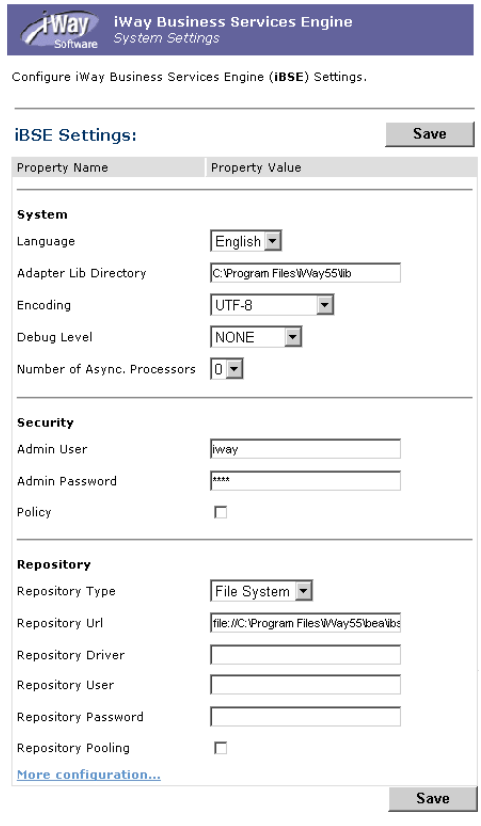
   `http://localhost:7001/ibse/IBSEConfig`

   where:

   localhost

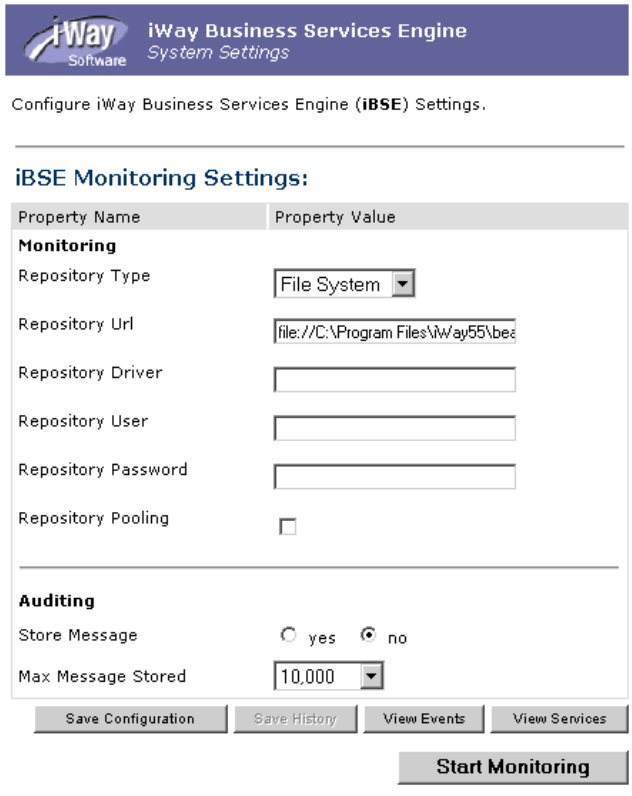
   Is where your application server is running.

The iBSE Settings page opens:



3. Scroll to the bottom of the page and click *More configuration*.

The iBSE Monitoring Settings page opens:



Tip: To access the monitoring console directly, enter the following URL in your Web browser:

`http://localhost:7001/ibse/IBSEStatus`

where:

localhost

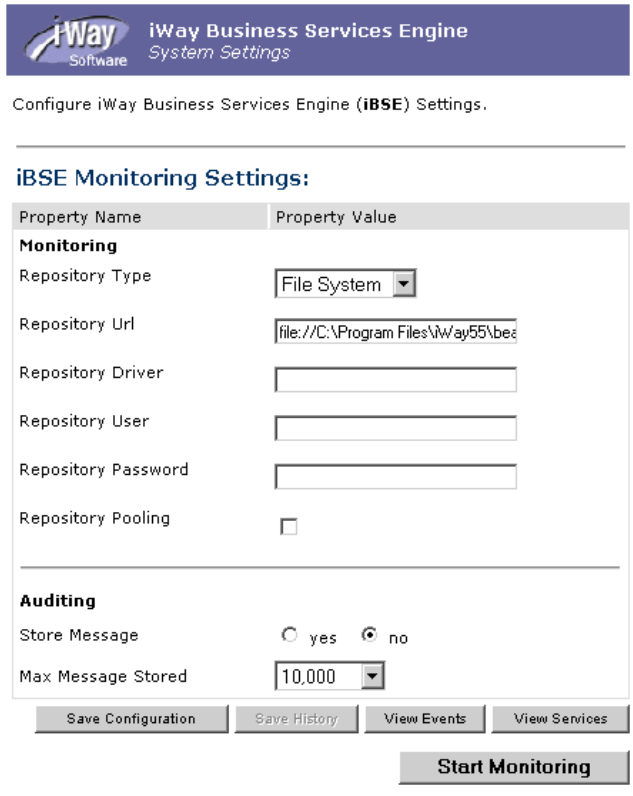
Is where your application server is running.

Procedure How to Configure Monitoring Settings

To configure monitoring settings:

1. Ensure that BEA WebLogic Server is started.
2. Access the monitoring console.

The iBSE Monitoring Settings page opens:



3. Perform the following steps in the Monitoring section:

   a. Select the type of repository you are using from the Repository Type drop-down list.

   b. Enter a JDBC URL to connect to the database in the Repository URL field.

   c. Enter a JDBC Class to connect to the database in the Repository Driver field.

   d. Enter a user ID and password to access the monitoring repository database.

   e. Click the *Repository pooling* check box if you want to enable pooling.

4. Perform the following steps in the Auditing section:

   a. Select *yes* if you want to store messages. This option is disabled by default.

      Note: You must start and then stop monitoring to enable this option.

   b. Select the maximum number of messages you want to store. By default, 10,000 is selected.

Note: Depending on your environment and the number of messages that are exchanged, storing a large number of messages may affect system performance. If you need more information about your system's resources, consult your system administrator.

5. Click *Save Configuration*.
6. Click *Start Monitoring*.

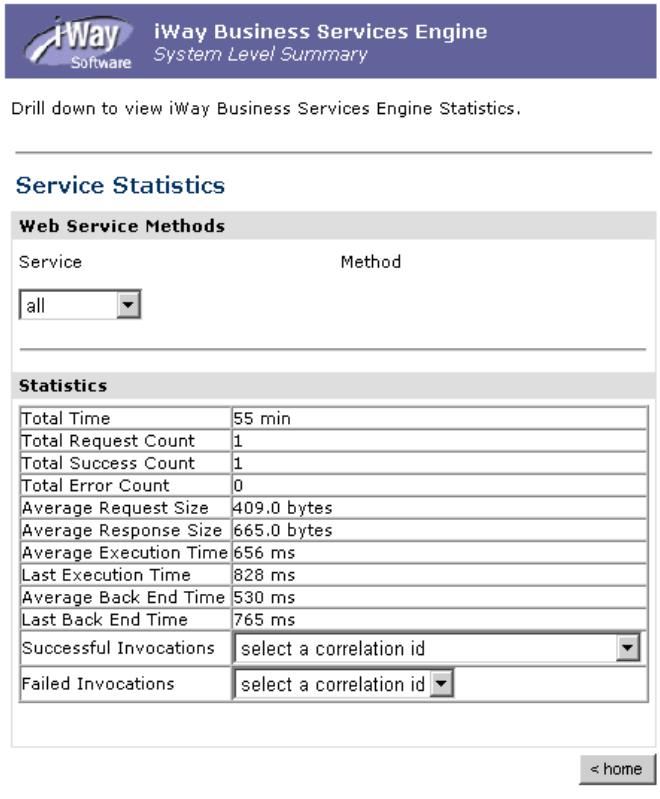
iBSE begins to monitor all services and events currently in use and store messages, if you selected this option. If you want to stop monitoring, click *Stop Monitoring*.

Procedure **How to Monitor Services**

To monitor services:

1. Ensure that BEA WebLogic Server is started.
2. Click *Start Monitoring* from the iBSE Monitoring Settings page.
3. Click *View Services*.

The System Level Summary page opens.



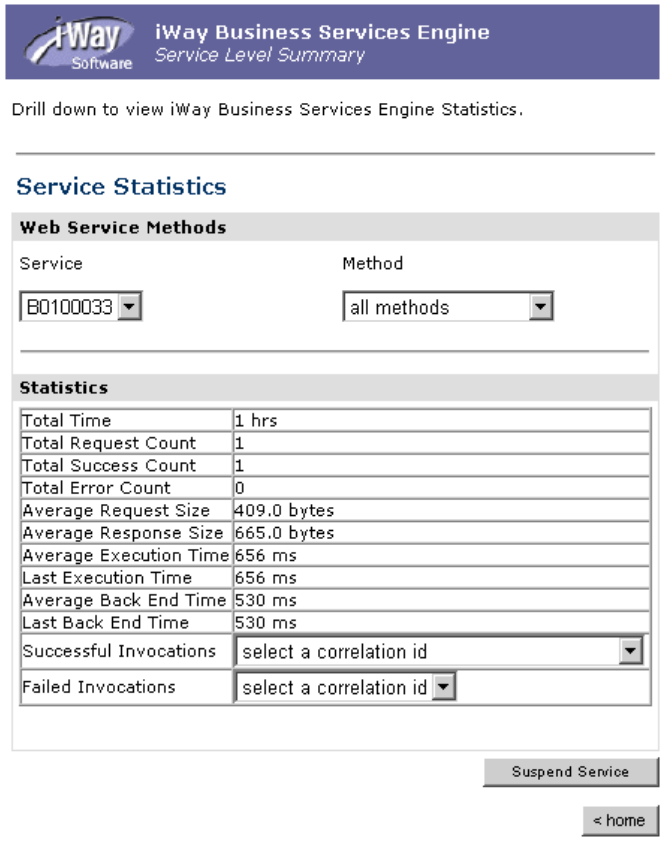
The system level summary provides services statistics at a system level. The following table provides a description of each statistic.

Statistic	Description
Total Time	The total amount of time iBSE is monitoring services. This time starts when you click *Start Monitoring* from the iBSE Monitoring Settings page.
Total Request Count	The total number of services requests that were made during this monitoring session.
Total Success Count	The total number of successful service executions.

Statistic	Description
Total Error Count	The total number of errors that were encountered.
Average Request Size	The average size of a service request that is available.
Average Response Size	The average size of a service response size that is available.
Average Execution Time	The average execution time for a service.
Last Execution Time	The last execution time for a service.
Average Back End Time	The average back end time.
Last Back End Time	The last back end time.
Successful Invocations	A list of successful services listed by correlation ID. Select a service from the drop-down list to retrieve more information for that service.
Failed Invocations	A list of failed services listed by correlation ID. Select a service from the drop-down list to retrieve more information for that service.

4. Select a service from the drop-down list.

The Service Level Summary page opens.



A list of available methods for that service appears in the Method drop-down list.

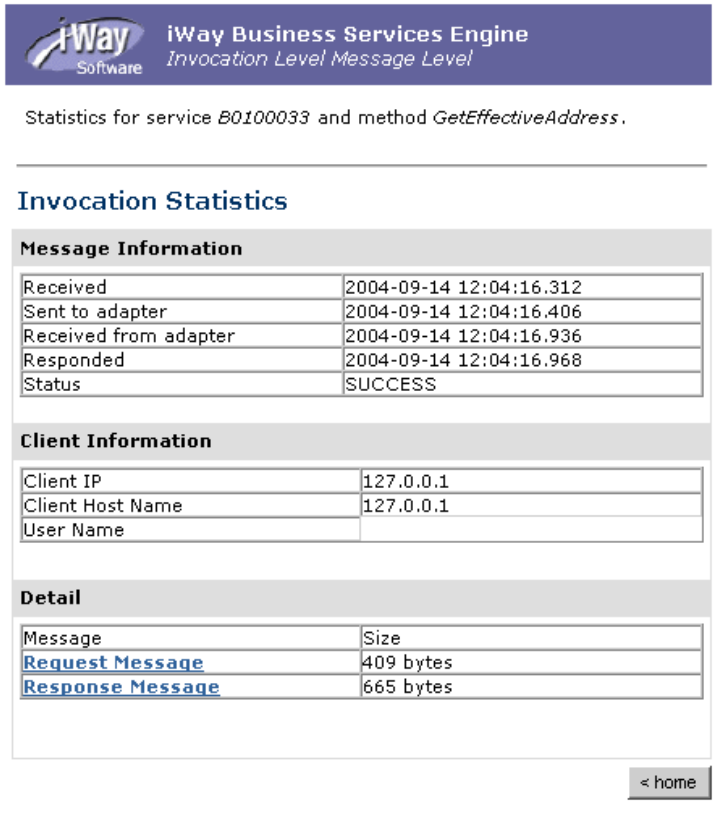
To stop a service at any time, click *Suspend Service*. To start the service, click *Resume Service*.

5. Select a method for the service from the Method drop-down list.

The Method Level Summary page opens.

6. For additional information about a service and its method that is successful, select a service based on its correlation ID from the Successful Invocation drop-down list.

The Invocation Level Statistics page opens.



Information pertaining to the message and client is provided.

7. Click the *Request Message* link to view the XML request document in your Web browser.

   You can also view the XML response document for the service.

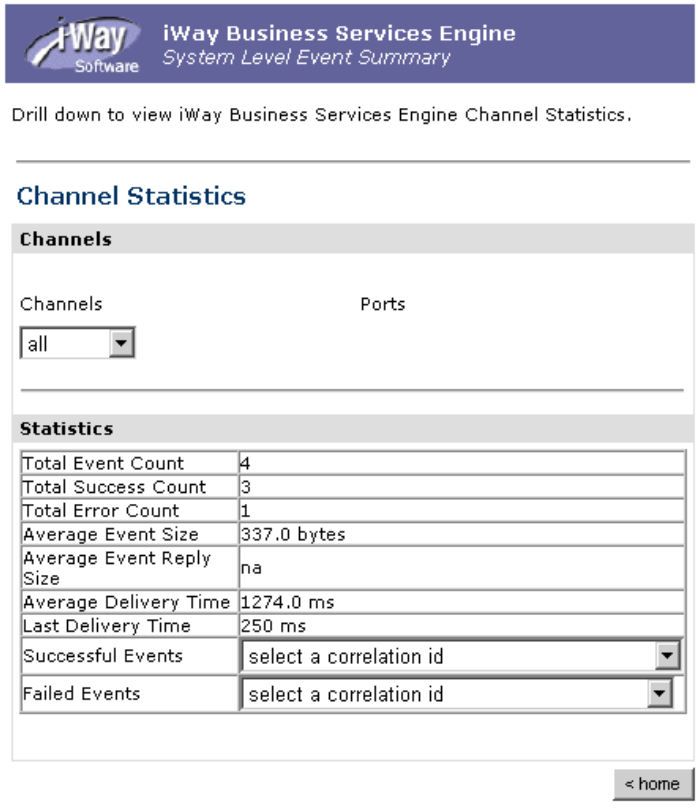
8. Click *home* to return to the iBSE Monitoring Settings page.

Procedure How to Monitor Events

To monitor events:

1. Ensure that BEA WebLogic Server is started.
2. Click *Start Monitoring* from the iBSE Monitoring Settings page.
3. Click *View Events.*

   The System Level Summary page opens.



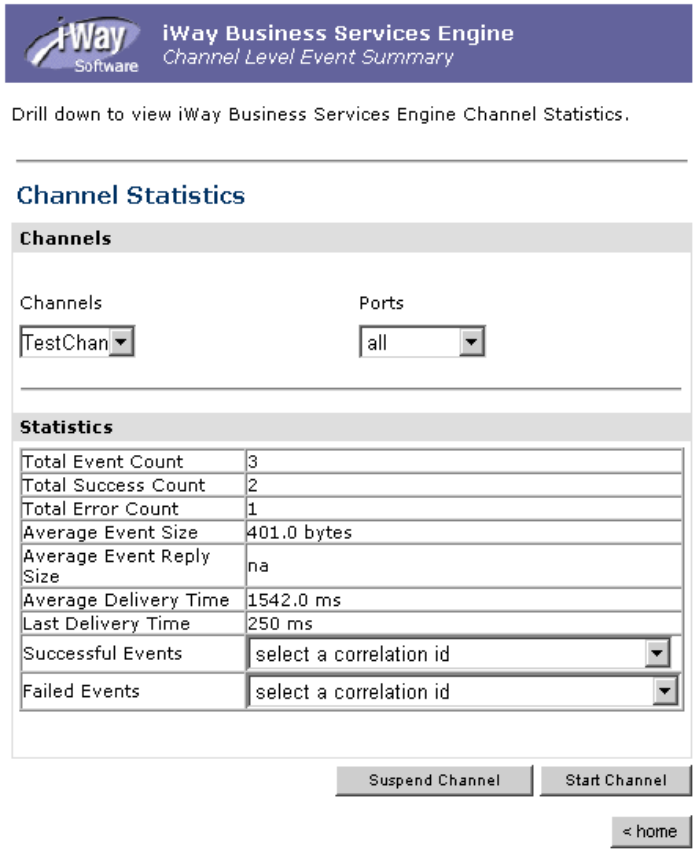
The system level summary provides event statistics at a system level. The following table provides a description of each statistic.

Statistic	Description
Total Event Count	The total number of events.
Total Success Count	The total number of successful event executions.
Total Error Count	The total number of errors that were encountered.
Average Event Size	The average size of an event request that is available.
Average Event Reply Size	The average size of an event response that is available.

Statistic	Description
Average Delivery Time	The average delivery time for an event.
Last Execution Time	The last execution time for an event.
Last Delivery Time	The last delivery time.
Successful Events	A list of successful events listed by correlation ID. Select an event from the drop-down list to retrieve more information for that event.
Failed Events	A list of failed events listed by correlation ID. Select an event from the drop-down list to retrieve more information for that event.

4. Select a channel from the drop-down list.

The Channel Level Event Summary page opens.

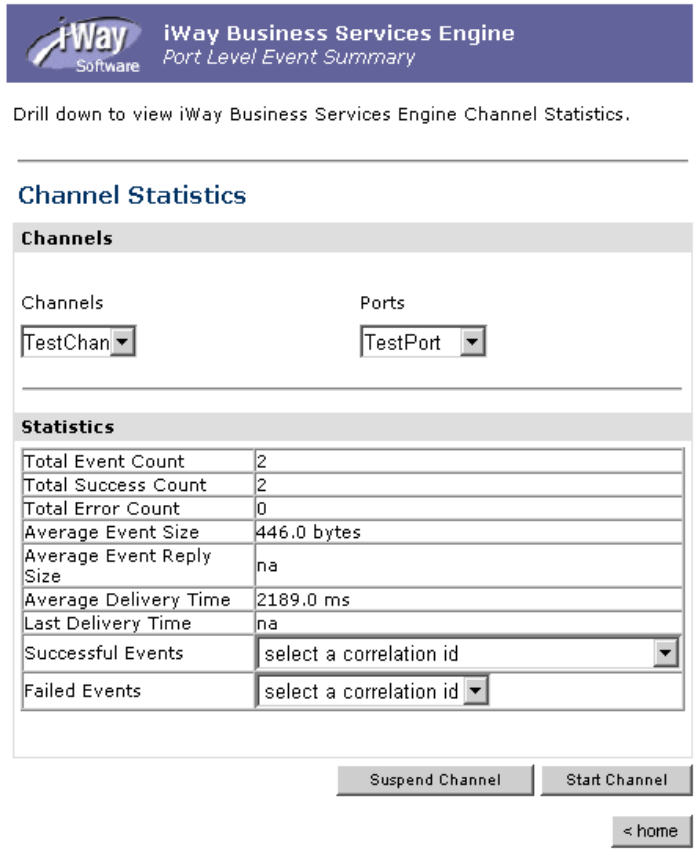


A list of available ports for that channel appears in the Ports drop-down list.

To stop a channel at any time, click *Suspend Channel*. To start the service, click *Start Channel*.

5. Select a port for the channel from the Ports drop-down list.

The Port Level Event Summary page opens.



6. For additional information about an event and its port that is successful, select an event based on its correlation ID from the Successful Events drop-down list.

The Event Level Statistics page for the channel and port you selected opens.

Information pertaining to the event message is provided.

7. Click the *Event Message* link to view the XML event document in your Web browser.
8. Click *home* to return to the iBSE Monitoring Settings page.

Managing and Monitoring Services and Events Using iWay JCA

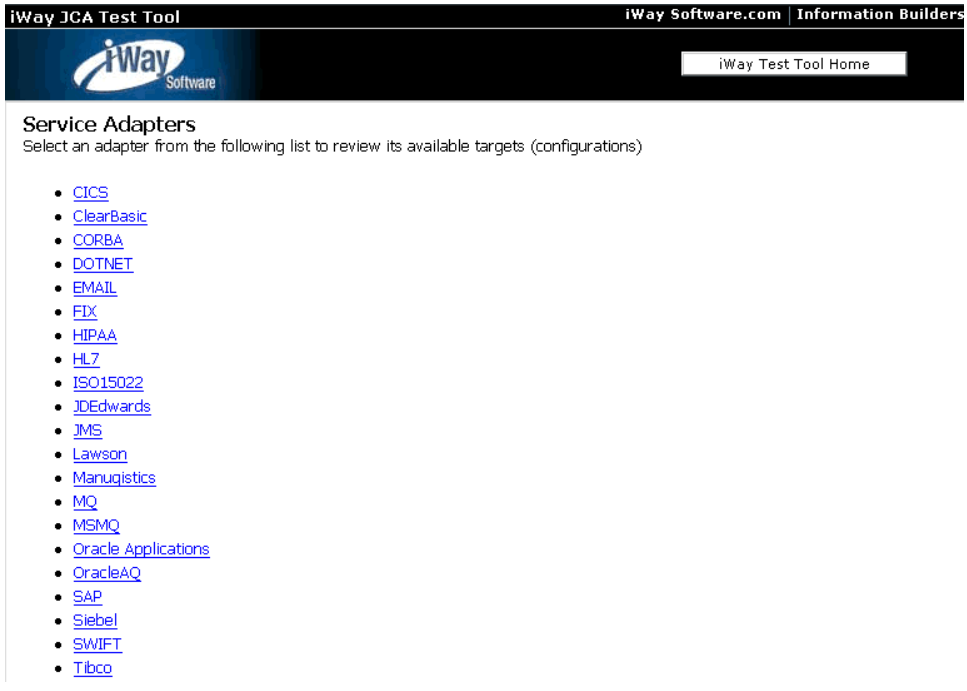
The following topics describe how to test service and event adapters using the iWay JCA Installation Verification Program (IVP).

Procedure How to Test the iWay Service Adapters

To test the iWay service adapters using the IVP:

1. To ensure that the targets you configured in iWay Application Explorer appear in the IVP, click *Refresh Manage Connection Factory.*
2. To display the available adapters, click the *Service adapters* link.

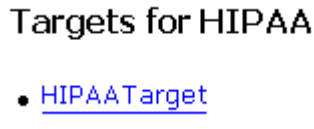
The following window, showing the list of deployed service adapters, opens.



3. Select the adapter that you want to test.

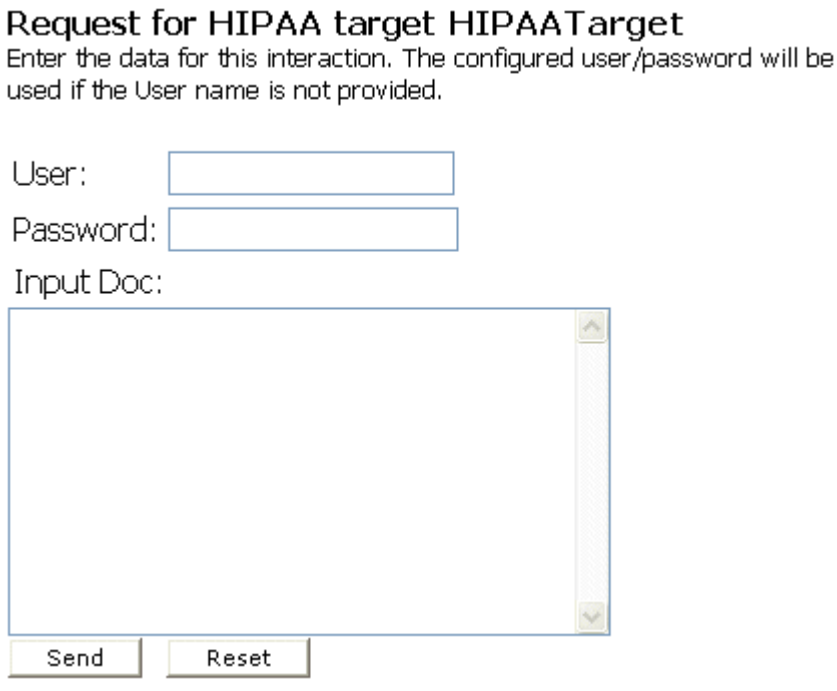
The adapter displays all of the targets currently configured in the iWay repository for that adapter.

The following window shows that there is one target, HIPAATarget, configured for the iWay Adapter for HIPAA.



4. Click the desired target, for example, *HIPAATarget*.

   The following pane, showing an input area in which you can provide XML code with which to test the adapter, opens.



5. Enter a username and password to connect to HIPAA.
6. In the input area, enter a request document built from the iWay request schema.
7. Click *Send*.

   A response is returned from HIPAA.

Testing the iWay Event Adapters Using the IVP

The iWay JCA Installation Verification Program (IVP) enables you to start and stop iWay event channels.

The tool also enables you to monitor events and provides statistics on channels.

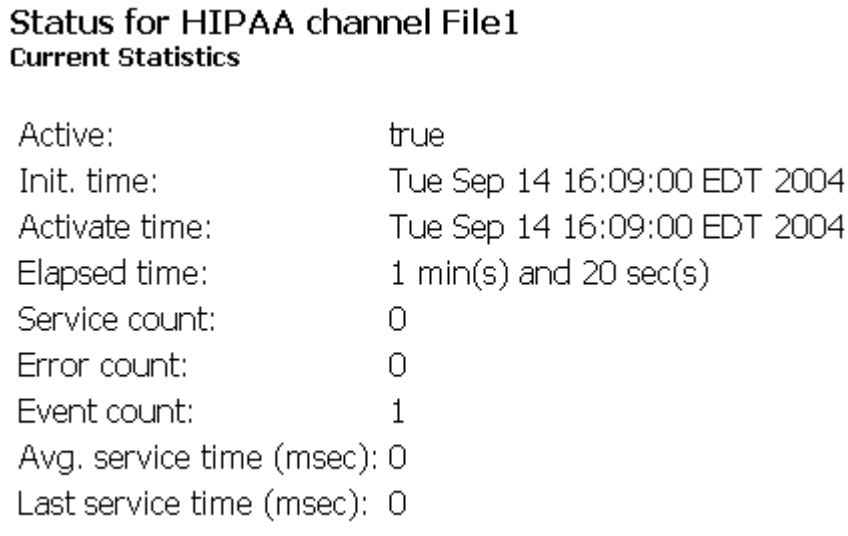
Procedure How to Test the iWay Event Adapters

To test the iWay event adapters using the IVP:

1. Click *Refresh Manage Connection Factory.*
2. To display the available adapters, click the *Events adapter* link.
3. Select the adapter that you want to monitor, for example, HIPAA.

   The tool displays the channels that you already configured.

4. Click the *start* hyperlink to start the channel.



   Statistics for the event channel are returned, including:

   - The status of the channel.
   - The time the channel was initialized.
   - The number of events.
   - The event response time.

5. To stop the channel, click the *stop* hyperlink.

Monitoring Services

The following section describes how to use the iWay JCA Installation Verification Program (IVP) in Managed mode and monitor services in BEA WebLogic.

Procedure How to Use iWay JCA IVP in Managed Mode.

To use iWay JCA IVP in managed mode:

1. Open the *web.xml* file in a text editor.

   It is located in the following directory:

   ```
   <installDir>\bea\iwjcaivp\WEB-INF\web.xml
   ```

   where:

   <installDir>

   Is the location of your iWay 5.5 installation.

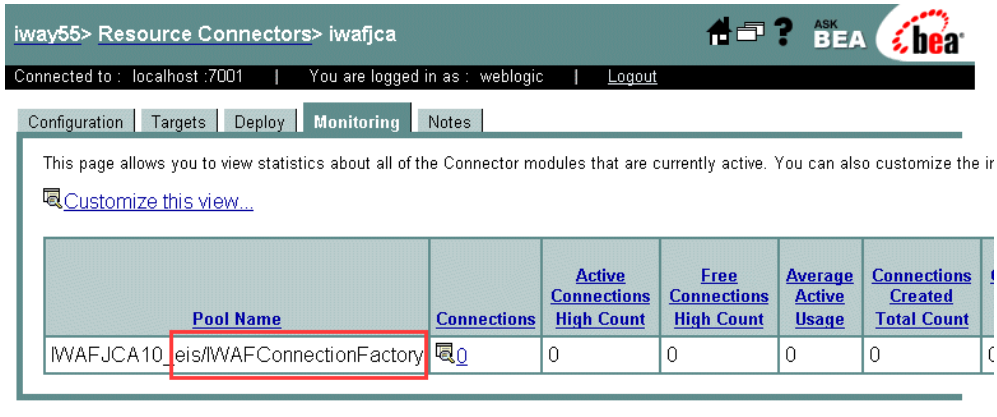
2. Locate the following lines:

   ```
   <context-param><param-name>iway.jndi</param-name><param-value></param-value><description>JNDI name for the IWAF JCA Resource Adapter. If not provided, the application will create a new one based on iway.home, iway.config and iway.loglevel.</description></context-param>
   ```

3. Enter the path to the JCA module for the iway.jndi parameter, for example:

   ```
   <param-value>eis/IWAFConnectionFactory</param-value>
   ```

   You can find this value by browsing to the Resource Connectors section in BEA WebLogic and checking the Pool Name for the JCA connector module. For example:



4. Restart WebLogic Server or redeploy the JCA connector module.

5. Open a browser to:

`http://hostname:port/iwjcaivp`

where:

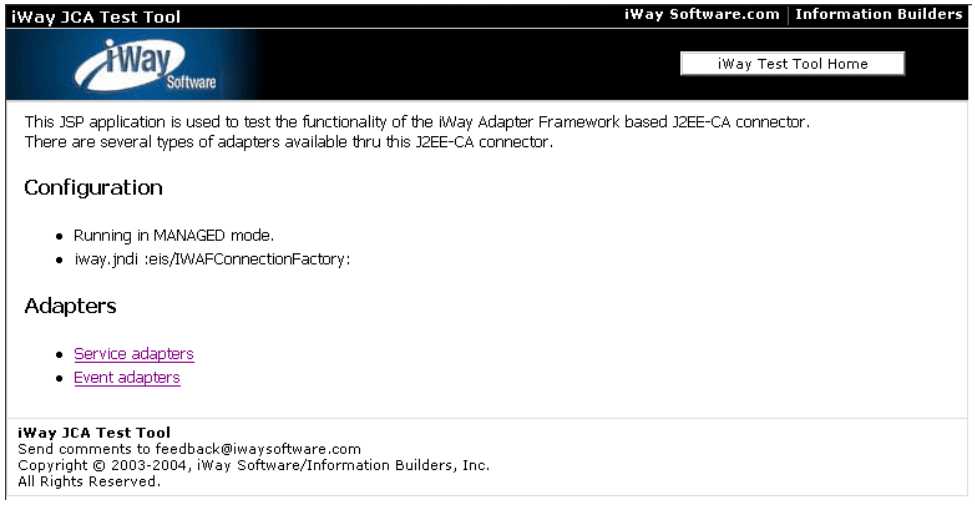
hostname

Is the name of the machine where your application server is running.

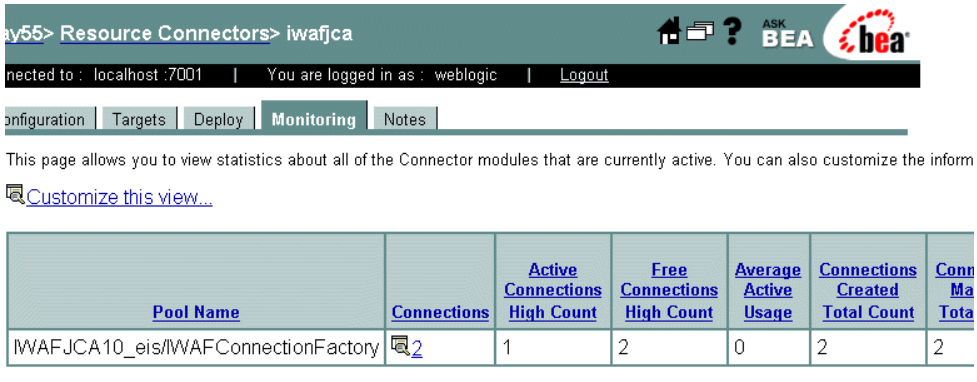
port

Is the port for the domain you are using for iWay. The port for the default domain is 7001.

The iWay JCA Test Tool window opens and provides links for viewing iWay Service or Event adapters. Notice that it is now running in managed mode.



6. Test a service you have created for an iWay Adapter using Application Explorer.
7. Return to the Resource Connectors section in BEA WebLogic.



Monitoring statistics pertaining to the services you have executed are now available.

Setting Engine Log Levels

The following section describes how to set engine log levels for Servlet iBSE and JCA. For more information, see the *iWay Installation and Configuration for BEA WebLogic* documentation.

Procedure How to Enable Tracing for Servlet iBSE

To enable tracing for Servlet iBSE:

1. Open the Servlet iBSE configuration page:

   `http://hostname:port/ibse/IBSEConfig`

   where:

   hostname

   Is the hostname of the application server machine.

   port

   Is the port for the domain you are using for iWay. The port for the default domain is 7001.

   For example:

   `http://localhost:7001/ibse/IBSEConfig`

2. In the top *System* area, specify the level of tracing from the *Debug* drop-down list.
3. Click *Save*.

The default location for the trace information on Windows is:

`C:\Program FIles\bea\ibse\ibselogs`

Procedure How to Enable Tracing for JCA

To enable tracing for JCA:

1. Open the extracted ra.xml file in a text editor.
2. Locate and change the following setting:

   LogLevel. This can be set to DEBUG, INFO, or ERROR.

```
<context-param>
<config-property>
    <config-property-name>LogLevel</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value></config-property-value>
</config-property>
```

For example:

```
<config-property-value>DEBUG</config-property-value>
```

A directory in the configuration directory contains the logs. Also, be sure to review logs generated by your application server.

Leave the remainder of this file unchanged.

3. Save the file and exit the editor.
4. Redeploy the connector.

Configuring Connection Pool Sizes

The following section describes how to configure connection pool sizes using JCA.

Procedure How to Configure Connection Pool Sizes

To configure connection pool sizes:

1. Open the extracted weblogic-ra.xml file in a text editor.
2. Locate and change the following setting:

   pool-params. The JCA Resource Connector has an initial capacity value of 0 by default, and cannot be changed. The maximum capacity value is 10 by default and can be changed to a higher value.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE weblogic-connection-factory-dd (View Source for full
doctype...)>
- <weblogic-connection-factory-dd>
  <connection-factory-name>IWAFJCA</connection-factory-name>
  <jndi-name>eis/IWAFConnectionFactory</jndi-name>
  - <pool-params>
    <initial-capacity>0</initial-capacity>
    <max-capacity>10</max-capacity>
    <capacity-increment>1</capacity-increment>
    <shrinking-enabled>false</shrinking-enabled>
    <shrink-period-minutes>200</shrink-period-minutes>
  </pool-params>
  <security-principal-map />
</weblogic-connection-factory-dd>
```

3. Save the file and exit the editor.
4. Redeploy the connector.

APPENDIX A

Using Application Explorer in BEA WebLogic Workshop

Topics:

- Starting Application Explorer in BEA WebLogic Workshop
- Creating a New Configuration
- Connecting to HIPAA
- Creating an XML Schema
- Creating an iWay Business Service
- Understanding iWay Event Functionality
- Creating an Event Port
- Modifying an Event Port
- Creating a Channel
- Modifying a Channel
- Deploying iWay Components in a Clustered BEA WebLogic Environment
- Adding a Control for an iWay Resource in BEA WebLogic Workshop
- Adding an iWay Extensible CCI Control to a BEA WebLogic Workshop Application

This section describes how to use iWay Java Swing Application Explorer running in BEA WebLogic Workshop to create XML schemas for HIPAA. In addition, this section provides information on listening for events in HIPAA and creating Web services that are published by the iWay Business Services Engine (iBSE).

Starting Application Explorer in BEA WebLogic Workshop

The server must be started where iWay Application Explorer is running. Before you can use Application Explorer, you must start BEA WebLogic server.

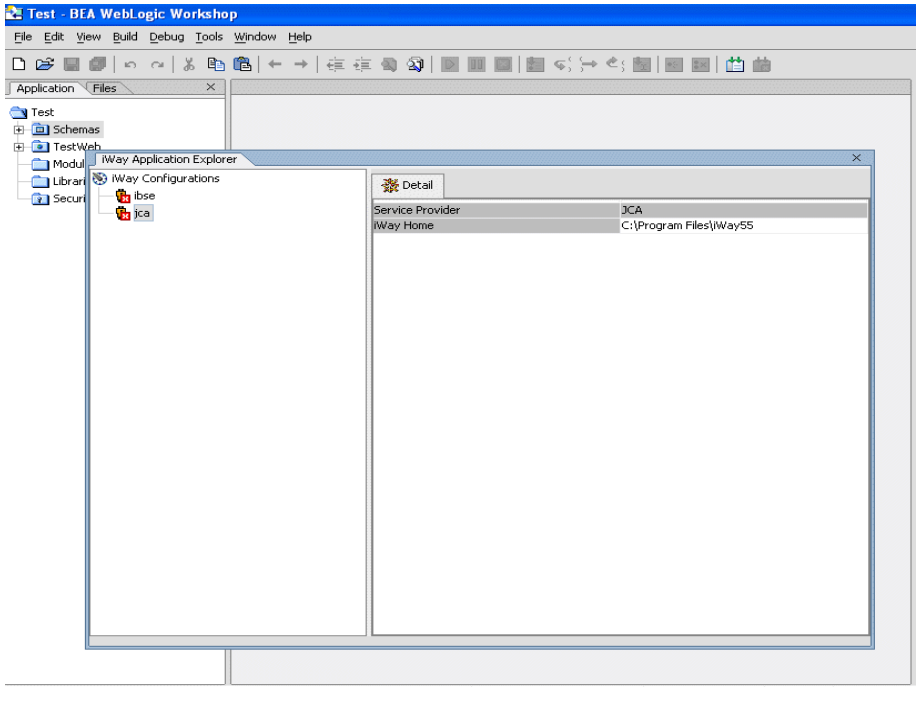
You can run Application Explorer in BEA WebLogic Workshop using an iWay Business Services Engine (iBSE) configuration. If you want to use Application Explorer with a JCA configuration instead of iBSE, you must use the servlet version of Application Explorer that runs outside of WebLogic Workshop. For more information about the servlet version, see Chapter 2, *Creating XML Schemas or Web Services for the iWay Adapter for HIPAA for BEA WebLogic*.

Procedure How to Start Application Explorer in BEA WebLogic Workshop

To start Application Explorer running in BEA WebLogic Workshop:

1. Before starting Application Explorer, ensure that BEA WebLogic Server is running.
2. Start BEA WebLogic Workshop.
3. From the BEA WebLogic Workshop View menu, select *Windows* and then, *iWay Application Explorer.*

   Application Explorer opens in BEA WebLogic Workshop.



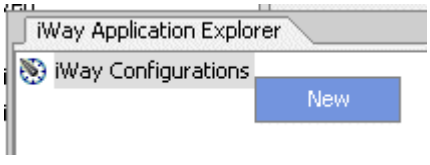
You can resize and drag-and-drop the Application Explorer window within BEA WebLogic Workshop. For example, you can drag it to the upper part of BEA WebLogic Workshop.

Creating a New Configuration

Before you can start using Application Explorer, you must define a new configuration for iBSE or JCA.

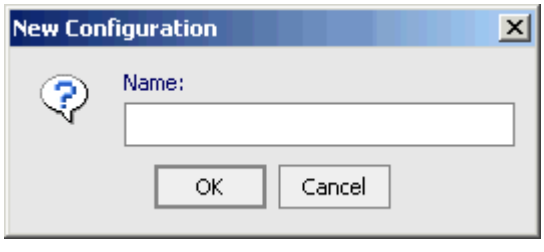
Procedure How to Create a New Configuration for iBSE or JCA

To create a new configuration:



1. Right-click *iWay Configurations* and select *New*.

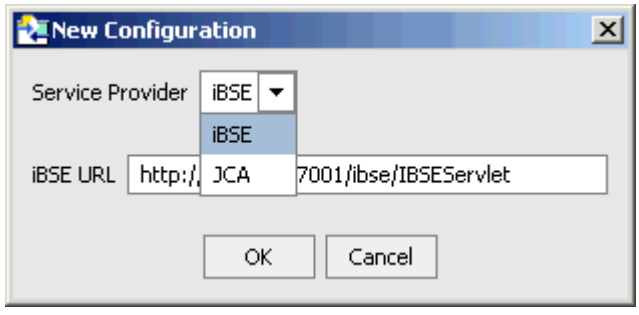
   The New Configuration dialog box opens.



2. Type the name of the new configuration and click *OK*.

   Note: If you are creating a new JCA configuration, type *base* in the name field. You must use this value if you are pointing to the default iWay configuration.

   The following dialog box opens.



3. From the Service Provider drop-down list, select *iBSE* or *JCA*.

- If you select iBSE, type the URL for iBSE, for example,

```
http://localhost:7001/ibse/IBSEServlet
```

where:

localhost

Is where your application server is running.

- If you select JCA, enter the full path to the directory where iWay 5.5 is installed, for example,

```
C:\Program Files\iWay55
```

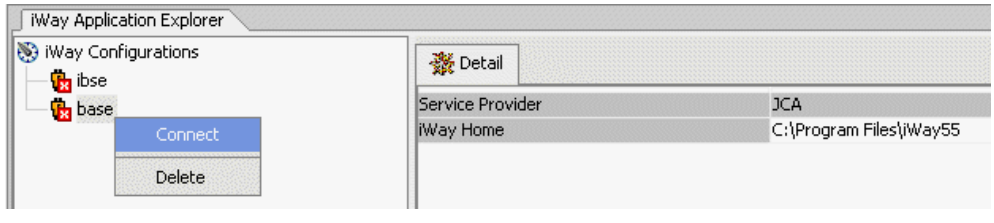
where:

iWay55

Is the full path to your iWay installation.

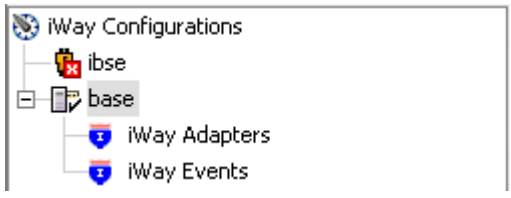
A node representing the new configuration appears under the iWay Configurations node. The right pane provides details of the configuration you created.

After you add your configuration, you must connect to it.

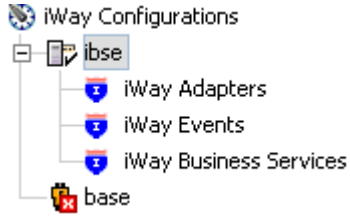


4. Right-click the configuration to which you want to connect, for example, base, and select *Connect*.

The iWay Adapters and iWay Events nodes appear.



When you connect to iBSE, the iWay Adapters, iWay Events, and iWay Business Services nodes appear.



5. To display the service and event adapters that are installed, expand each node.

The iWay Adapters list includes a HIPAA node that enables you to connect to HIPAA metadata and create XML request and response schemas to use to listen for events or create Web Services. For more information, see *Creating an iWay Business Service* on page A-15.

The iWay Events list includes a HIPAA node that enables you to create ports and channels for HIPAA event handling. For more information, see *Understanding iWay Event Functionality* on page A-19.

Connecting to HIPAA

To browse HIPAA, you must create a HIPAA target and connect to it. The target serves as your connection point. You must establish a connection to HIPAA every time you start iWay Application Explorer or after you disconnect from HIPAA.

The left pane displays the application systems supported by Application Explorer. These are based on the iWay adapters you installed and are licensed to use.

Creating and Connecting to a Target

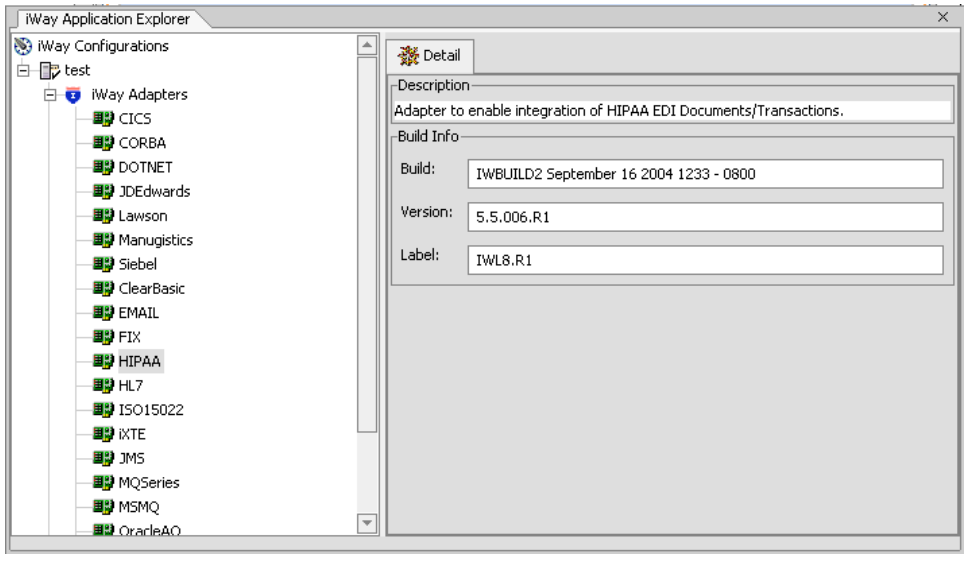
To connect to HIPAA for the first time, you must create a new target. The target is automatically saved after it is created.

Procedure How to Create a New Target

To create a target:

1. In the left pane, expand *iWay Adapters* and click the HIPAA node.

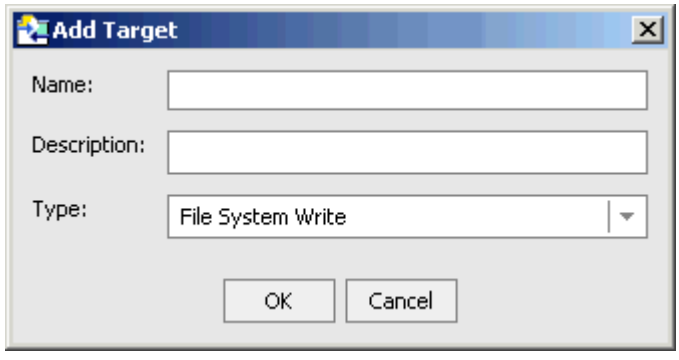
   Descriptive information (for example, title and product version) for the iWay Adapter for HIPAA appears in the right pane.



2. To view the options, right-click the *HIPAA* node.

3. Select *Add Target*.

The Add target dialog box opens.



a. In the Name field, type a descriptive name for the target, for example, HIPAATarget.

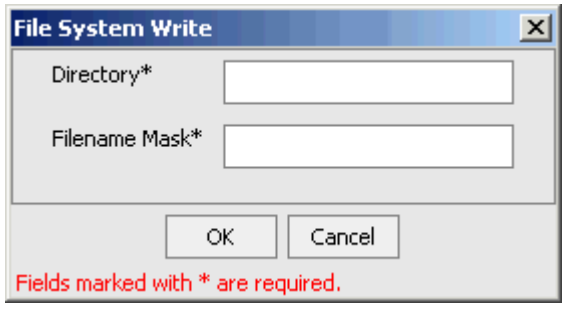
b. In the Description field, type a brief description of the target.

c. From the Target Type drop-down list, select one of the following transports from the drop-down list:

- File System Write. For more information on the properties required, see *File System Write Properties* on page A-8.
- File Transfer Protocol (FTP). For more information on the properties required, see *File Transfer Protocol Properties* on page A-9.
- HyperText Transfer Protocol (HTTP). For more information on the properties required, see *HyperText Transfer Protocol Properties* on page A-9.
- IBM MQSeries (MQ). For more information on the properties required, see *MQSeries Properties* on page A-10.
- TCP Session. For more information on the properties required, see *TCP Properties* on page A-10.

4. Click *OK*.

The File System Write dialog box opens.

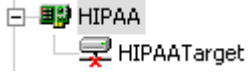


a. In the Directory field, type the location where the output of the service is placed.

b. In the Filename Mask field, type a file pattern, which can contain an asterisk which gets expanded to a fine timestamp.

5. Click *OK*.

In the left pane, the new target (HIPAATarget) appears below the HIPAA node.



You can now connect to the target you defined.

Reference File System Write Properties

The following table provides definitions for the properties required for the File System Write target type.

Property	Definition
Directory	The directory to which output messages are emitted.
Filename Mask	The output file name (can contain an asterisk), which gets expanded to a timestamp. A pound sign can be used as a mask for a sequence count. Each pound symbol represents a whole number integer value. For example, File## counts up to 99 before restarting at 0, File### counts up to 999 before restarting at 0, and so on.

Reference File Transfer Protocol Properties

The following table provides definitions for the properties required for the File Transfer Protocol target type.

Settings tab

Property	Definition
Host	FTP target system.
Port	FTP target system port.
User	User ID to use when connecting to the FTP host.
Password	Password associated with the user ID.
Directory	The directory to which output messages are emitted.
Filename Mask	The output file name (can contain an asterisk), which gets expanded to a timestamp. A pound sign can be used as a mask for a sequence count. Each pound symbol represents a whole number integer value. For example, File## counts up to 99 before restarting at 0, File### counts up to 999 before restarting at 0, and so on.

Advanced tab

Property	Definition
Retry Interval	The maximum wait interval between retries when a connection fails. Retry interval duration in *xx*H:*xx*M:*xx*S format. For example, 1H:2M:3S is 1 hour 2 minutes and 3 seconds.
Maxtries	Maximum number of retry attempts if a write failure occurs.

Reference HyperText Transfer Protocol Properties

The following table provides definitions for the properties required for the File Transfer Protocol target type.

Property	Definition
HTTP URL	The HTTP URL.

Property	Definition
Header	The HTTP header field.

Reference MQSeries Properties

The following table provides definitions for the properties required for the MQSeries target type.

Settings tab

Property	Definition
Queue Manager	Name of the MQSeries queue manager to be used.
Queue Name	Queue on which request documents are received.
Correlation ID	The correlation ID to set in the MQSeries message header.

MQ Client tab

Property	Definition
Host	Name of the MQSeries queue manager to be used.
Port	Queue on which request documents are received.
Channel	The correlation ID to set in the MQSeries message header.

Reference TCP Properties

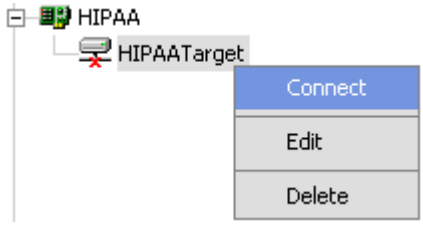
The following table provides definitions for the properties required for the TCP target type.

Property	Definition
Host	Host name or host address.
Port	TCP listening port.
Encoding	Document character set.

Procedure How to Connect to a Target

To connect to a HIPAA target:

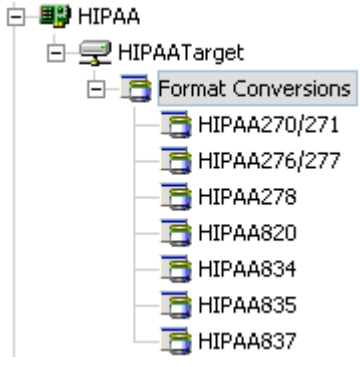
1. In the left pane, expand the *HIPAA* node and select the target to which you want to connect, for example, HIPAATarget.



2. In the left pane, right-click the target and select *Connect*.

   The HIPAATarget node in the left pane changes to reflect that a connection was made.

3. Expand the target node to reveal the list of HIPAA interfaces.



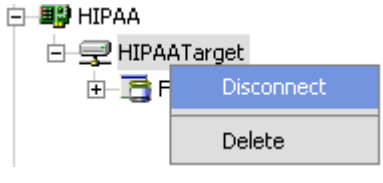
Managing a Target

Although you can maintain multiple open connections to different application systems, iWay Software recommends that you close connections when they are not in use. After you disconnect, you can modify an existing target.

You can modify the connection parameters when your system properties change. You also can delete a target. The following procedures describe how to disconnect from a target, edit a target, and delete a target.

Procedure How to Disconnect From a Target

To disconnect from a target:



1. Right-click the HIPAA target from which you want to disconnect.

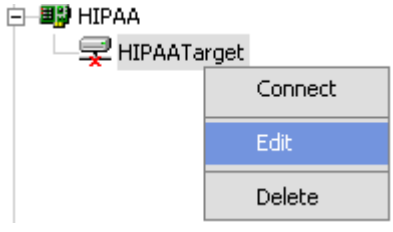
2. Select *Disconnect*.

   Disconnecting from the application system drops the connection, but the node remains. The HIPAATarget node in the left pane changes to reflect that you disconnected from the target.

Procedure How to Edit a Target

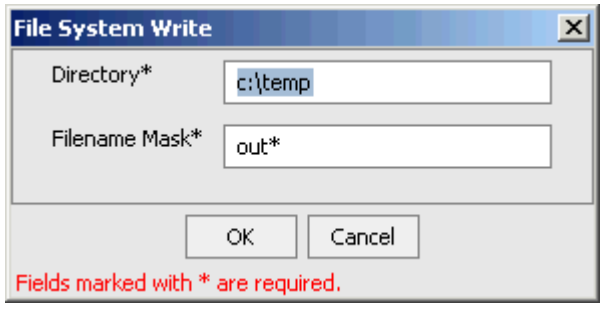
To edit a target:

1. Ensure that the target you want to edit is disconnected.



2. In the left pane, right-click the target and select *Edit*.

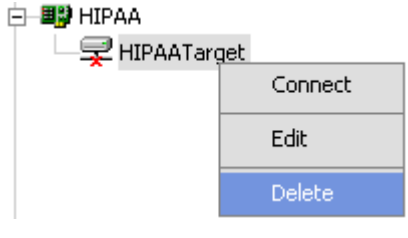
   The following dialog box opens.



3. Change the properties in the dialog box as required and click *OK*.

Procedure How to Delete a Target

To delete a target:



1. In the left pane, right-click the target.
2. Select *Delete*.

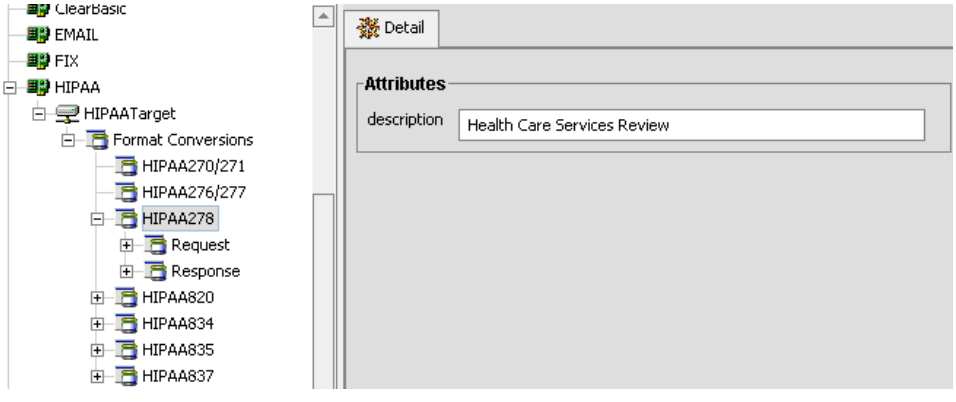
   The HIPAATarget node disappears from the left pane.

Creating an XML Schema

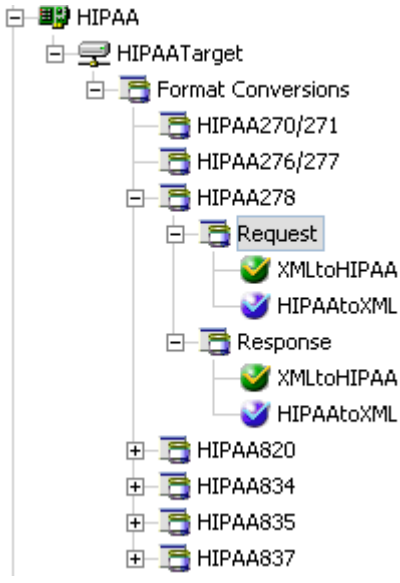
After you create a new configuration and connect to HIPAA, iWay Application Explorer enables you to create a request or response schema.

Procedure How to Create a Request and Response Schema

To create a request and response schema:



1. Expand the HIPAA node and select the node for which you want to create the schema.



The following XML schemas appear for the interface:

- Request
- Response

2. To view the appropriate schema in the right pane, click the *Request Schema* or the *Response Schema* tab.

Reference Schema Location

After you browse the Component Interfaces and make a selection, the request and response XML schemas are automatically created for that Component Interface and stored in the repository you created, for example:

```
drive:\Program Files\iWay55\bea\ibse\wsdl\schemas\service\HIPAA
\HIPAATarget\SA45280C
```

where:

HIPAATarget

Is the name of the HIPAA target.

SA45280C

Is a randomly generated folder name indicating where the schemas are stored.

Creating an iWay Business Service

You can create an iWay business service (also known as a Web service) for objects you want to use with your adapter. To generate a business service, you must deploy the iWay Adapter for HIPAA using the iWay Business Services Engine (iBSE). iBSE exposes functionality as Web services and serves as a gateway to heterogeneous back-end applications and databases.

A Web service is a self-contained, modularized function that can be published and accessed across a network using open standards. It is the implementation of an interface by a component and is an executable entity. For the caller or sender, a Web service can be considered as a "black box" that may require input and delivers a result. Web services integrate within an enterprise as well as across enterprises on any communication technology stack, whether asynchronous or synchronous, in any format.

You can make a Web service available to other services within a host server by generating WSDL (Web Services Description Language) from the Web service.

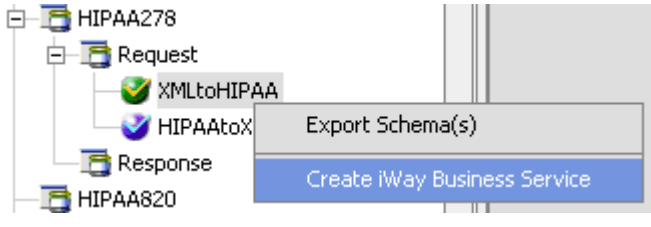
Because Application Explorer runs within BEA WebLogic Workshop, you can easily incorporate iWay Web services into BEA WebLogic Workflows. To enable BEA WebLogic Workshop to use iWay Web services, you export the WSDL to a directory accessible to BEA WebLogic Workshop.

Note: In a J2EE Connector Architecture (JCA) implementation of iWay adapters, Web services are not available. When the adapters are deployed to use the iWay Connector for JCA, the Common Client Interface provides integration services using the iWay adapters. For more information, see the *iWay Installation and Configuration for BEA WebLogic* manual and the i*Way Connector for JCA for BEA WebLogic Server User's Guide*.

Procedure How to Create an iWay Business Service

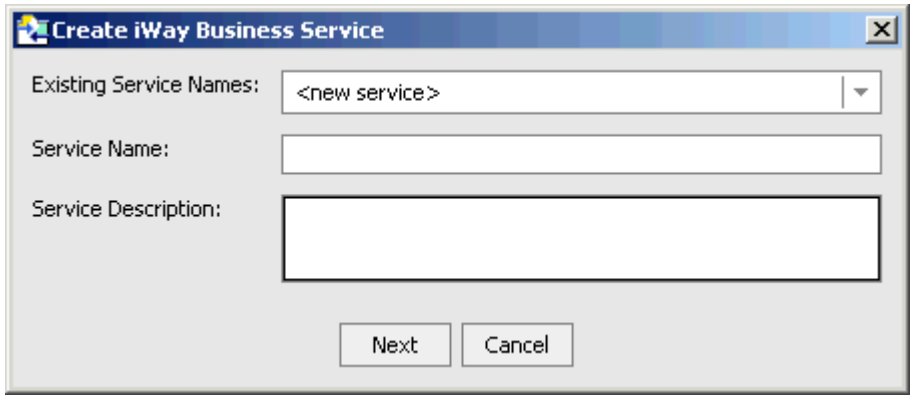
To create an iWay Business service:

1. Expand the HIPAA node and select the interface for which you want to create a business service.



2. Right-click and select *Create iWay Business Service*.

The Create iWay Business Service dialog box opens.



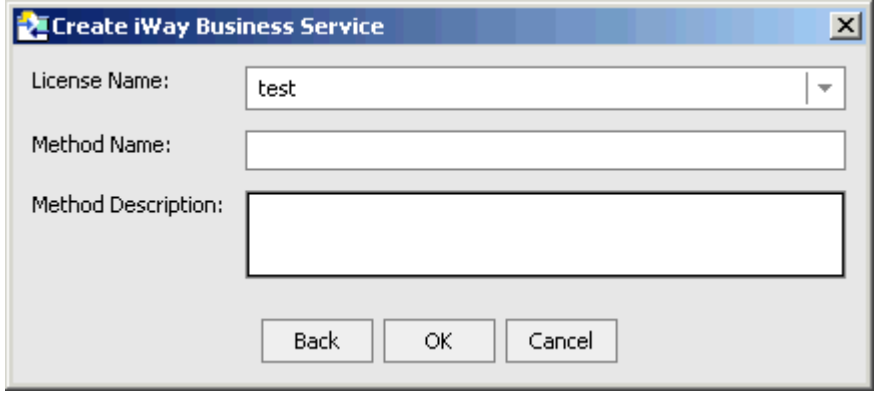
a. From the Existing Service Names drop-down list, select whether you want to create a new service name or use an existing service name.

b. In the Service Name field, type a name for the business service, for example, 278request.

c. In the Service Description field, type a brief description of the business service.

3. Click *Next*.

The Create iWay Business Service dialog box displays additional fields.



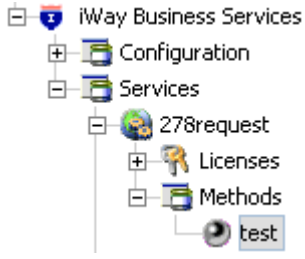
a. From the License Name drop-down list, select a license.

b. In the Method Name field, type a name for the method.

c. In the Method Description field, type a brief description for the method.

4. Click *OK*.

The business service and method appear below the iWay Business Services node.



In the left pane, all the available business services that were created appear.

5. Click the node for which you created the business service in the right pane.

The test pane opens in a new browser window.

6. To invoke the service, enter a sample XML document in the input xml field.

7. Click *Invoke*.

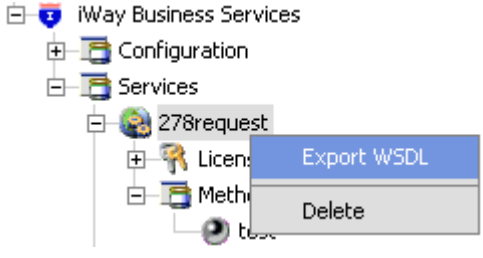
   The result appears in the right pane.

Exporting iWay WSDL for Use in BEA WebLogic Workshop Workflows

Because iWay Application Explorer runs within BEA WebLogic Workshop, you can easily incorporate iWay Web services into BEA WebLogic Workflows. To enable BEA WebLogic Workshop to use iWay Web services, you simply export the WSDL to a directory accessible to BEA WebLogic Workshop.

Procedure How to Export iWay WSDL for Use in BEA WebLogic Workshop Workflows

To export WSDL to a directory accessible to BEA WebLogic Workshop:

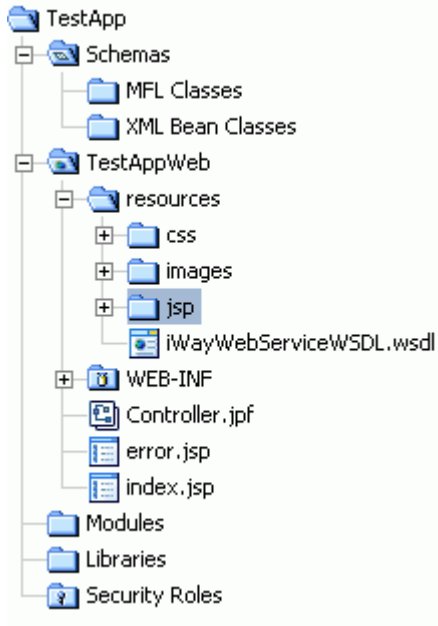


1. After you create a Web service, right-click the Web service name and select *Export WSDL*.

   The Save dialog box appears.

2. Save the WSDL to a directory accessible to BEA WebLogic Workshop, for example, the \resources directory in your BEA WebLogic Workshop Web application directory structure.

The WSDL file appears under the resources folder of your Web application:



Understanding iWay Event Functionality

Events are generated as a result of activity in an application system. You can use events to trigger an action in your application. For example, HIPAA may generate an event when customer information is updated. If your application must perform in response to activity, your application is a consumer of this event.

After you create a connection to your application system, you can add events using Application Explorer. To define an iWay event, you must create a port and a channel.

- Port

  A port associates a particular business object exposed by the adapter with a particular disposition. A disposition defines the protocol and location of the event data. The port defines the end point of the event consumption. For more information, see *Creating an Event Port*.

- Channel

  A channel represents configured connections to particular instances of back-end systems. A channel binds one or more event ports to a particular listener managed by the adapter. For more information, see *Creating a Channel* on page A-35.

Creating an Event Port

The following procedures describe how to create an event port using iWay Application Explorer. The following port dispositions are available when using iBSE:

- File
- iBSE
- MSMQ
- JMSQ
- SOAP
- HTTP
- MQ Series
- Mail

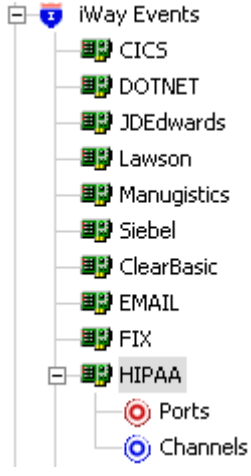
Note: The MAIL disposition option will be supported in a future release.

With a JCA implementation, the following port dispositions are available:

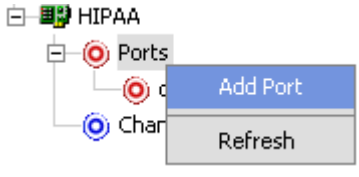
- File
- JMSQ
- MQ Series
- HTTP

Procedure How to Create an Event Port for File

To create an event port for File:

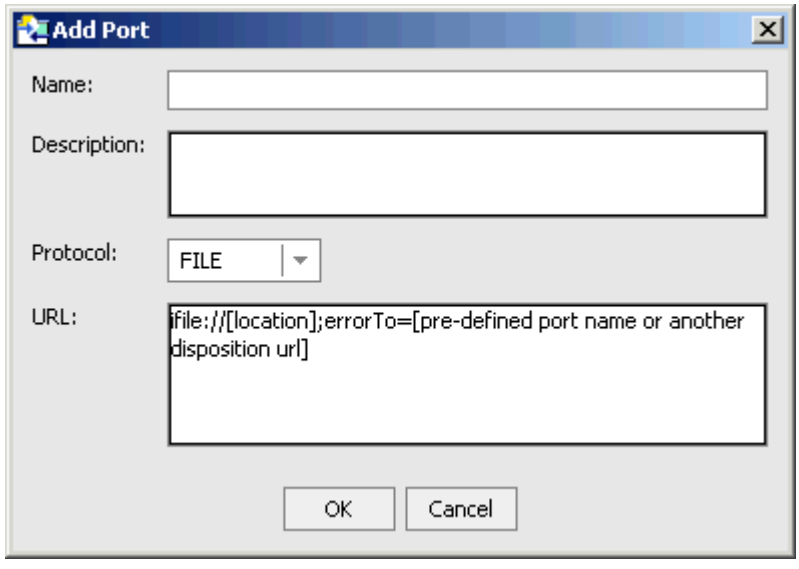


1. In the left pane of Application Explorer, expand the HIPAA node under iWay Events, and then select *Ports*.



2. Right-click and select *Add Port*.

The Add Port dialog box opens.



a. In the Name field, type a name for the event port, for example, HIPAAFile.

b. In the Description field, type a brief description.

c. From the Protocol drop-down list, select *FILE*.

d. In the URL field, type a destination file to which the event data is written, using the following format:

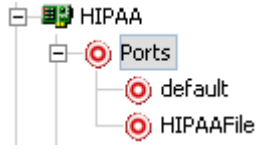
```
file://location[;errorTo=errorDest]
```

The following table describes the URL parameters.

Parameter	Description
location	The full directory path and file name to which the data is written.
errorTo	Location where error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

3. Click *OK*.

In the left pane, the event port appears below the Ports node.



4. To review the port settings, select the port name.

   In the right pane, a table appears that summarizes the information associated with the event port you created.

Detail

Name	Value
Name	HIPAAFile
Description	
Disposition	ifile://c:\temp\x.txt;errorTo=c:\error
Content	all messages accepted

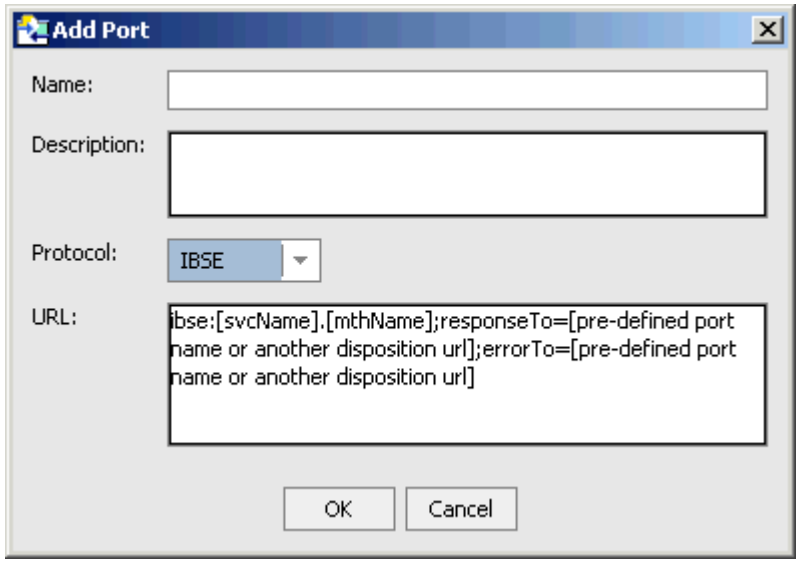
You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

Procedure How to Create an Event Port for iBSE

To create an event port for iBSE:

1. In the left pane of Application Explorer, expand the HIPAA node under iWay Events, and then select *Ports*.
2. Right-click and select *Add Port*.

The Add Port dialog box opens.



a. In the Name field, type a name for the event port, for example, HIPAAiBSE.

b. In the Description field, type a brief description.

c. From the Protocol drop-down list, select *IBSE*.

d. In the URL field, enter an iBSE destination using the following format:

```
ibse:/svcName.methName[;responseTo=respDest][;errorTo=errorDest]
```

The following table describes the disposition parameters.

Parameter	Description
svcName	Name of the service created with iBSE.
methName	Name of the method created for the Web service.
respDest	Location where responses to the Web service are posted. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.
errorDest	Location where error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

3. Click *OK*.

In the left pane, the event port appears below the Ports node.

4. To review the port settings, select the port name.

   In the right pane, a table appears that summarizes the information associated with the event port you created.

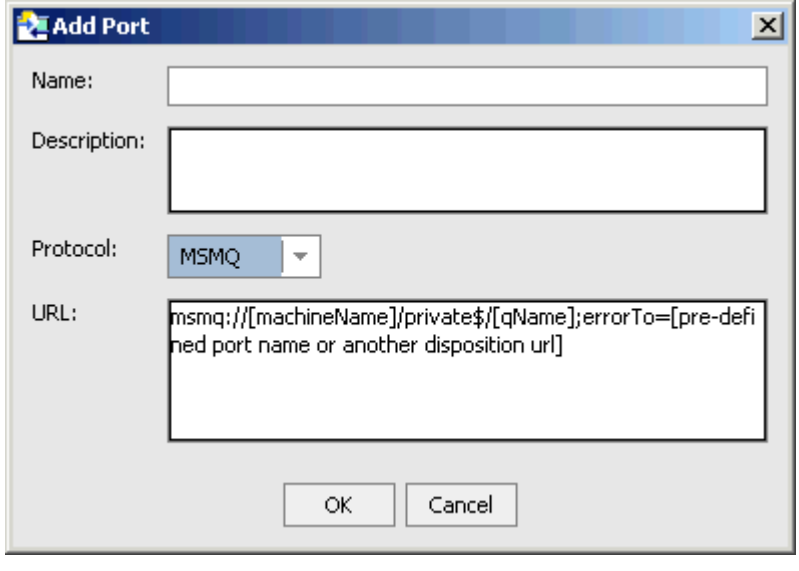
   You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

Procedure How to Create an Event Port for MSMQ

To create an event port for a Microsoft Message Queuing (MSMQ) queue:

1. In the left pane of Application Explorer, expand the HIPAA node under iWay Events, and then select *Ports*.
2. Right-click and select *Add Port*.

   The Add Port dialog box opens.



   a. In the Name field, type a name for the connection, for example, HIPAAMSMQ.
   b. In the Description field, type a description for the target name you just created.
   c. From the Protocol drop-down list, select *MSMQ*.
   d. In the URL field, enter an MSMQ destination in the following format:

      `msmq:/host/queueType/queueName[;errorTo=errorDest]`

The following table defines the disposition parameters.

Parameter	Description
host	Name of the host on which the Microsoft Queuing system runs.
queueType	The type of queue. For private queues, enter *Private$*. Private queues are queues that are not published in Active Directory. They appear only on the local computer that contains them. Private queues are accessible only by Message Queuing applications that recognize the full path name or format name of the queue.
queueName	Name of the queue where messages are placed.
errorDest	Location where error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

3. Click *OK*.

   In the left pane, the event port appears below the Ports node.

4. To review the port settings, select the port name.

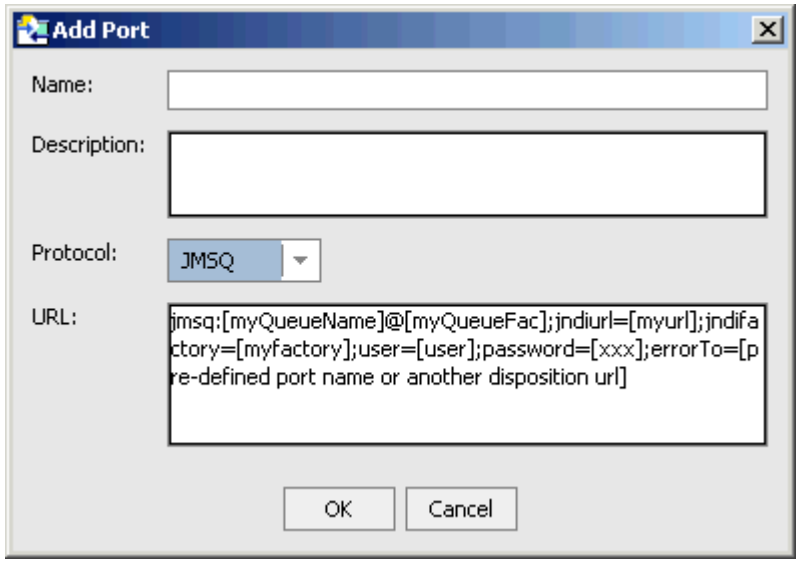
   In the right pane, a table appears that summarizes the information associated with the port you created. You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

Procedure How to Create a Port for JMS

To create a port for a JMS queue:

1. In the left pane of Application Explorer, expand the HIPAA node under iWay Events, and then select *Ports*.
2. Right-click and select *Add Port*.

The Add Port dialog box opens.



a. In the Name field, type a name for the event port, for example, HIPAAJMSQ.

b. In the Description field, type a brief description.

c. From the Protocol drop-down list, select *JMSQ*.

d. In the URL field, enter a JMSQ destination using the following format:

```
jmsq:queue@conn_factory;jndiurl=jndi_url;jndifactory=jndi_factory;
user=userID;password=pass[;errorTo=errorDest]
```

The following table describes the URL parameters.

Parameter	Description
queue	Name of a queue to which events are emitted.
conn_factory	The connection factory, a resource that contains information about the JMS Server. The WebLogic connection factory is: `javax.jms.QueueConnectionFactory`

Parameter	Description
jndi_url	The URL of the application server. For BEA WebLogic Server, the URL is `t3://host:port` where: *host* Is the machine name where BEA WebLogic Server resides. *port* Is the port on which BEA WebLogic Server is listening. The default port if not changed at installation, is 7001.
jndi_factory	Is JNDI context.INITIAL_CONTEXT_FACTORY and is provided by the JNDI service provider. For BEA WebLogic Server, the WebLogic factory is weblogic.jndi.WLInitialContextFactory.
userID	User ID associated with this queue.
pass	Password associated with this user ID.
errorDest	Location where error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

3. Click *OK*.

   The event port appears below the Ports node in the left pane.

4. To review the port settings, select the port name.

   In the right pane, a table appears that summarizes the information associated with the event port you created.

   You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

Procedure How to Create a Port for the SOAP Disposition

This topic describes how to configure the SOAP disposition for synchronous event processing.

The SOAP disposition allows an event response to launch a Web service specified by a WSDL file. A soapaction is optional, the default is "".

To create a port for a SOAP disposition using Application Explorer:

1. Click the *iWay Events* tab.

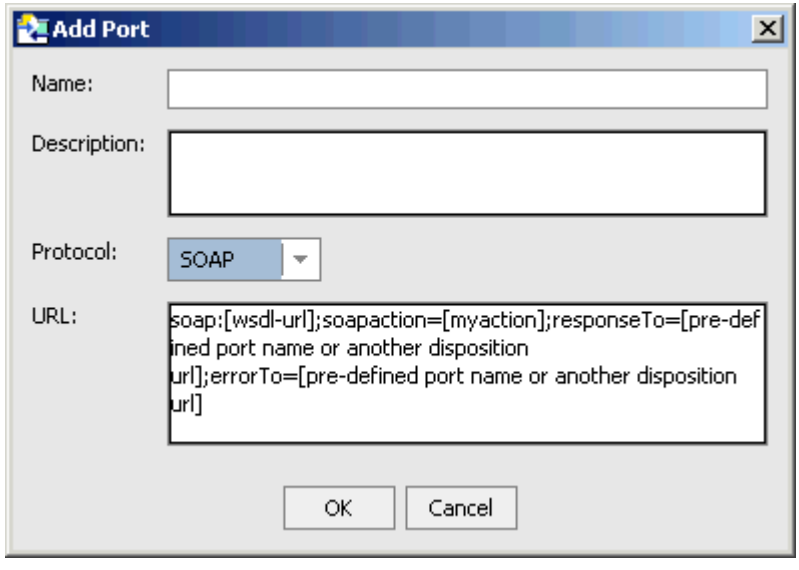
   The iWay Event Adapters window opens.

2. In the left pane, expand the HIPAA adapter node.

3. Select the *ports* node.

4. Move the pointer over *Operations* and select *Add a new port*.

   The Add Port dialog box opens.



   a. Type a name for the event port and provide a brief description.

   b. From the Disposition Protocol drop-down list, select *SOAP*.

   c. In the Disposition field, enter a SOAP destination using the following format:

```
soap:wsdl-url;soapaction=action[;responseTo=respDest]
   [;errorTo=errorDest]
```

The following table lists and describes the disposition parameters for SOAP.

Parameter	Description
wsdl-url	The URL to the WSDL file that is required to create the SOAP message. For example: `http://localhost:7001/ibse/IBSEServlet/test/sw2xml2003MQ.ibs?wsdl` This value can be found by navigating to the iWay Business Services tab and opening the *Service Description* link in a new window. The WSDL URL appears in the Address field. You can also open the WSDL file in a third party XML editor (for example, XMLSPY) and view the SOAP request settings to find this value.

action	The method that will be called by the disposition. For example:
	`HIPAAMT.mt200Request@test@@`
	where
	`HIPAA`
	Is the name of the Web service you created using Application Explorer.
	`mt200`
	Is the method being used.
	`test`
	Is the license that is being used by the Web service.
	This value can be found by navigating to the iWay Business Services tab and opening the *Service Description* link in a new window. Perform a search for *soapAction*.
	You can also open the WSDL file in a third party XML editor (for example, XMLSPY) and view the SOAP request settings to find this value.

respDest	The location to which responses are posted. A predefined port name or another full URL. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

Parameter	Description
errorDest	The location to which error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

5. Click *OK*.

The port appears under the ports node in the left pane. In the right pane, a table appears that summarizes the information associated with the port you created.

You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

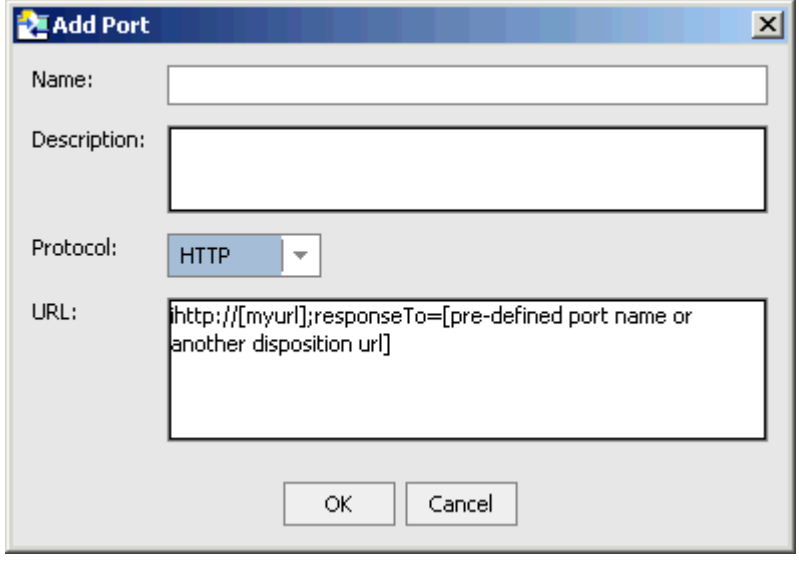
Procedure How to Create an Event Port for HTTP

The HTTP disposition uses an HTTP URL to specify an HTTP end point to which the event document is posted.

To create an event port for HTTP disposition:

1. In the left pane of Application Explorer, expand the HIPAA node under iWay Events, and then select *Ports*.
2. Right-click and select *Add Port*.

   The Add Port dialog box opens.



a. In the Name field, type a name for the event port, for example, HIPAAHTTP.

b. In the Description field, type a brief description.

c. From the Protocol drop-down list, select *HTTP*.

d. In the URL field, enter an HTTP destination using the following format:

```
ihttp://url;responseTo=respDest
```

The following table describes the URL parameters.

Parameter	Description
url	The URL target for the post operation.
respDest	Location where responses are posted. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.
host	Name of the host on which the Web server resides.
port	Port number on which the Web server is listening.

3. Click *OK*.

The event port appears below the Ports node in the left pane.

4. To review the port settings, select the port name.

In the right pane, a table appears that summarizes the information associated with the event port you created.

You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

Procedure How to Create an Event Port for MQ Series

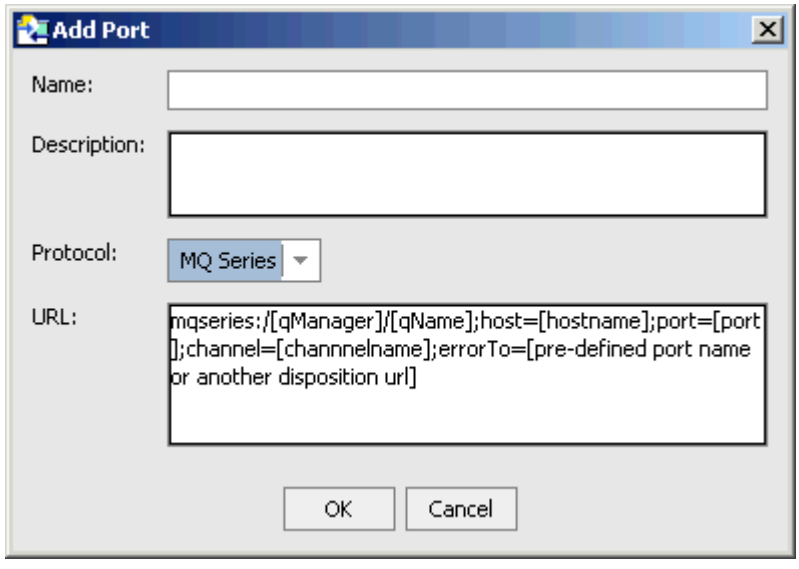
The MQ Series disposition allows an event to be enqueued to an MQ Series queue. Both queue manager and queue name may be specified.

To create a port for an MQ Series queue:

1. In the left pane of Application Explorer, expand the HIPAA node under iWay Events, and then select *Ports*.

2. Right-click and select *Add Port*.

The Add Port dialog box opens.



a. In the Name field, type a name for the event port, for example, HIPAAMQSeries.

b. In the Description field, type a brief description.

c. From the Protocol drop-down list, select *MQ Series*.

d. In the URL field, enter an MQ Series destination using the following format:

```
mqseries:/qManager/qName;host=hostName;port=portNum;
channel=chanName[;errorTo=errorDest]
```

The following table describes the URL parameters.

Parameter	Description
qManager	Name of queue manager to which the server must connect.
qName	Name of the queue where messages are placed.
hostName	Name of the host on which MQ Series resides (MQ client only).
portNum	Port number for connecting to an MQ Server queue manager (MQ client only).
chanName	Case-sensitive name of the channel that connects with the remote MQ Server queue manager (MQ client only). The default MQ Series channel name is SYSTEM.DEF.SVRCONN.

Parameter	Description
errorDest	Location where error logs are sent. Optional. A predefined port name or another disposition URL. The URL must be complete, including the protocol.

3. Click *OK*.

   The event port appears below the Ports node in the left pane.

4. To review the port settings, select the port name.

   In the right pane, a table appears that summarizes the information associated with the event port you created.

   You are ready to associate the event port with a channel. For more information, see *Creating a Channel* on page A-35.

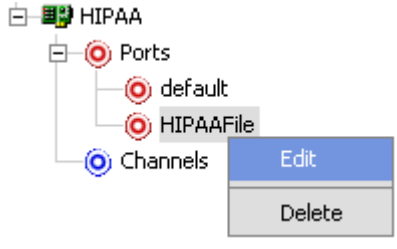
Modifying an Event Port

The following procedures describe how to edit and delete an event port using iWay Application Explorer. To review the port settings, select the port name. In the right pane, a table appears that summarizes the information associated with the event port you created.

Procedure How to Edit an Event Port

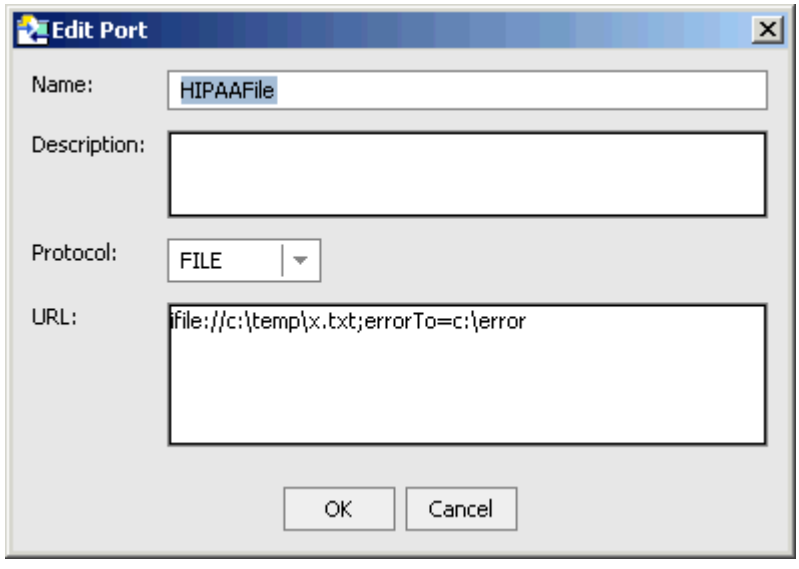
To edit an event port:

1. To view the available ports, click the *Ports* node in the left pane.



2. Right-click the port you want to edit, and select *Edit*.

The Edit Port dialog box opens.

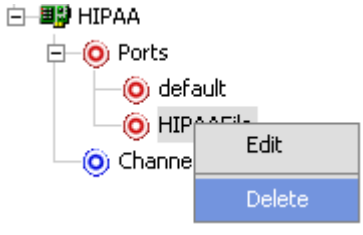


3. Make the required changes and click *OK*.

Procedure How to Delete an Event Port

To delete an existing event port:

1. To view the available ports, click the *Ports* node in the left pane.



2. Right-click the port you want to remove, and select *Delete*.

   The event port node disappears from the ports list in the left pane.

Creating a Channel

The following procedure describes how to create a channel for a HIPAA event. All defined event ports must be associated with a channel.

You can create the following types of channels using Application Explorer:

- File System Listener (File)
- Hypertext Transfer Protocol (HTTP)
- TCP Listener (TCP)
- IBM MQSeries (MQ)
- File Transfer Protocol (FTP)

Procedure How to Create a Channel for a File System Listener

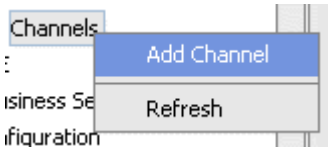
To create a channel for a File System Listener (FILE):

1. In the left pane, below the configuration you created, expand the *iWay Events* node.

   The list of adapters appears.

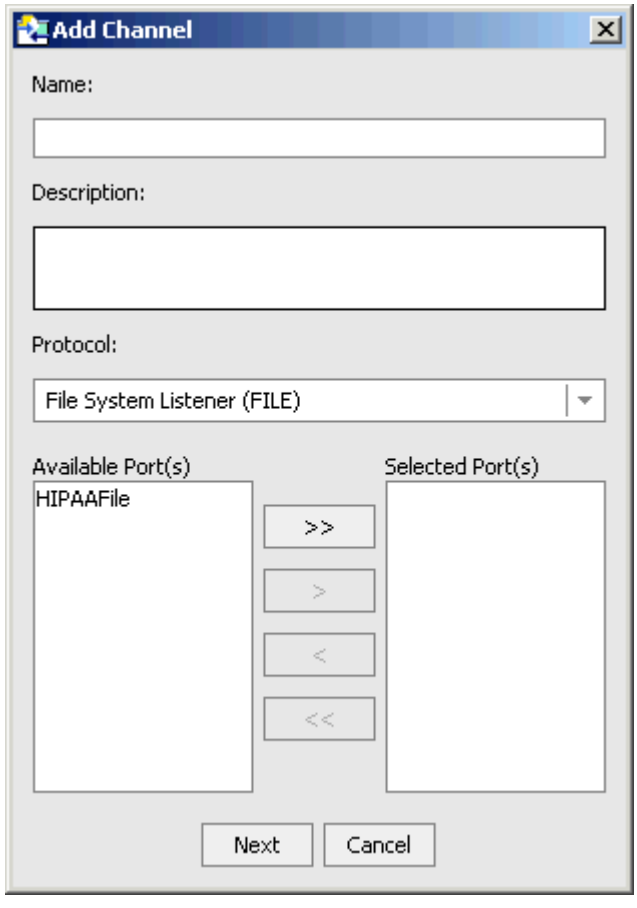
2. Click the adapter node, for example, HIPAA.

   The node expands and displays the Ports and Channels nodes.



3. Right-click the *Channels* node and select *Add Channel*.

The Add Channel dialog box opens.



a. In the Name field, type a name for the channel, for example, HIPAAChannel.

b. In the Description field, type a brief description.

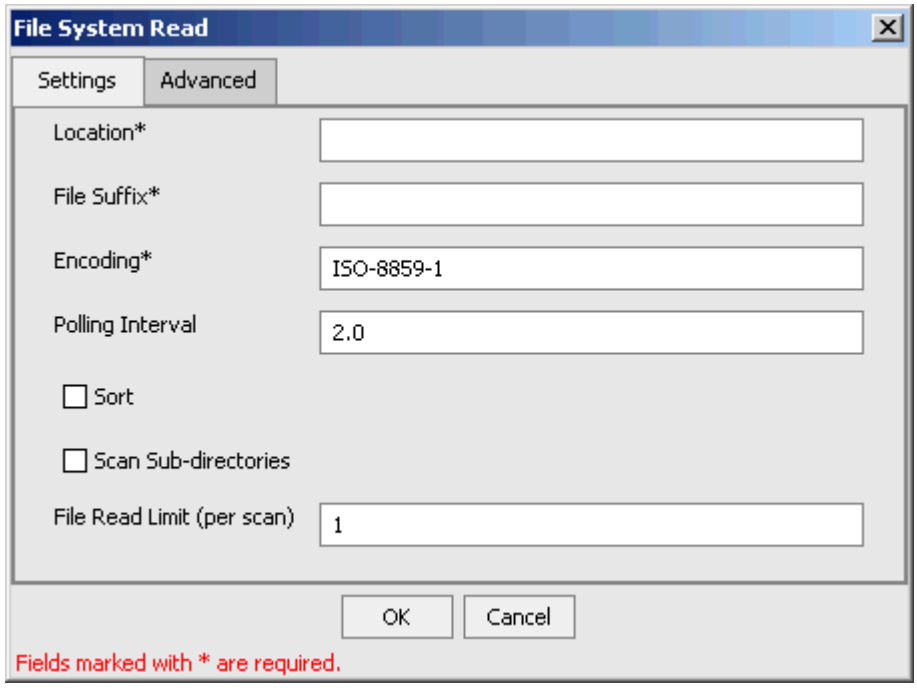
c. From the Protocol drop-down list, select a type of listener:

- File System Listener (FILE)
- HyperText Transfer Protocol
- TCP Listener (TCP)
- IBM MQ Series (MQ)

d. To associate one or more available ports with this channel, select the port in the Available box and click the double right arrow (>>) button to move it to the Selected box.

4. Click *Next*.

   A dialog box opens that is specific to the protocol you selected.



5. Enter values for the parameters that are listed.

   For information on the parameters for a File System Listener (FILE) listener, see *File System Listener (FILE) listener Configuration Parameters* on page A-40.

   For information on the parameters for a HyperText Transfer Protocol listener, see *HyperText Transfer Protocol Listener Configuration Parameters* on page A-41.

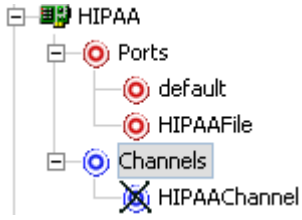
   For information on the parameters for a TCP Listener, see *TCP Listener Configuration Parameters* on page A-42.

   For information on the parameters for an IBM MQ Series (MQ) listener, see *IBM MQ Series (MQ) Listener Configuration Parameters* on page A-42.

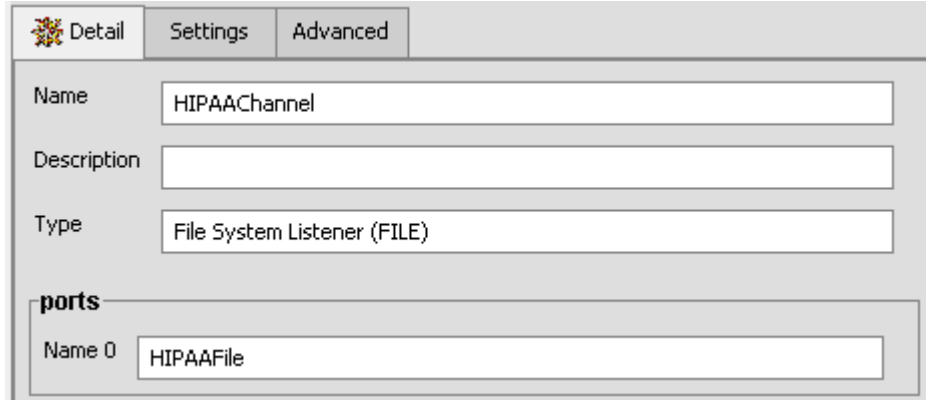
   For information on the parameters for a File Transfer Protocol (FTP) listener, see *File Transfer Protocol (FTP) Listener Configuration Parameters* on page A-43.

6. Click *OK*.

   The channel appears below the Channels node in the left pane.

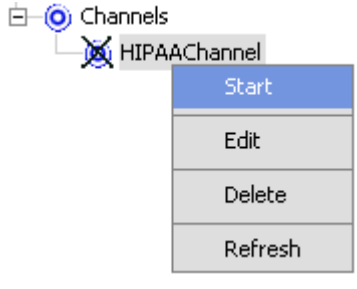


When you select the event port, the channel information appears in the right pane.



A Ports area appears on the Details tab that displays the name of the event port you assigned to this channel.

You are ready to start your channel to listen for events.



7. To activate your event configuration, right-click the channel node, for example, HIPAAChannel.

a. Select *Start*.

b. To stop the channel at any time, right-click the channel and select *Stop*.

Reference File System Listener (FILE) listener Configuration Parameters

On the Settings tab:

Parameter	Description
Location	The directory where messages are received. DOS-style file patterns are valid for this parameter. You can specify a file pattern as well as a directory. For example, c:\xyz\ab*cd (without a file suffix) takes the file suffix from that parameter. If you use a pattern, files are selected based on the suffix and then the pattern. AB?CD selects ABxCD. AB*CD selects ABxxxCD.
File Suffix	File extension for the file event. This limits input files to those with the specified extensions. The "." is not required. The minus sign ("-") indicated that there is no extension. If the file extension is zip, the unzipped files must conform to the event schema, or they will fail. This function also works with transform configured.
Encoding	The host on which the MQ Server is located (for the MQ Client only).
Polling Interval	This is a time, expressed as xxH:xxM:xxS For example 1 hour, 2 minutes, and 3 seconds is: 1H:2M:3S The maximum interval between checks for new documents. The higher this value, the longer the interval, and the fewer system resources that are used. The side-effect of a high value is that a worker thread cannot respond to a stop command. If this value is set to 0, the listener runs once and terminates. The default value is 2 seconds.
Sort	The case-sensitive name of the channel that connects with the remote MQ Server queue manager (for the MQ client only). The default channel name for MQSeries is SYSTEM.DEF.SVRCONN.
Scan Sub-directories	Location where error documents are sent. This can be a predefined port name or another full URL. Optional.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference **HyperText Transfer Protocol Listener Configuration Parameters**

On the Settings tab:

Parameter	Description
Port	The port where the adapter listens for the HTTP transfer.
Encoding	The character set encoding for inbound documents. For example, UTF-8. The default is ISO-8859-1 US and Western Europe.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference TCP Listener Configuration Parameters

On the Settings tab:

Parameter	Description
Port	The port where the adapter listens for the TCP transfer.
Encoding	The character set encoding for inbound documents. For example, UTF-8. The default is ISO-8859-1 US and Western Europe.
Allowable Client Host	The name or address of the client restricted to accessing this adapter.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference IBM MQ Series (MQ) Listener Configuration Parameters

On the Settings tab:

Parameter	Description
Queue Manager	The name of the MQ queue manager to be used.
Queue Name	The name of the MQ Series or WebSphere MQ queue that the HIPAA system polls.

Parameter	Description
Polling Interval	The maximum wait interval (in the format *nn*H:*nn*M:*nn*S) between checks for new documents. The higher this value, the longer the interval, and the fewer system resources that are used. However, with a high value, the worker thread cannot respond to a stop command. If timeout is set to 0, the listener runs once and terminates. The default is 2 seconds.

On the MQ Client tab:

Parameter	Description
Host	The host where the MQ Server is located.
Port	The port number used to connect to an MQ Server.
Channel	The channel between an MQ Client and an MQ Server.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

Reference **File Transfer Protocol (FTP) Listener Configuration Parameters**

On the Settings tab:

Parameter	Description
Host	The name of the FTP host.
Port	The port where the adapter listens on the FTP transfer.

Parameter	Description
User	The user name to log onto the FTP Server.
Password	The password for the FTP user.
Location	The directory where messages are received. DOS-style file patterns are available for this parameter. You can specify a file pattern as well as a directory. For example, c:\xyz\ab*cd (without a file suffix) takes the file suffix from that parameter. If you use a pattern, files are selected based on the suffix and then the pattern. AB?CD selects ABxCD. AB*CD selects ABxxxCD.
Encoding	The character set encoding for inbound documents. For example, UTF-8. The default is ISO-8859-1 US and Western Europe.
Polling Interval	The maximum wait interval (in the format *nn*H:*nn*M:*nn*S) between checks for new documents. The higher this value, the longer the interval, and the fewer system resources that are used. However, with a high value, the worker thread cannot respond to a stop command. If timeout is set to 0, the listener runs once and terminates. The default is 2 seconds.

On the Advanced tab:

Parameter	Description
Transform Type	Select the pre-built transform template from the drop-down list. To enable batch processing, select *BatchSplitter* from the drop-down list. The batch splitter preparses an entire EDI document and splits the document into individual transactions. Each transaction retains its Interchange Header/Trailer information. Once the batch splitter is finished splitting the EDI document, the transactions are ready to be transformed into XML.
Location for ack copies	The directory in which the acknowledgement document is placed.

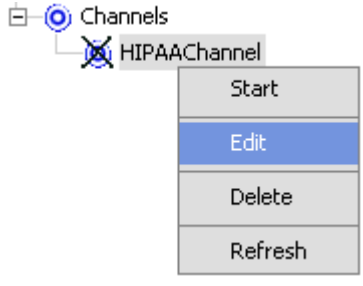
Modifying a Channel

The following procedures describe how to edit and delete a channel using Application Explorer. To review the channel settings, you select the channel name. In the right pane, a table appears that summarizes the information associated with the channel you created.

Procedure How to Edit a Channel

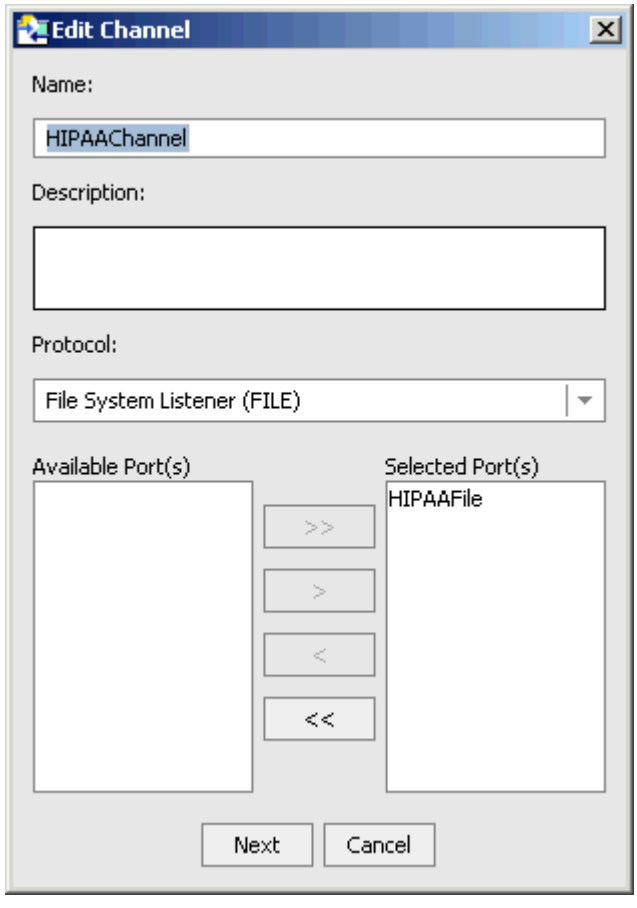
To edit a channel:

1. To view the available channels, click the *Channels* node in the left pane.



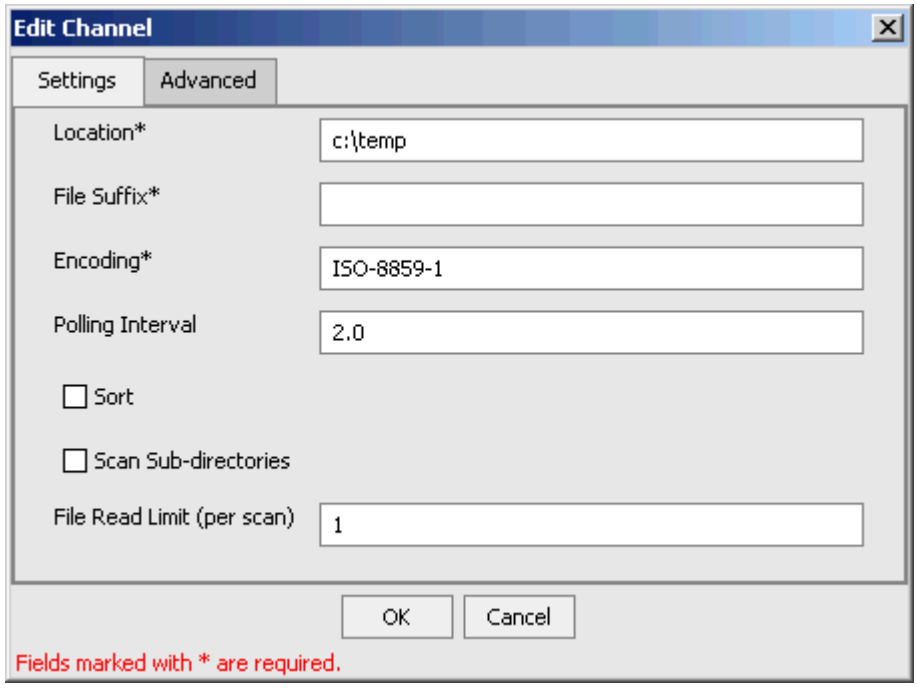
2. Right-click the channel you want to edit, for example, HIPAAChannel, and select *Edit*.

The Edit Channel dialog box opens.



3. Make the required changes to the channel configuration.
4. Click *Next*.

The following dialog box opens.

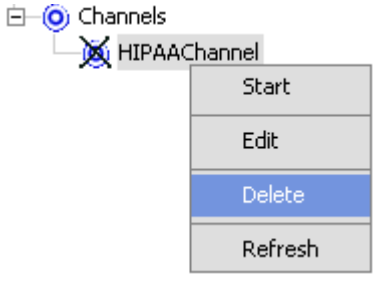


5. Make the required changes and click *OK*.

Procedure How to Delete a Channel

To delete an existing channel:

1. In the left pane, right-click the channel, for example, HIPAAChannel.



2. Select *Delete*.

   The channel disappears from the Channels list.

Deploying iWay Components in a Clustered BEA WebLogic Environment

iWay events can be configured in a clustered BEA WebLogic environment.

A cluster consists of multiple server instances running simultaneously, yet appears to clients to be a single server instance. The server instances that contain a cluster can be run on one machine, but are usually run on multiple machines.

Clustering provides the following benefits:

- Load balancing
- High availability

Service requests are processed through the HTTP router and routed to an available managed server.

Events are server-specific and are not processed through the HTTP router. You must configure each server separately.

Procedure How to Deploy iWay Components in a Clustered Environment

To deploy iWay components in a clustered environment:

1. Using the BEA Configuration Wizard:
   a. Configure an administrative server to manage the managed servers.
   b. Add and configure as many managed servers as required.
   c. Add and configure an HTTP router. This does not have to be a part of WebLogic and can be an outside component.
   d. If you configure the HTTP router within WebLogic, start it by entering the following command:

   ```
   StartManagedWebLogic HTTPROUTER http://localhost:7001
   ```

   where:

   HTTPROUTER
   Is the name of the server on which the HTTP router is running.

   http://localhost:7001
   Is the location of the admin console.

   e. Add the managed servers to your cluster/clusters.

For more information on configuring WebLogic Integration for deployment in a clustered environment, see *Deploying WebLogic Integration Solutions*.

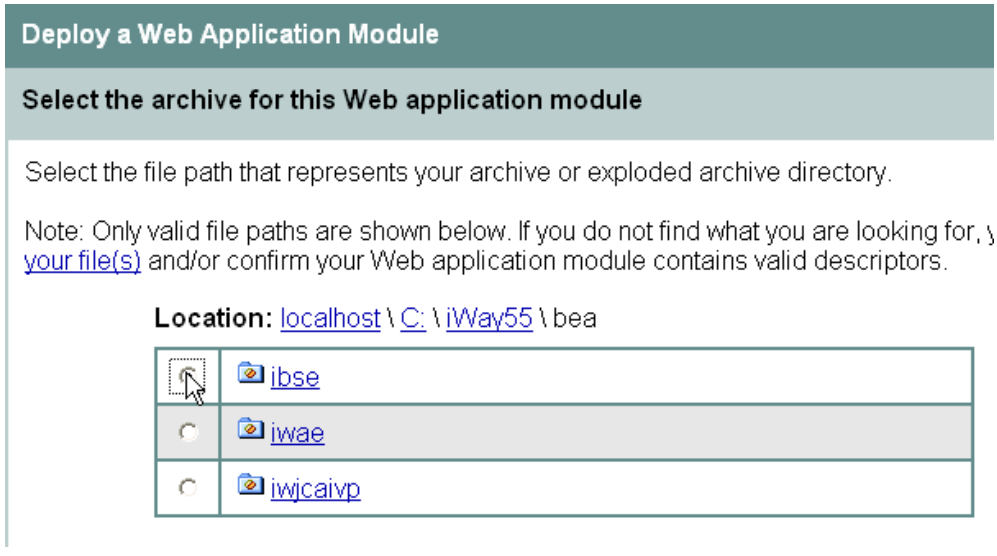
2. Start the WebLogic Server and open WebLogic Server Console.

3. Deploy iBSE to the cluster by selecting *Web Application Modules* from the Domain Configurations section, and clicking *Deploy a new Web Application Module*.

   A page appears for you to specify where the Web application is located.

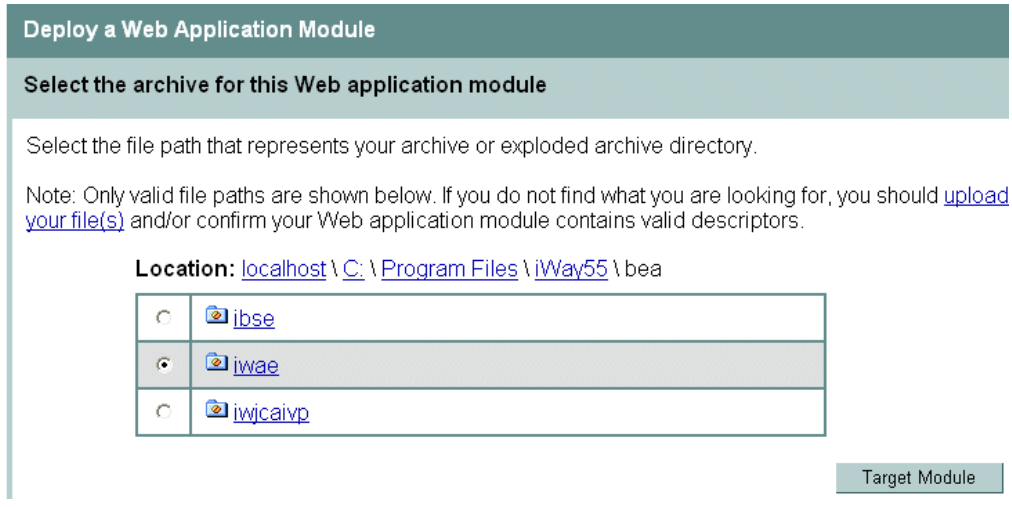
   Note: You can deploy JCA to a cluster, but you can only point it to one directory, and to the machine on which it is installed.

4. To deploy iBSE, select the option button next to the ibse directory and then click *Target Module*.

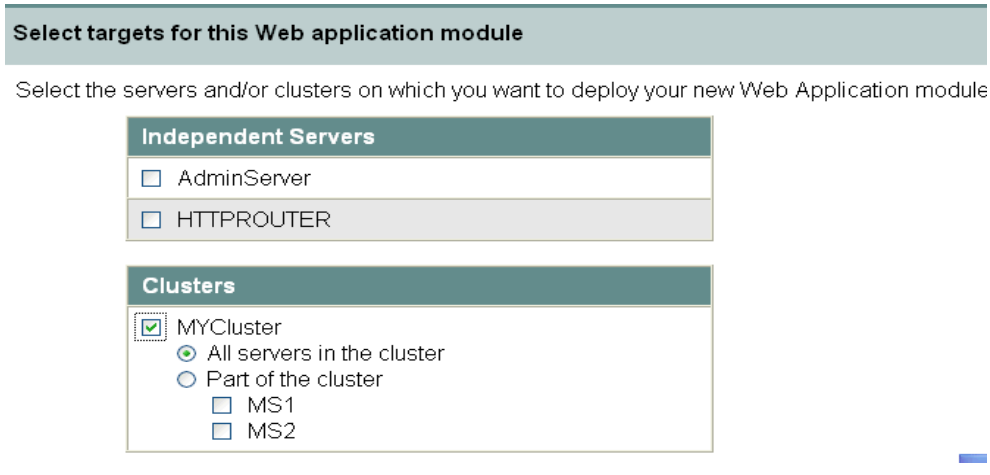


5. To deploy servlet Application Explorer, select the option button next to the iwae directory and then click *Target Module*.

   If you are using servlet Application Explorer, deploy it only on the admin server or one of the managed servers.

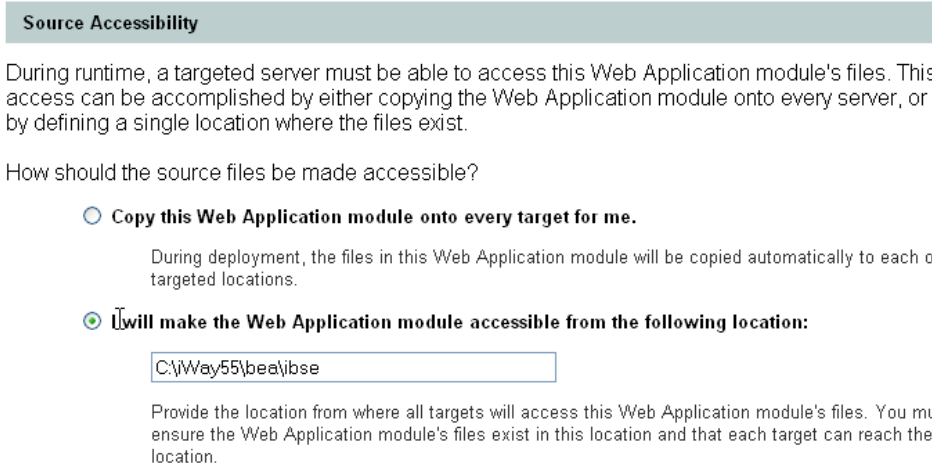


The following window opens.



6. Select the servers and/or clusters on which you want to deploy the application and click *Continue*.

The following window opens.



7. Select the *I will make the Web Application module accessible from the following location* option button and provide the location from which all targets will access iBSE.

   iWay Software recommends that you use a single instance of iBSE, rather than copying iBSE onto every target.

   Note: iBSE must use a database repository (SQL or Oracle). Do not use a file repository. You can select this in the Repository Type drop-down list in the iBSE monitoring page. After configuring a database repository, you must restart all of the managed servers.

   `http://hostname:port/ibse/IBSEConfig/`

   where:

   hostname

   Is where your application server is running. Use the IP address or machine name in the URL; do not use localhost.

   port

   Is the port specific to each server, since you deploy iBSE to an entire cluster. For example, 8001, 8002, or any other port that is specified for each managed node.

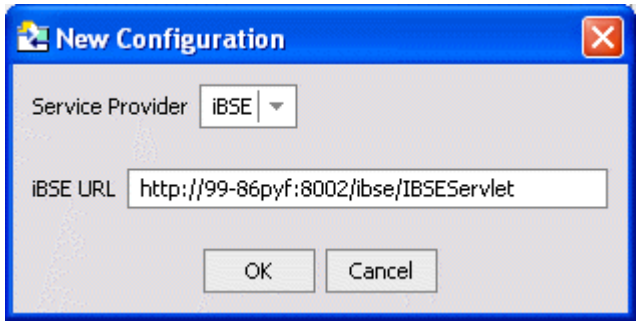
8. Click *Deploy*.

Procedure Configuring Ports and Channels in a Clustered Environment

To configure ports and channels in a clustered environment:

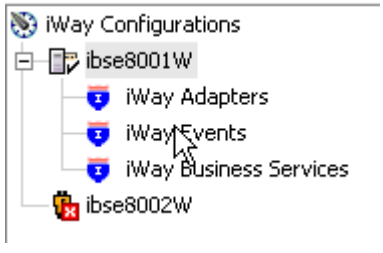
1. Open Swing Application Explorer in BEA WebLogic Workshop.

2. Create a new connection to the iBSE instance. For information on creating a new configuration, see *Creating a New Configuration* on page A-3.

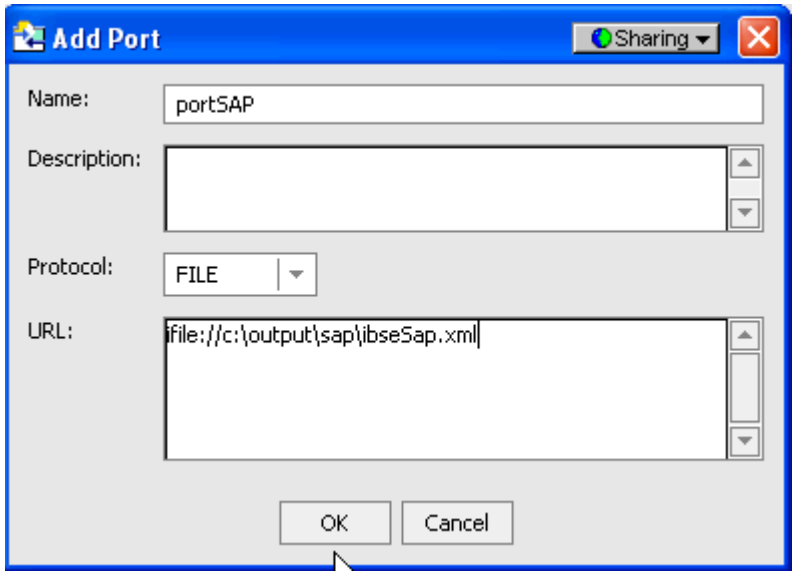


Note: Use the IP address or machine name in the URL; do not use localhost.

3. Connect to the new configuration and select the iWay Events node in the left pane of Application Explorer.



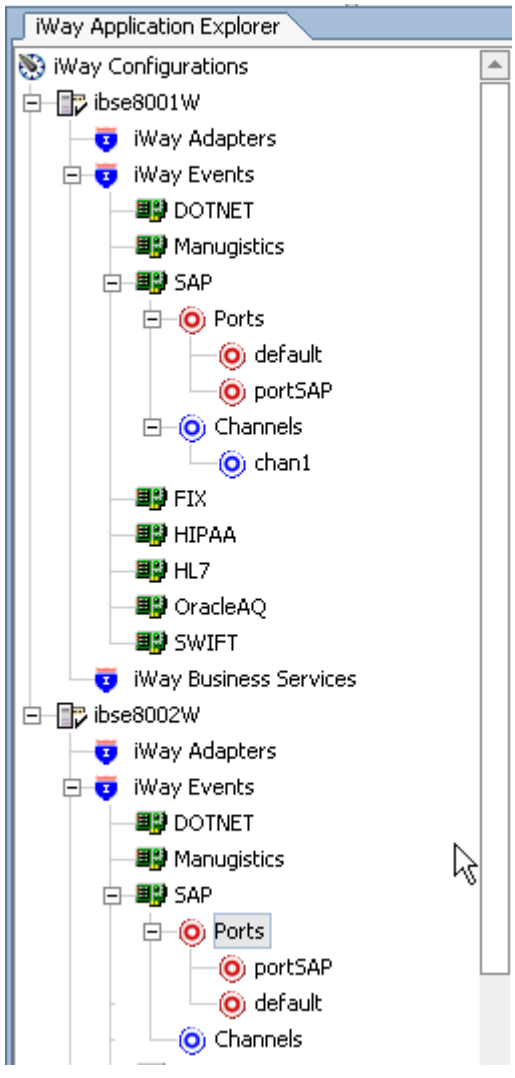
4. Select an adapter from the adapter list (in this example, SAP) and add a new port. For more information, see *Creating an Event Port* on page A-20.



5. Create a channel and add the port you created. For more information, see *Creating a Channel* on page A-35.
6. Click *Next* and enter the application server parameters.
7. Start the channel.
8. Create a new configuration and connect to the second iBSE instance.

   The connection to iBSE must be configured to each instance of the managed server.

The following graphic shows two configurations.



The following operations performed on one managed server will be replicated on all other managed servers:

- Create port and channel: Creates the channel and port under all available servers.
- Delete port and channel. Deletes the port and channel under all available servers.

The following operations must be performed on each server:

- Start channel. Starts the channel for the specific server.

- Stop channel. Stops the channel for the specific server.

Adding a Control for an iWay Resource in BEA WebLogic Workshop

Java controls provide a convenient way to incorporate access to iWay resources. You can add controls in BEA WebLogic Workshop to use Web services created by the Java Swing version of iWay Application Explorer, or you can add controls that enable you to take advantage of the JCA resources of Application Explorer.

Adding a Web Service Control to a BEA WebLogic Workshop Application

After you create an iWay Web service using Application Explorer and export the WSDL file, you can create a control for the Web service.

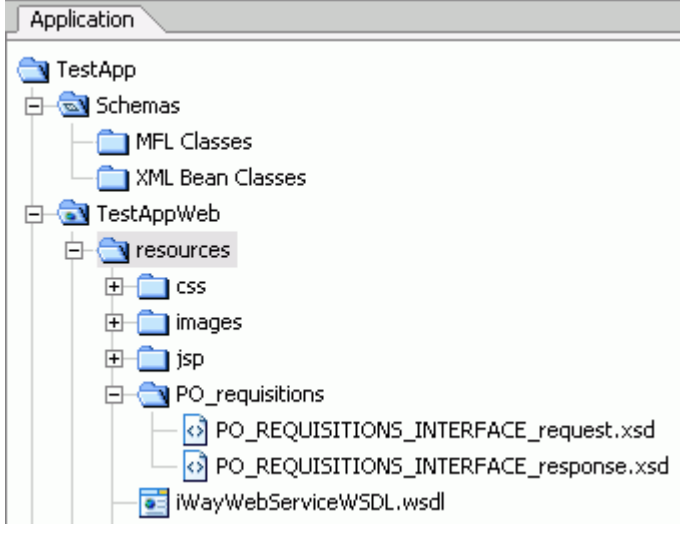
For more information on exporting a WSDL file, see *How to Export iWay WSDL for Use in BEA WebLogic Workshop Workflows* on page A-18.

Procedure How to Add a Web Service Control

To add a Web service control:

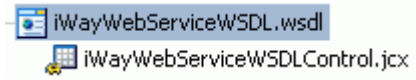
1. After exporting the WSDL file from Application Explorer, locate the file in the Application tab of your BEA WebLogic Workshop application.

   For example, a WSDL file saved to the \resources directory in your BEA WebLogic Workshop Web application directory structure appears as follows.



2. Right-click the *WSDL* file and select *Generate Service Control*.

The control for the WSDL appears below the WSDL file in the resources tree.



Adding an iWay Extensible CCI Control to a BEA WebLogic Workshop Application

An iWay control enables access to resources provided by Application Explorer when it is used in conjunction with a JCA deployment. You must add an iWay control before using it in a BEA WebLogic Workshop application. You must add the control in each application you create with BEA WebLogic Workshop.

The following section describes the enhanced CCI control, which is extensible and provides JCX with typed inputs and outputs for JCA in BEA WebLogic Workshop.

Overview

The extensible iWay CCI control provides:

- **Method and tag validation.** BEA WebLogic Workshop provides warnings regarding invalid methods and tags.
- **Improved error handling.**

You can now define new methods that rely on the generic *service* and *authService* methods. For example, you can define a JCX with a new method such as the following, without having to write casting code or explicit transformations:

```
sapComDocumentSapRfcFunctions.BAPIMATERIALGETDETAILResponseDocument
getDetail(sapComDocumentSapRfcFunctions.BAPIMATERIALGETDETAILDocument
aRequest) throws java.lang.Exception
```

In addition, the extensible CCI control now generates a JCX file to which you can add your own methods.

Using the Extensible CCI Control

The extensible CCI control functions much like a database control since it generates JCX files to which you can add your own methods.

Your own methods can use the correct input and output types rather than the generic XmlObject types that the JCA control uses. Since the control is just a proxy that uses a reflection to call the relevant method, it will take care of the casting for you. There is no longer a need to write custom code that does the cast or transformations that are cast between an XmlObject.

For example, instead of the generic XmlObject:

```
XmlObject service(XmlObject input) throws java.lang.Exception;
```

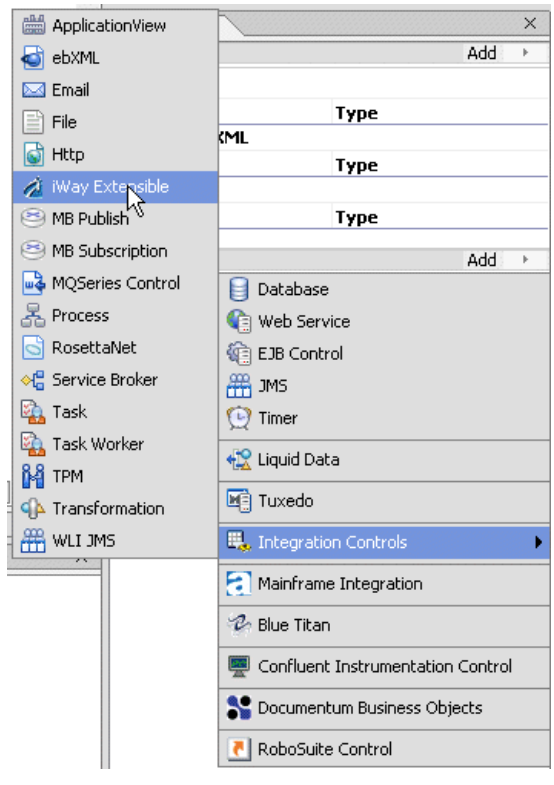
you will be calling:

```
BAPIMATERIALGETDETAILResponseDocument
getDetail(BAPIMATERIALGETDETAILDocument aRequest) throws
java.lang.Exception;
```

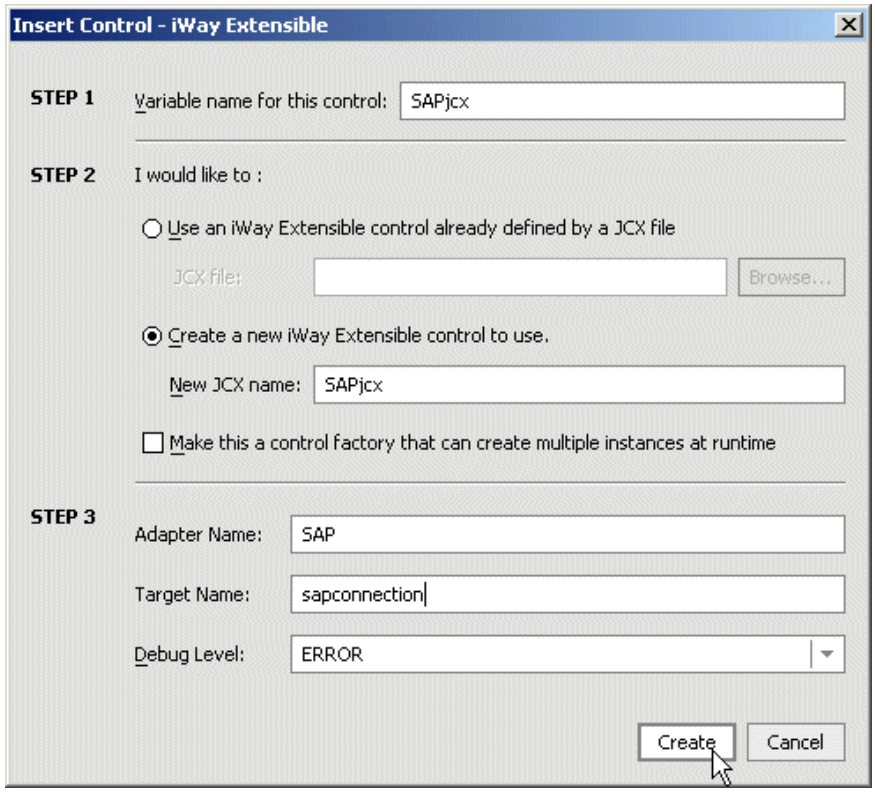
Example Defining a Control Using the Extensible CCI Control

The following sample JCX demonstrates how to define a control that uses the SAP BAPI_MATERIAL_GET_DATA using the extensible CCI control in BEA WebLogic Workshop.

1. Start BEA WebLogic Workshop and create a new project.
2. Click *Integration Controls* and select *iWay Extensible*.



The Insert Control - iWay Extensible dialog box opens.



3. Perform the following steps:

a. Provide a variable name for this control.

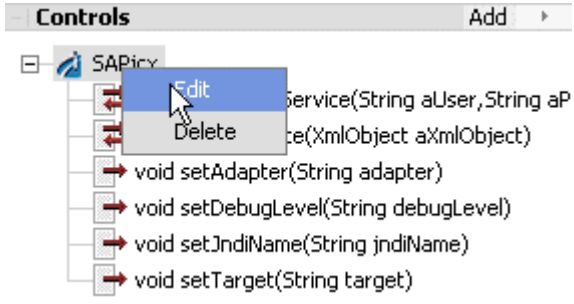
b. Click *Create a new iWay Extensible control* to use and provide a new JCX name.

c. Enter the adapter name, target name, and select a debug level from the drop-down list.

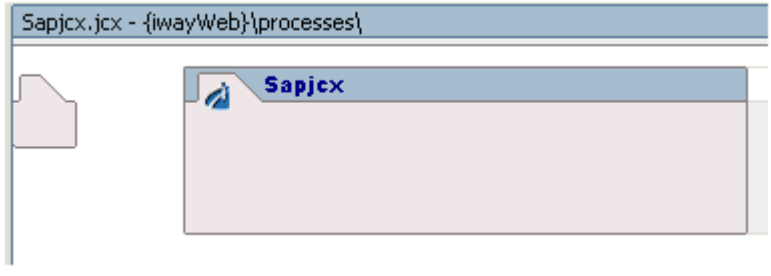
4. Click *Create*.

A new JCX file is created.

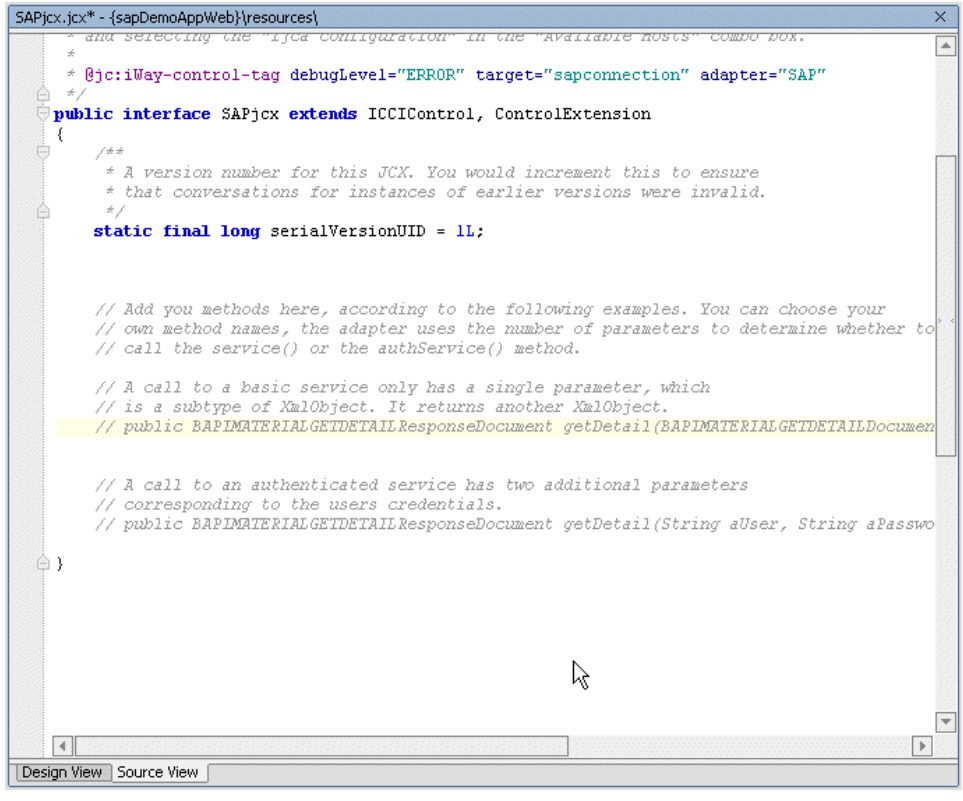
To edit an existing control, right click the control and select *Edit*.



The Design view is displayed.



5. Click *Source View*.



You can add your own methods that call the adapter's services

Reader Comments

In an ongoing effort to produce effective documentation, the Documentation Services staff at Information Builders welcomes any opinion you can offer regarding this manual.

Please use this form to relay suggestions for improving this publication or to alert us to corrections. Identify specific pages where applicable. You can contact us through the following methods:

Mail: Documentation Services - Customer Support
Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898

Fax: (212) 967-0460

E-mail: books_info@ibi.com

Web form: http://www.informationbuilders.com/bookstore/derf.html

Name:_____

Company:_____

Address:_____

Telephone:_____Date:_____

E-mail:_____

Comments:

Reader Comments

Information Builders, Two Penn Plaza, New York, NY 10121-2898 **(212) 736-4433**