CHAPTER 3

First Steps

This chapter introduces the ACE XML Manager web console. It covers these topics:

Logging In to the ACE XML Manager Web Console

Once the ACE XML Manager is installed on your network, you can log into the browser-based environment for developing the ACE XML Gateway policy, the ACE XML Manager web console.

The ACE XML Manager web console works with recent versions of most types of browsers. It is specifically supported on Mozilla Firefox 1.5.0.*x* and 2.0.0.*x* and Microsoft Internet Explorer 5.5 and 6. JavaScript functionality must be enabled in the browser for many ACE XML Manager web console features to work properly.

To log in to the ACE XML Manager web console:

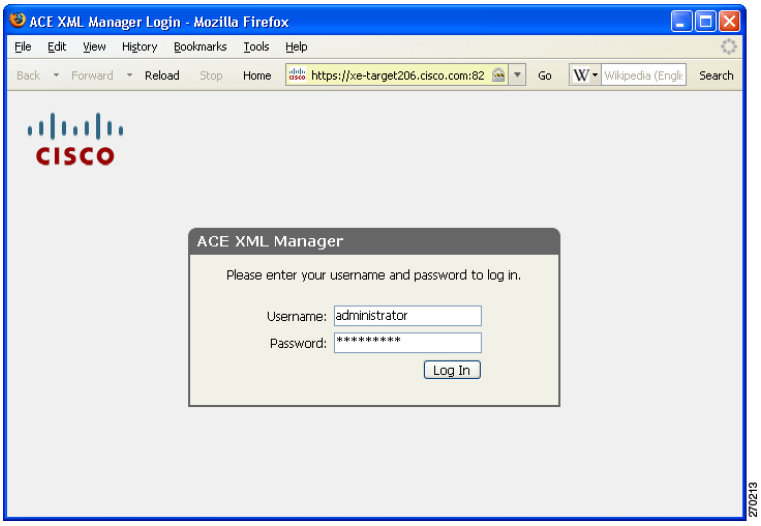
Step 1 On a computer accessible by network to the ACE XML Manager appliance, open a browser and go to the following address:

https://<*hostname*>:8243

Where <*hostname*> is the IP address or hostname of your ACE XML Manager. Notice that secure HTTP (HTTPS) is used for the connection and the default port on which the ACE XML Manager listens for console requests is 8243.

The browser displays the login page, as shown in Figure 3-1.

Figure 3-1 ACE XML Manager web console login



The hostname for the ACE XML Manager is configured at initial installation time. If you don't know the path to the login page for your installation, ask your administrator.

Other users who are already logged into the web console are listed on the login page. It is important to note when other users are logged into the console. The ACE XML Manager does not prevent you from overwriting each others' changes (the last save wins if a single settings page is edited by multiple users at the same time). For this reason, it is important that you check your work carefully and test new policies in a testing environment before deploying them to production.

Step 2 If this ACE XML Manager is used to administer multiple clusters of ACE XML Gateways, a menu may appear that allows you to choose which cluster policy you want to access. In this case, choose the name of the cluster to edit from the menu.

Step 3 Enter your username in the **Username** field. For example, if you are the administrator, enter `administrator` in this field. This is a preconfigured user account with full privileges to the console.

Note For details on adding user accounts for the ACE XML Manager web console, see Chapter 30, "Managing Web Console Users."

Step 4 Enter the password in the **Password** field.

Note The default password for the Administrator user is "swordfish". For security reasons, be sure to change the default password.

Step 5 Click the **Log In** button.

If you do not enter a valid username and password combination, an error message appears. Depending on how your administrator has configured Manager access, you may have a limited number of failed login attempts before the ACE XML Manager exits unconditionally and disables the user account (three, by default). This security feature applies to all user accounts except the administrator user account. (It does apply to user accounts created with the administrator user type).

For information on this feature and restoring a user account, see "Configuring Failed Login Attempt User Blocking" section on page 32-304.

If you enter a valid username/password combination, one of several pages may appear:

- The license error page appears if a license has not yet been configured for the ACE XML Manager. See the *ACE XML Gateway Administration Guide* for more information on acquiring and applying licenses for the ACE XML Gateway and Manager.
- The **Welcome** page appears if the ACE XML Manager has a valid license and the policy is not yet configured for service routing. From the **Welcome** page, you can start defining virtual services.
- If the policy contains virtual services, the **Dashboard** page appears. The Manager Dashboard provides an overview of system events and activities.

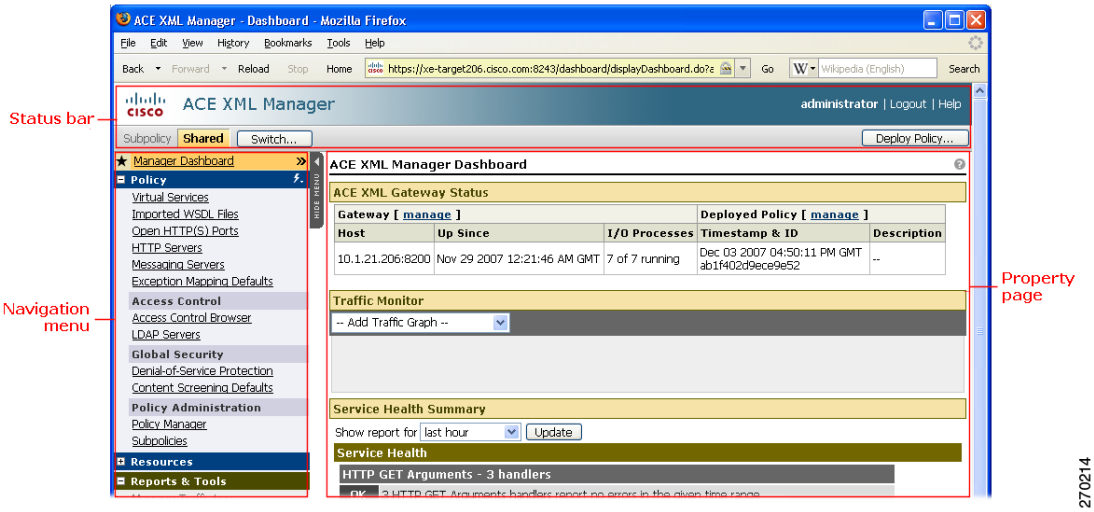
It is recommended that you change the password from the one assigned to you upon first login. To do so, click on your username at the top right of the page. In the **User Information** window, click the **Change Password** button to specify a new password.

By default, the console requires passwords to meet a minimum level of complexity. The password must be at least eight characters long, it should not consist of a dictionary word as more than a minimum percentage of the overall password, and it should not resemble a social security number or national ID number. In general, it is recommended that you use a combination of letters, numerals, and special characters in your password.

Navigating the ACE XML Manager Web Console

Figure 3-2 shows the main parts of the ACE XML Manager web console interface.

Figure 3-2 ACE XML Manager Dashboard



As discussed in the following sections, the ACE XML Manager web console is organized into these areas:

- Navigation Menu
- Status Bar
- Property Pages

Navigation Menu

The navigation menu appears at the left side of the console. It provides links to the primary settings and monitoring pages in the console, organized into these categories:

- **Policy** section contains links for pages for defining the rules and processing operations applicable to traffic handled by the ACE XML Gateway.
- **Resources** section links to pages for managing the resource files used in the policy. For more information, see Chapter 24, "Managing Resource Files."
- **Reports & Tools** links to pages for monitoring the status of the ACE XML Gateway and the network.
- **Administration** has links to pages that allow console administrators to control the ACE XML Manager itself, for example, for licenses, user accounts, audit logging, and diagnostics.

The Quick Links button () appears next to the **Policy** heading of the navigation menu. It provides access to common tasks, including importing a WSDL file, creating a virtual service, and creating an authenticator (the policy object used to control access to services).

Status Bar

The status bar appears at the top of every page in the console. It displays the currently active subpolicy and the username of the user account currently accessing the console. It provides buttons for common operations in the console, such as deploying the policy and logging out.

Administrator users can configure banner text that appears in the status bar, for example, to post notifications or other types of information for other console users.

A subpolicy is a container for organizing objects within a policy. The *Shared* subpolicy is a built-in subpolicy that's present whether or not you are using subpolicies to organize your work. It contains the common objects used throughout all subpolicies.

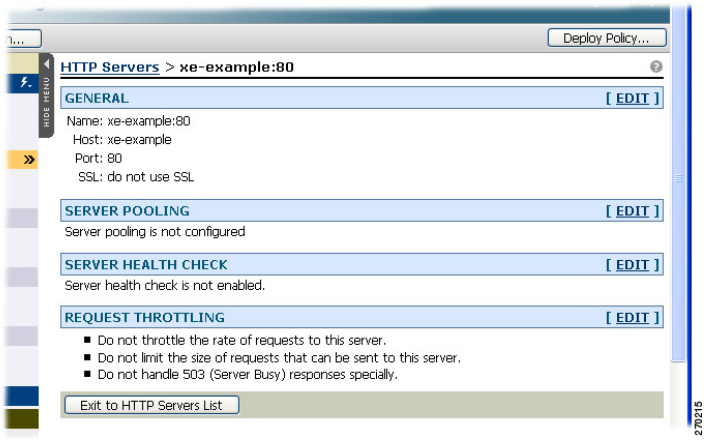
If subpolicies besides Shared exist in the policy in your environment, the **Switch** button appears next to the subpolicy label. Click the **Switch** button to change your working context to another subpolicy.

For more information on subpolicies, see "Working with Subpolicies" section on page 26-240.

Property Pages

A property page displays information or settings for a particular area of the system's operations. In general, property pages are divided into sections bounded by color headings. The sections display the current setting for a settings category. To access controls where you can change the settings, click the **Edit** link in the heading, as in Figure 3-3.

Figure 3-3 Property Page



Adding Gateways to the Manager's Control

As described in the *ACE XML Gateway Administration Guide*, an ACE XML appliance can operate in one of three modes: as a Gateway, Manager, or standalone appliance (in which the appliance operates as both Gateway and Manager).

For a standalone appliance, after initial configuration, the ACE XML Manager is already configured for self-management (that is, an entry for itself exists in the Manager's managed Gateway list). You can start working on the policy immediately, without having to add Gateways to the configuration.

However, if the appliance is in Manager-only mode, you will need to add a Gateway to the Manager's administrative control before you can deploy and test a policy, as described here.

Note For a standalone appliance, the ACE XML Manager can control other Gateway appliances as well as its own Gateway instance. Therefore, these steps are also applicable if you want to add Gateways to the administrative control of a Manager on a standalone appliance.

An ACE XML Gateway should not be configured to be in the control of more than one ACE XML Manager at a time. This restriction applies to management by actual Manager appliances or Manager instances created with the Multiple Cluster Management feature.

The general steps for adding a Gateway to the Manager's control are:

1. When configuring the operating mode of the Gateway from the appliance shell interface, specify the IP address of the Manager that is to control this Gateway.

Note For more information, see the *Cisco ACE XML Gateway Administration Guide*.

2. In the web console for the ACE XML Manager, add the Gateway to one of the Manager's cluster pools, such as to its default cluster.
3. Check the licensing status of the added ACE XML Gateway in the web console. If needed, request and apply a license.

This section describes step 2, how to add a gateway to one of the Manager's clusters. Once the gateway belongs to a cluster group, it can receive policy deployments from the Manager. In turn, the gateway reports on its activities back to the Manager, which aggregates logging information for all Gateways in its control. For more information on steps 1 and 3, see the *ACE XML Gateway Administration Guide*.

Note An ACE XML Manager can control more than one cluster of Gateways. While all Gateways in a single cluster should have the same policy version, multiple clusters in the Manager's control can apply different policy versions. For more information, see Chapter 31, "Managing Gateway Clusters."

Adding Gateways to the Default Cluster

To add an ACE XML Gateway to the Manager's control, you add it to a cluster in the Manager configuration. As noted, you do not need to perform these steps for a standalone appliance; they are needed only if configuring a Manager-only appliance or to add additional Gateways to a standalone appliance's administrative control.

The Manager comes with a preconfigured cluster named "Default Cluster" to which you can add ACE XML Gateways. Notice that you can rename the default cluster and make other changes to its settings. You should not add new clusters to the Manager configuration unless you specifically intend to maintain separate ACE XML Gateway environments. For more information, see Chapter 31, "Managing Gateway Clusters."

To add an ACE XML Gateway to the default cluster:

Step 1 As a user with administrator privileges in the Manager web console, click the **Cluster Management** link from the navigation menu.

The cluster management page should show a cluster named "Default Cluster." On the Manager of a standalone mode appliance, the Default Cluster lists this appliance as the only member. Otherwise, new installations will show the default cluster as empty.

Step 2 Add the gateway to the cluster by clicking the **edit** link next to the **Default Cluster**.

Step 3 Optionally, modify the preconfigured settings for the default cluster, such as its name and HTTPS port and the security certificate used for SSL access to the Manager web console.

The **SSL Certificate** shown on this page applies to the connection from a web browser to the Manager web console. As indicated in the menu, the Manager provides a temporary certificate that is used by default. It is recommended that you replace the built-in certificate with a server certificate you generate. If the Manager and development workstations will be operating within a secure network, you may choose to use a self-signed certificate. However, for greater security it is recommended that you use a CA-signed certificate, particularly if the cluster is deployed in a production environment.

You can generate a new certificate to use for the browser connection by clicking the **Manage SSL Certificates** button on the **Cluster Management** page. From there, use the **Generate CSR** button to generate a certificate signing request. For more information, see "Generating a CSR" section on page 24-224. Once the server certificate is generated and uploaded in the Manager, choose it from the menu on this page to apply it to the browser connection.

Step 4 In the **Cluster Members** text field, type the IP address and administration port of each ACE XML Gateway you want to add to this cluster. The address for each Gateway should be on its own line in the text field, such as:

10.0.5.12
10.0.5.22

The administration port used by the Manager and Gateway to exchange administrative information, such as log events, is 8200. If you have a specific network prerequisite that prevents you from using it, you can specify another port by appending it to the IP address.

Step 5 Click **Save Changes**.

Step 6 After being added to a cluster, the Gateway usually needs to be configured with a license. To check the license status of the gateway, open the License Management page in the web console. If a license is required for the gateway, refer to the *ACE XML Gateway Administration Guide* for information on acquiring and applying product licenses to the appliance.

The ACE XML Gateway should appear as a member of the cluster in the Cluster Management page. You can now deploy the policy to this ACE XML Gateway from the Policy Manager.

For more information on working with clusters, see Chapter 31, "Managing Gateway Clusters."

Virtualizing Services by WSDL Import

The easiest way to get started on policy development for the ACE XML Gateway is using the web service configuration wizard. The wizard generates policy objects based on a WSDL that describes the backend services you want to virtualize at the ACE XML Gateway. The wizard can also discover services by querying a UDDI registry.

Note You can import RPC- or Document-style WSDLs into the Manager. The WSDLs can indicate literal or encoded style usage. However, when the Manager generates WSDLs describing the services virtualized at the ACE XML Gateway, it produces only RPC/literal or Document/literal WSDLs only, not encoded style WSDLs, which are not WS-I-compliant. For more information on generating WSDLs, see "Generating WSDLs for Services at the ACE XML Gateway" section on page 28-260.

After service discovery, you have the option of importing the services into the policy. Importing generates the policy objects that effectively virtualize the service at the ACE XML Gateway, enabling traffic for that service to be routed through the ACE XML Gateway. These objects include virtual services (or handlers and service descriptors), server objects and ports.

There are a few points to note about WSDL import and service discovery:

- To discover services on a UDDI registry, you will need to know the inquiry URL for the registry.
- A WSDL file can be imported directly from a file system or network location (by URL). However, if the WSDL contains URL references and you are attempting to import the WSDL from a file system location, the URL references must be fully qualified (not relative) for a successful import.

To generate policy setting by WSDL import:

Step 1 While logged in to the ACE XML Manager web console as an Administrator user or a Privileged user with the Routing role, open the Virtual Services page by clicking the **Virtual Services** link in the navigation menu.

Step 2 From the Virtual Services menu, choose **Start Virtual Web Service Wizard** and click **Go**.

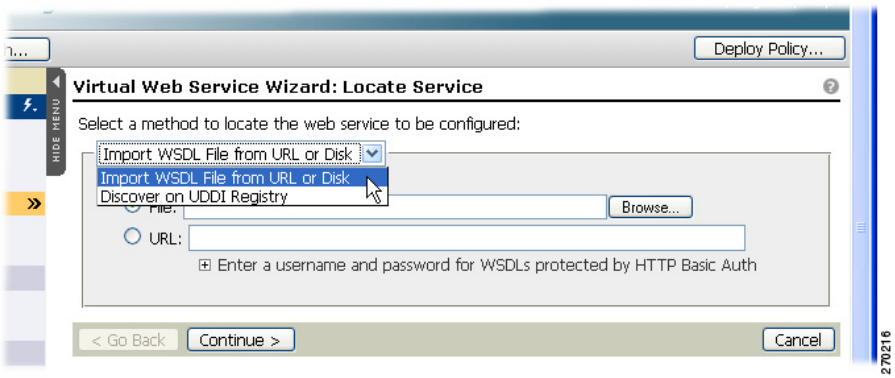
The menu appears at the top of the page in the Virtual Services browser.

Step 3 In the locate service menu, choose the source of the WSDL to be imported from these options:

- Import WSDL File from URL or Disk

- Discover on UDDI Registry

Figure 3-4 Locate Service options



Step 4 If you chose the **Import WSDL File from URL or Disk** option, access the WSDL file from a disk file system location as follows:

a. Click the **Browse** button.

b. Use the controls in the **File Upload** dialog box to specify the WSDL file. The path to the selected WSDL file appears in the **File** field on the **Import a New WSDL File** page.

For security reasons, the Manager will not accept WSDL files imported from a disk location that have `import` statements for resources (such as schema files) identified by relative URI. The ACE XML Manager requires fully qualified resource identifiers in `import` statements.

Alternatively, retrieve the WSDL file from a network location by URL:

a. Specify the URL that identifies the WSDL file location.

b. If access to the WSDL requires authentication, click the expand control labeled **Click here to enter a username and password for WSDLs protected by HTTP Basic Auth** and enter a username and password.

Step 5 If you chose the **Discover on UDDI Registry** import option:

a. In the **UDDI Inquiry URL** field, enter the full URL that the UDDI presents for service inquiries, such as:

http://uddihost.example.com:8090/uddi/inquiry

b. If needed, enter the publish URL for the UDDI server in the **UDDI Publish URL** field and a username and password for a user account with publishing access to the UDDI server.

In most cases, the inquiry API value is sufficient for service discovery. However, to achieve password-protection of the information they publish, registries often use the publish API mechanism. For registries that do so, enter the publish URL in the **UDDI Publish URL** field and username and password.

c. If the source UDDI registry is version 3, you need to supply the Security URL for the registry with a username and password. If you do not know the values to use, contact the administrator of the UDDI registry.

d. Click **Continue**.

After a moment, the ACE XML Manager shows what services it found on the UDDI registry. You can view more information on the WSDL by expanding **WSDL details**.

If service discovery does not find services on the UDDI source, it indicates the fact on the next page.

The ACE XML Manager attempts to resolve any link referenced by the UDDI registry, not all of which may refer to WSDLs. In this case, the following message appears:

The following URLs were found, but did not refer to readable WSDLs

A WSDL-read attempt may also fail if:

- The WSDL is invalid.
- The link results in a HTTP 404 response (file not found) or for other network or security issues is unresolvable.
- Access to the link requires authentication.
- The WSDL imports another file (typically an XML schema or other WSDL) that in turn could not be retrieved for some reason.

e. If service discovery was successful, in the **Choose WSDL** page click the radio button of the service that you want to import and click **Continue**.

Step 6 In the **Consumer Interface** page, choose a port on which you want the services to be exposed at the ACE XML Gateway from the **HTTP Port** menu. In most cases, the default value can be accepted.

Step 7 In **Exposed Path**, change if desired the default URL at which the services will be exposed at the ACE XML Gateway. This path is appended to the ACE XML Gateway hostname to form the full URL clients use to access the service at the gateway.

Step 8 By default, the wizard creates server objects in the policy based on connection information in the WSDL. Select the checkbox labelled **Override host '<host>' in WSDL with** to use a server chosen from the menu instead of the one indicated in the WSDL. The server you choose from the menu is configured to be the backend service for the virtual services resulting from the WSDL import.

If this option is selected, server objects are not created for the hosts in the WSDL. This option is useful if the host for the service indicated in the WSDL (and shown in the label) is not the actual backend host that the Gateway needs to address in outgoing requests. The menu lists the servers defined in the policy. See Chapter 14, "Configuring Backend Server Settings," for more information.

Step 9 Choose access control setting for the service. You can choose no access, public access, or controlled access, in which consumers must meet the requirements specified by the authorization group you choose.

Note Credential-based access control is available for the XML Security Gateway and Secure XML Router appliances only, not for the XML Accelerator.

Public access allows you to test the service configuration before creating access policies. However, in most cases, access to services will eventually need to be controlled in some manner. For more information, see Chapter 6, "Controlling Access to Services."

Step 10 For the **Default Message Logging** option, choose the logging level for the services. For initial development and testing, you may want to log message bodies. However, for production traffic or performance testing, you should log statistics only.

Note You can reset the logging level for all operations at once later from the **Handler Group** settings page.

Step 11 Optionally, configure these settings by clicking the expand control next to the **Advanced Options** heading:

- **Import Bindings**. A WSDL may specify multiple protocol bindings for the operations it describes. You can choose one or more protocol bindings to import, from SOAP, HTTP GET, and HTTP POST. This choice determines the protocol type of the virtual services created in the policy as a result of the import. Since multiple bindings—if a WSDL has them—usually describe the same set of services, you can usually leave binding at the default option, SOAP.
- **Validate the WSDL file before importing**. Before the WSDL is imported, the ACE XML Manager can check that it is valid with this option. The WSDL is checked against the schema for the WSDL specification. If the WSDL is invalid, the ACE XML Manager displays line-by-line errors found in the results page.
- **Strip elementFormDefault attributes from XML schemas imported from WSDL files**. Use this option to avoid problems that arise when attempting to import RPC-style services using WSDLs that were generated by frameworks that implement this attribute incorrectly.

  Selecting this option ensures that this element is stripped for SOAP RPC virtual services upon WSDL import. (It does not affect SOAP Document-style virtual services.) The `elementFormDefault` are incorrectly given a value of `qualified` by some frameworks, which prevents the ACE XML Manager from importing the WSDL successfully.
- **Configure SOAP Document virtual services to match requests based on SOAP method in addition to SOAPAction**. If document-style SOAP services use SOAP method values to distinguish the operation addressed by a message, choose this option to have the ACE XML Gateway match traffic to a generated virtual service based on the values of both the SOAP method and SOAPAction.

  For some virtual services, this is required to disambiguate service invocations. The SOAP method is the first child node of the SOAP body in the SOAP message.

  This option is enabled automatically if the ACE XML Manager detects that the SOAPAction does not alone disambiguate the operations in a WSDL.

  For more information, see "About SOAPAction and SOAP Method Name" section on page 3-26.
- **Condense SOAP Document operations into one virtual service per WSDL "Service" element, if possible**. If importing a WSDL that defines SOAP Document, you have the option of creating a virtual service for each operation in the WSDL or of combining the operations from each service element of the WSDL into a single virtual service.

  It is suggested that you leave this option enabled, since using a condensed virtual service provides a single point to configure settings for multiple related operations. If specific settings are needed for an operation, you can later override that operation's definition in the common virtual service.

  For more information, see "Working with Multiple Operation Virtual Services" section on page 4-37.
- **Create a separate handler and service descriptor for each operation**. If selected, the ACE XML Manager creates separate handlers and service descriptors instead of basic virtual services for the service operations. You should choose this option if you want to employ branched routing (that is, have messages routed between a single consumer interface and multiple backend services, or vice versa) or to use other features not available in basic virtual services, such as response caching or argument mapping.

  In most cases, you can leave this option cleared and, if necessary, switch the virtual service to advanced mode later.

  For more information, see Chapter 5, "Working with Handlers, Routes, and Service Descriptors."
- **Create a direct-mapping route between each handler and service instead of a pass-through route**. Controls how the ACE XML Gateway processes messages according to these modes:

  - With direct mapping, an incoming message is disassembled at the ACE XML Gateway and recreated according to policy settings and the Gateway's usual normalization measures. Headers or other message elements that are not standard for the message protocol or specifically provided for in the policy configuration are removed. This option provides greatest security and imparts the benefits of message normalization, but can lead to unanticipated integration problems.
  - A pass-through route is more permissive. Instead of completely disassembling and recreating the message, the ACE XML Gateway propagates unexpected headers and other message attributes to the outgoing interface.

  Since direct-mapping mode may result in unexpected message modifications, do not choose this mode unless you are confident it is suitable for your case.

- **Subscribe to updates of this WSDL from UDDI**. If using UDDI discovery to generate virtual services and the UDDI registry supports UDDI version 3, you can subscribe to changes to the WSDL. When this feature is enabled, the Manager polls the UDDI registry whenever the **Imported WSDL Files** page is accessed. If the source WSDL has changed, a notice on the page indicates that the policy is out-of-date. You can then update the WSDL from the **Imported WSDL Files** page, which propagates the changes from the source to the working policy.

  To subscribe to WSDL updates, enable the checkbox and configure the URL fields under the option (most fields will be prepopulated with the values you entered on the WSDL discovery page). For more information on what values to use, contact the administrator of the UDDI registry.

Step 12 When finished, click **Continue**.

Step 13 In the final page of the sequence, either deploy the changes to the ACE XML Gateway (making the services available through the ACE XML Gateway), request approval, or navigate to other pages of the console to continue working. If approval-based deployment is enabled and you do not have sufficient privileges to deploy the policy, the **Request Approval** button appears on the final page. You use it to start the approval request process. (For more information, see Chapter 25, "Deploying the Policy.")

The resulting policy objects contain minimal settings for the service configuration. In most cases, you will want to add access requirements, encryption behavior, message validation requirements, and other settings and behaviors associated with the service.

Troubleshooting WSDL Import

The WSDL import process may not always complete successfully due to a variety of potential issues. Validating the WSDL file against the XML Schema that defines the Web Services Description Language may help you avoid certain problems. When this optional behavior is enabled, the ACE XML Manager attempts to validate the WSDL file before it imports the file. If the validation fails, or if the WSDL file is not syntactically correct XML, the ACE XML Manager does not import the WSDL file.

Examples of conditions that produce import errors include:

- **The WSDL file uses an embedded XML Schema that does not define a valid target namespace.** You must replace the WSDL file with a corrected version that provides a valid target namespace.
- **The WSDL file contains duplicate operation names.** You may possibly correct this error by editing the WSDL file manually to remove duplicate operations.
- **The WSDL file refers to a complex type that is not defined.** You must correct the error in the WSDL file.

- **The WSDL file imports another WSDL file that is not available.** You must edit the WSDL file to remove the dependency or you must make the imported WSDL file available.

  Supplying a URL to a WSDL file that may be available at a later time is not sufficient to resolve this problem. For security reasons, the ACE XML Gateway never downloads WSDL or other resources during enforcement of a policy. Instead, it downloads them at the time the policy is prepared for deployment. Therefore, all WSDL and other resource files must be available to the policy before deployment.

- **The WSDL file imports an XML Schema that is not available.** You must edit the WSDL file to remove the dependency or you must make the imported XML Schema available.

  All external files the WSDL file imports—including XML Schema files—must be available to the policy before deployment.

When import fails because a WSDL file imports another WSDL file or XML Schema that is not available, you have two options to correct the problem: first, you can manually import the required additional WSDL or XML Schema file. If that is not practical, you can instead edit the WSDL file to remove references to the unavailable files. Be aware that in many cases it may not be easy, or even possible, to edit a WSDL by hand to produce a working import.

About SOAPAction and SOAP Method Name

SOAPAction is defined in the SOAP 1.1 specification as an HTTP header that helps distinguish one operation from another. It is a required header for SOAP 1.1; an HTTP request is not recognized as a SOAP 1.1 request unless it has at least an empty SOAPAction header. For SOAP 1.2 it is optional. Specifically, in SOAP 1.2 it is defined as an optional amendment to the HTTP Content-type header.

SOAP method name is a concept that applies only to SOAP RPC-style messages. In RPC-style SOAP, the method name is the fully qualified name of the first child of the SOAP Body element. The SOAPAction identifies a Document-style SOAP service so that the receiving node is not required to inspect the contents of the SOAP Body. The SOAP Method Name is typically used to identify an RPC-style SOAP service, with the SOAPAction containing an empty or generic value.

Some SOAP frameworks do not rigorously respect this convention (WebLogic 8, for example), and instead emit WSDL files with operations that have identical SOAP actions. For these cases, the ACE XML Gateway provides an optional flag for SOAP Document-style handlers that indicates that the name and namespace of the body element of incoming messages should be considered when they are assigned to a handler. This flag can be set at WSDL import time (the ACE XML Manager can usually determine whether this option is necessary, and enable it at WSDL import time if required) or from the SOAP Document Consumer Interface settings.

The ACE XML Gateway always checks that incoming SOAP messages have the expected SOAPAction value. The fully-qualified SOAP Method Name (with name and namespace) is always checked for RPC-style SOAP services. The element name and namespace of the Body Entry element are checked for Document-style services only if the flag is set.

Importing BPEL WSDL Files

Business Process Execution Language (or BPEL) is a language for modeling potentially complex, long-running processes that involve multiple transactions, participants, and services. BPEL prescribes the use of Web services for interaction between process participants. Therefore, BPEL information may be included in WSDLs (in the form of a WSDL extension).

When you import a WSDL into the ACE XML Manager that includes a BPEL definition, the Manager recognizes and retains the BPEL information, associating it with the policy objects generated as a result of the WSDL import. While this information does not affect ACE XML Gateway handling of messages for the services, it is often needed by service endpoints. Therefore, when you generate WSDL from the Gateway policy for those services, the ACE XML Manager propagates the BPEL information to the generated WSDL.

Note the following points regarding BPEL support in the ACE XML Manager and Gateway:

- BPEL 1.1 is supported (BPEL 2.0 is not).
- At import time, the Manager can validate the WSDL. However, the ACE XML Manager does not check the WSDL against the BPEL-defined schema, only against the WSDL schema.
- BPEL information import occurs at WSDL import time automatically, based on the content of the WSDL. No import options need to be set for this capability. A notice appears in the Manager web console at import time that indicates that BPEL extensions were found in the WSDL and will be imported.

Logging Out of the Console Securely

For security reasons, it is extremely important that you do not leave any user session with the ACE XML Manager unattended. When you finish a user session or cannot be physically present at the console that presents your user session, you must log out of the ACE XML Manager and close all browser windows you used. If you do not, other users could view pages cached by your browser during the user session.

Take the following steps to log out of the ACE XML Manager securely:

Step 1 Click the **Logout** button.

Step 2 In the confirmation dialog, click the **OK button** to log out.

Step 3 Close all browser windows used in your console session.

For additional security, clear your browser's cache after you log out of the ACE XML Manager.