HP SOA Systinet

Software Version: 2.52, Standard Edition

User Guide

Document Release Date: November 2007
Software Release Date: November 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Third-Party Web Sites

Mercury provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

Trademark Notices

Java™ is a US trademark of Sun Microsystems, Inc. Microsoft®, Windows® and Windows XP® are U.S. registered trademarks of Microsoft Corporation. IBM®, AIX® and WebSphere® are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries. BEA® and WebLogic® are registered trademarks of BEA Systems, Inc.

Contents

Welcome to This Guide

Welcome to HP SOA Systinet, the foundation of Service Oriented Architecture, providing an enterprise with a single place to organize, understand, and manage information in its SOA. The standards-based architecture of SOA Systinet maximizes interoperability with other SOA products.

How This Guide is Organized

SOA Systinet User Guide describes the features and functionality of the product for normal users. It is organized according to the UI – a part for the common UI features and then a part for the features and functionality of each tab.

Important: This guide describes the default installation of SOA Systinet. The format and content of each tab can be modified using HP SOA Systinet Customization Editor. All screenshots in this guide are from the **Service Publisher** perspective. The **Administrator** perspective displays additional functionality described in HP SOA Systinet Administrator Guide and the **General** perspective may not display all the functionality described in this guide.

This guide contains the following parts:

Part I, “Getting Started”. An introduction to the features of the user interface and the common tasks that can be accessed from all pages.

Part II, “Dashboard”. The features of the **Dashboard** and the tasks performed there.

Part III, “Services”. A guide to the **Services** tab and the creation and management of services, lifecycles, and contracts.

Part IV, “Policies”. Describes the **Policies** tab and the use and management of policies.

Part V, “Tools”. A guide to the **Tools** tab and the governance and repository content management features accessed from it.

Document Conventions

The typographic conventions used in this document are:

run.bat make	Script name or other executable command plus mandatory arguments.
[--help]	A command-line option.
either | or	A choice of arguments.
replace_value	A command-line argument that should be replaced with an actual value.
{arg1 | arg2}	A choice between two command-line arguments where one or the other is mandatory.
`rmdir /S /Q System32`	Operating system commands and other user input that you can type on the command line and press **Enter** to invoke. Items in *italics* should be replaced by actual values.
`C:\System.ini`	Filenames, directory names, paths and package names.
`a.append(b);`	Program source code.
`server.Version`	An inline Java or C++ class name.
`getVersion()`	An inline Java method name.
Shift-N	A combination of keystrokes.
Service View	A label, word or phrase in a GUI window, often clickable.
OK	A button in a GUI window.
New->Service	Menu choice.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (**http://h20230.www2.hp.-com/svi_partner_list.jsp**), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.
- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: **http://hp.-com/go/hpsoftwaresupport**.
- For the latest information about support processes and tools available for products formerly produced by Systinet, we encourage you to visit the Systinet Online Support Web site at: **http://www.systinet.-com/support/index**.
- If you have additional questions, contact your HP Sales Representative.

HP Software Support

You can visit the HP Software Support Web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts

- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to: http://h20230.www2.hp.-com/new_access_levels.jsp

To register for an HP Passport ID, go to: http://h20229.www2.hp.com/passport-registration.html

Part I. Getting Started

This part explains how to access SOA Systinet, the features of the user interface, and the common functions accessible from every page.

This part contains the following chapters:

1 Accessing the User Interface

Before attempting to use SOA Systinet, ensure that it is running on the server you wish to access.

To access the web UI use one of the web browsers listed in the Supported Platforms section in the HP SOA Systinet Installation Guide.

Enter the URL into your browser in the form:

```
protocol://server:port/context/systinet/platform/web
```

where:

- *protocol* is either http, or https if you want to create a secure connection using SSL
- *server* and *port* and *context* are determined during installation

The default port is 8080 for HTTP and 8843 to use SSO. For example:

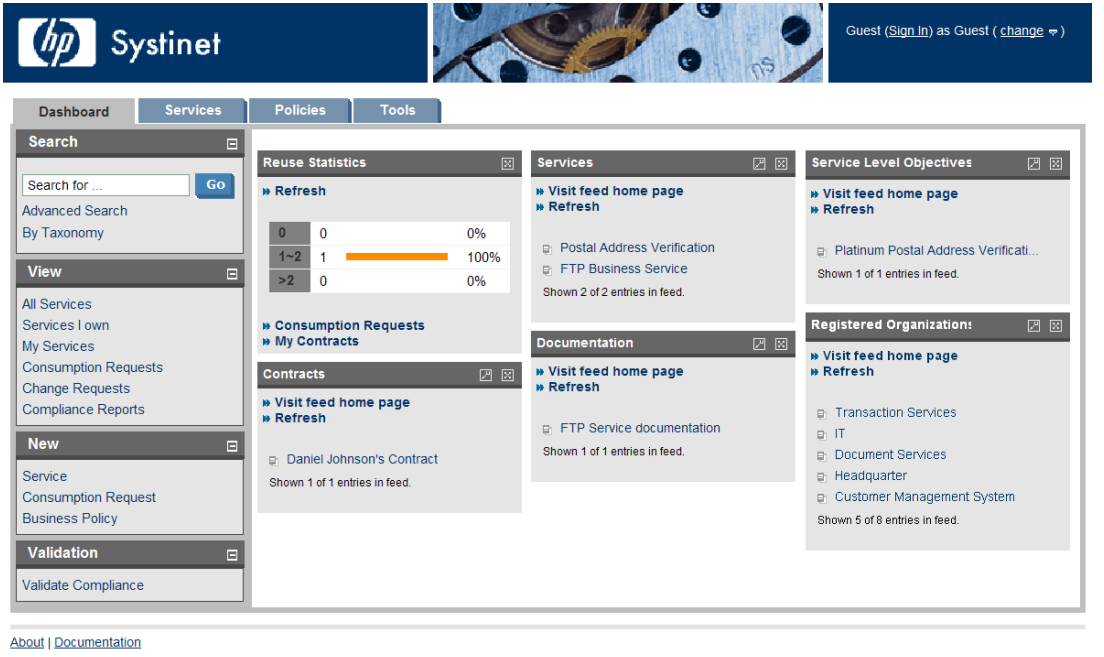
```
http://mypc:8080/soa/systinet/platform/web
```

or:

```
https://ourserver:8843/soa/systinet/platform/web
```

This should display the **Dashboard** in your browser:

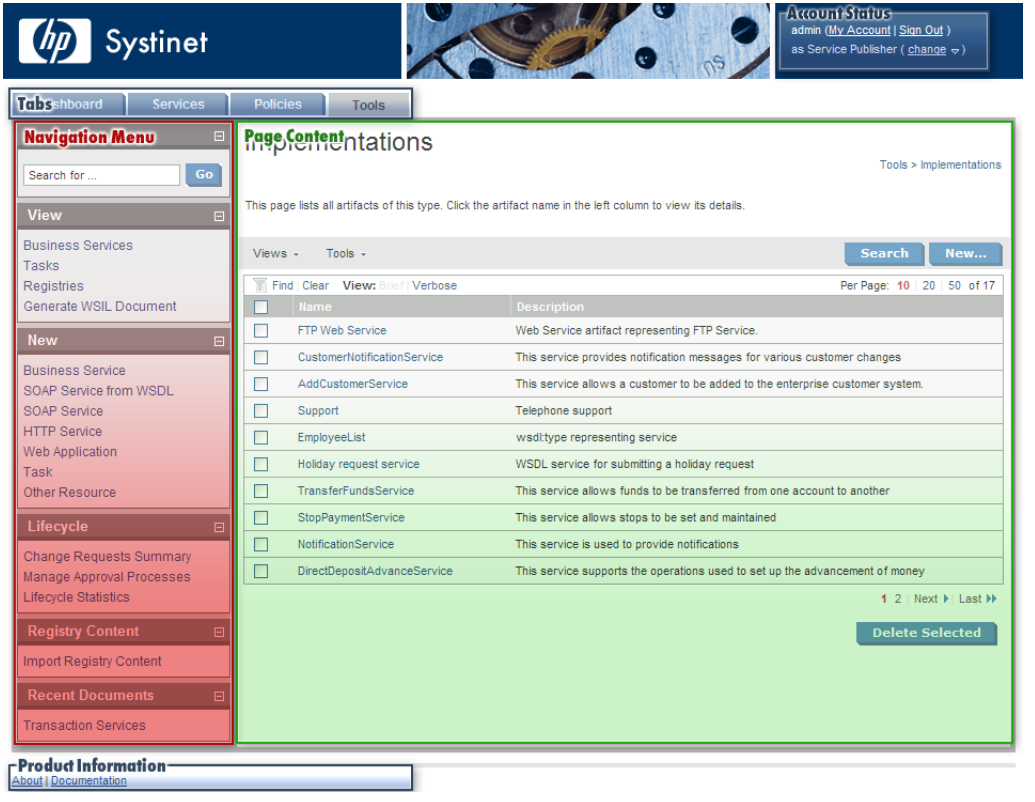
Figure 1. The Dashboard at Start-up



2 Features of the User Interface

The SOA Systinet user interface has the same look and feel throughout:

Figure 2. A Typical SOA Systinet Page



Every page contains the following common elements:

- **Tabs** are the access to the main components of SOA Systinet described in Tabs on page 20.
- The **Menu** contains a set of component specific links described in Menus on page 20.
- **Account Status** controls sign-in, personal account management and your view of SOA Systinet described in Account Status on page 21.
- **Product Information** gives access to product and documentation information.

Tabs

The UI is split into functional components. At the top of every page the tabs access these components.

Figure 3. SOA Systinet Tabs

Clicking a tab opens the main page of that component:

The **Dashboard** is the first page you see when you start SOA Systinet. It contains portlets showing a customizable real-time view of your SOA. The Dashboard is described in Features of the Dashboard Tab on page 39.

The **Services** tab is the central location which shows all information about services and contracts in one place to provide easy access and simple management. The **Services** tab is described in Features of the Services Tab on page 51.

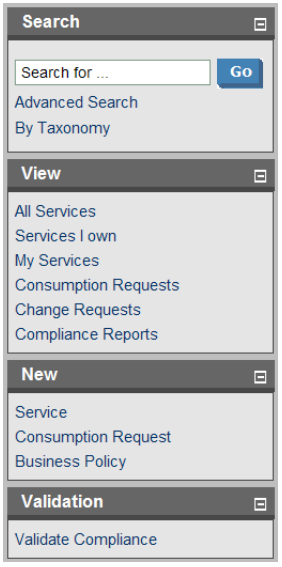
The **Policies** tab enables you to validate your business services against company policy and to manage those polices. The **Polices** tab is described in Features of the Policies Tab on page 93.

The **Tools** tab gives access to Information Management offering a generic low level view of the content of SOA Systinet and access to administration and governance tools. The **Tools** tab is described in Features of the Tools Tab on page 157.

Menus

On the left of each page is a section containing a menu of links and a search box.

Figure 4. Menu



The search feature is described in Full Text Search on page 29.

The menu is context specific for each component and each menu is described in:

- Dashboard Menu on page 40
- Services Menu on page 52
- Policies Menu on page 95
- Tools Menu on page 158

Account Status

At the top-right of each page is a section allowing you to sign-in, manage your account and change your perspective in SOA Systinet.

Figure 5. Account Status before Sign-In

Click **Sign In** and enter the credentials provided by your administrator. If permitted by the administrator you can also create a new account from the sign-in page as described in Creating an Account on page 23.

Figure 6. Account Status after Sign-In

My Account. Manage your account as described in Managing Your Account on page 27.

Sign Out. Sign out of SOA Systinet and become a guest user again.

Change. Move the cursor over **change** and select the perspective to alter your view of SOA Systinet.

3 Creating an Account

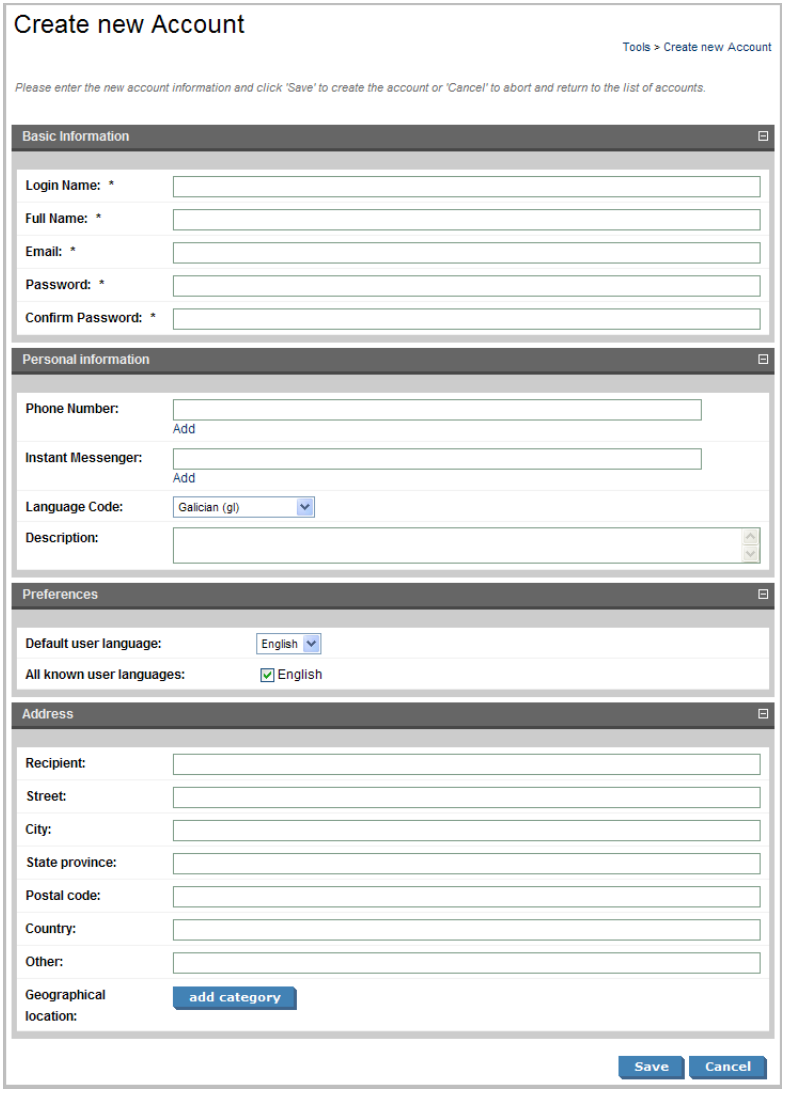
SOA Systinet provides account management features, however, if LDAP is used then the LDAP account management functions should be used instead.

To create an account:

1 Do one of the following:

- As the administrator, in **Tools > User Accounts** click **New Account**
- Alternatively, you may be permitted to register as a new user from **Sign In**. Click **Sign In** and then **register as a new user**.

The **Create New Account** dialog appears:



2 Complete the account details with the following parameters:

Table 1. Basic Information

Parameter	Definition
Login Name	The user id used to sign in
Full Name	The name of the user
Email	The email address for notifications
Password	The password used to sign in
Confirm Password	The password used to sign in

Table 2. Personal Information

Parameter	Definition
Phone Number	A contact telephone number – use **Add** to create multiple entries
Instant Messenger	A messenger id – use **Add** to create multiple entries
Language Code	The language spoken by the new user
Description	A description for the new user

Table 3. Preferences

Parameter	Definition
Default User Language	Select a language from the drop-down list
All known user languages	Check the boxes to select spoken languages
Platform Administrator	The administrator can check this box if the new user has administrator privileges (this box is not visible for new registrations)

The address section allows you to input a mailing address for the user with **Geographical Location** selection.

3 Click **Save** to create the new user.

4 Managing Your Account

Your accounts details are available to amend.

To change your account details:

1 Click **My Account** to display your account information.

2 You can change your general account details and your password.

To change your password:

1 Click **Change Password**.

2 Enter your old and new passwords.

3 Click **Save** to confirm the change.

To edit your account details:

1 Click **Edit**.

2 Change the parameters described in Creating an Account on page 23 with the exception of password.

3 Click **Save** to confirm the changes.

5 Service Discovery

SOA Systinet provides numerous ways to locate the service or artifact you need:

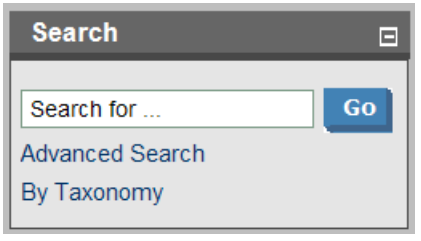
- Full text search is available in the menu on every page and is described in Full Text Search on page 29.
- Browsing by taxonomy is accessible from the search menu and is described in Taxonomy Browsing on page 32.
- The **Services** tab provides list views that enable you to browse and filter services by column heading, as described in List Views on page 55.
- The **Tools** tab provides browse artifact pages with more sophisticated filtering. Artifacts in a browse view can be filtered by column heading or by taxonomic categories assigned to them during artifact creation. Browse views are described in Browse Artifact Pages on page 167.
- Stored searches can be created and used to provide custom views of artifacts. This feature is described in full in Stored Searches on page 205.
- Custom RSS views can be added to the **Dashboard** to provide periodically updated views of specific artifact types. RSS portlets are described in RSS Content Feed Portlets on page 42 and the procedure to create new portlets in Adding a Content Feed on page 45.
- SOA Systinet integrates with UDDI registries giving access to the services indexed in the registry. Setting up registry integration is described in the Registry Setup and Configuration section of the HP SOA Systinet Administration Guide and importing and exporting data with the registry is described in Registry Integration on page 209.
- SOA Systinet integrates with IDEs enabling developers direct access to the SOA Systinet repository. This feature is described in the IDE Integration section of the HP SOA Systinet Developer Guide.

Full Text Search

Full text search is the simplest way to find an item in the repository.

Note: Full text search must be enabled on the database and in the configuration for this feature to function. See the Configuring the Database for Full Text Search section of the HP SOA Systinet Installation Guide and the SOA Systinet Configuration Options section of the HP SOA Systinet Administration Guide.

The search input is located at the top of the menu on every page in SOA Systinet:



Advanced Search enables you to perform a search using filters as described in Filtering Full Text Search Results on page 31.

By Taxonomy enables you to browse the repository by taxonomic categories as described in Taxonomy Browsing on page 32.

To perform a full text search of data in SOA Systinet repository:

- Type your full text search query in the input field, and then click **Go**.

Multiple search terms can be separated with a space to search for repository artifacts containing all the specified terms.

To search for a term including a space, enclose the search term in quotation marks (").

SOA Systinet allows the following wildcards:

- _ can be used to represent any character.
- % or * can be used to represent any text string.

For example, the search string: `C_st% service` finds both Customer Service and Cost Pricing Service if they exist in the repository.

The results of your search appear as a listing that can be further reduced using filters as described in Filtering Full Text Search Results on page 31.

Note: The default functionality of full text search adds a `%` to the end of any input search string that does not contain wildcards. For example, searching for `acc` finds all services that begin with acc. The addition of the % can be disabled as described in the Disabling the Addition of % to Search Terms section of the HP SOA Systinet Installation Guide.

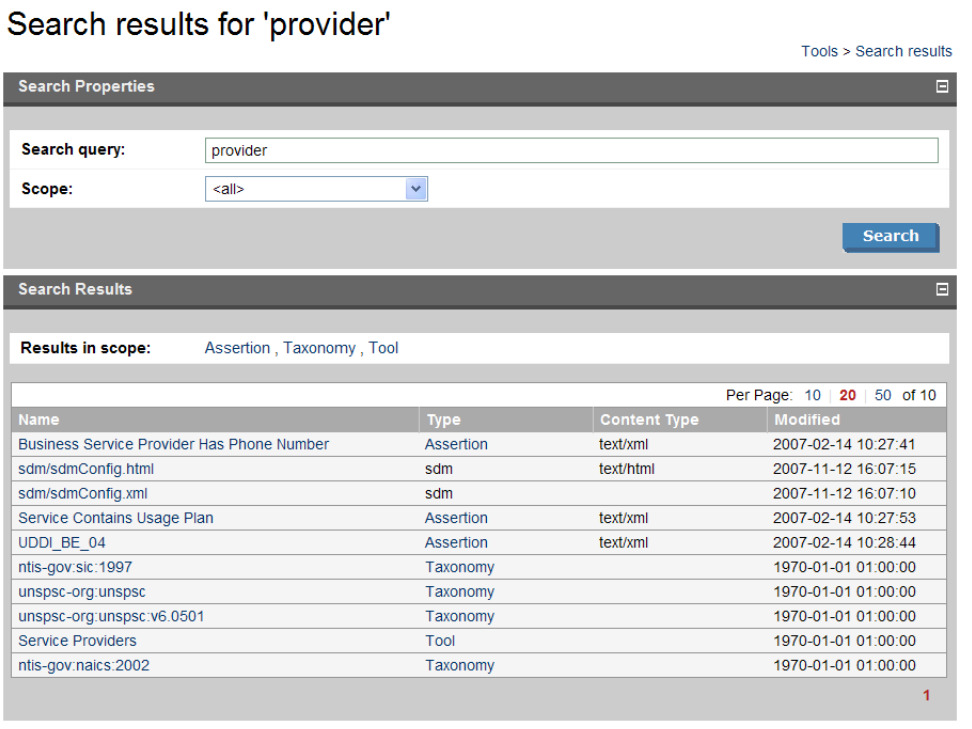
Warning: An exception can occur in the event of a wildcard resulting in excessive search terms. If this occurs then resolve the problem with one of the following methods:

- Remove unnecessary wildcards (%,*,_).
- Prevent the implicit appending of a % by enclosing your search terms with quotes.
- Remove unnecessary words from the expression.

Filtering Full Text Search Results

The results of a full text search can be reduced by using filters. This filter functionality can also be directly accessed using the **Advanced Search** link in the **Search** section of the menu.

Figure 7. Search Results Page



Scope enables you to filter your search by selecting one of the available artifact types. The search is then limited to this artifact type.

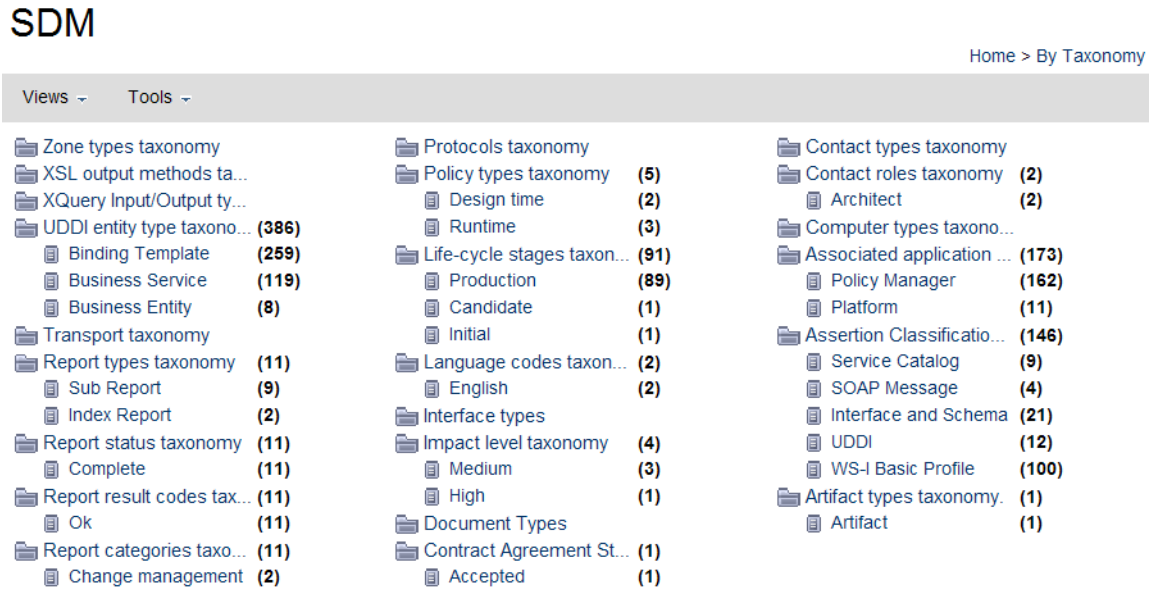
Alternatively, click one of the artifact types next to **Results in scope** in the **Search Results** section.

Taxonomy Browsing

SOA Systinet enables you to search the repository based on taxonomic categories.

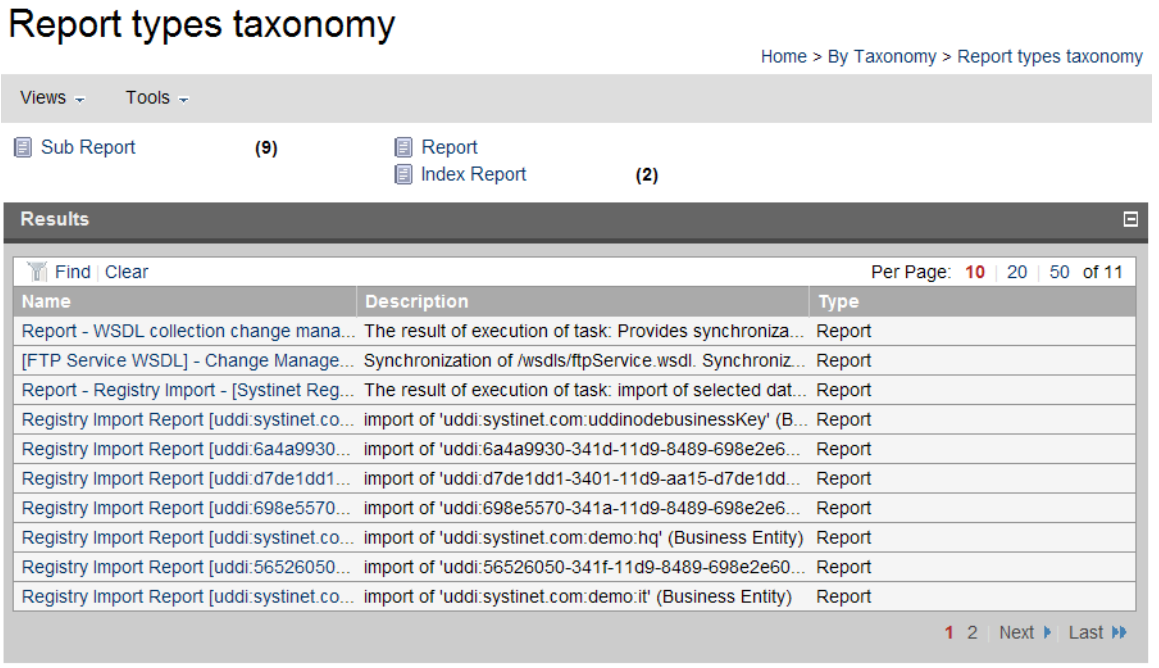
To browse by taxonomies:

1 In the **Search** section of the menu on any page, click **By Taxonomy**. The **SDM** page appears displaying a list of taxonomies and categories from the SOA Definition Model, and the number of artifacts in each taxonomy and category.



The number of items displayed next to each category in the list is approximate and for performance reasons is evaluated ignoring the ACLs. The number represents the cumulative number of items in all subcategories of the current category. The table displayed under the list of subcategories contains only items categorized by the current category (and does not contain items categorized by its subcategories).

2 Select a taxonomic category to view a list of artifacts classified by that category, or a taxonomy to view a list of all artifacts classified by those taxonomic categories and the available categories in that taxonomy.



These pages also contain context menu options enabling you to change the page display:

The **View** menu contains options:

- **All Taxonomies** displays all taxonomies in the repository.
- A set of options enabling you to select a subset of taxonomies. For example, **UDDI** displays the subset of taxonomies for UDDI registry categorization.
- **Manage Views** enables you to select or edit the taxonomy views displayed in the **Views** menu, and to create a new taxonomy view.

To create a new taxonomy view:

1. In the **Manage Views** page, click **New** to open the **Create View** page.

2 Input a name and description for the taxonomy view.

3 Use **add** and **Remove Selected** to select the taxonomies to display in the view.

4 Set the **Display Properties** to control the format of the view.

5 Click **Save** to create the new taxonomy view and add it to the **Views** menu.

The **Tools>Display Properties** option enables you to change the order of the taxonomies and the number listed in each column.

Part II. Dashboard

This part explains the features and use of the **Dashboard**, which is the initial page that opens when you start SOA Systinet.

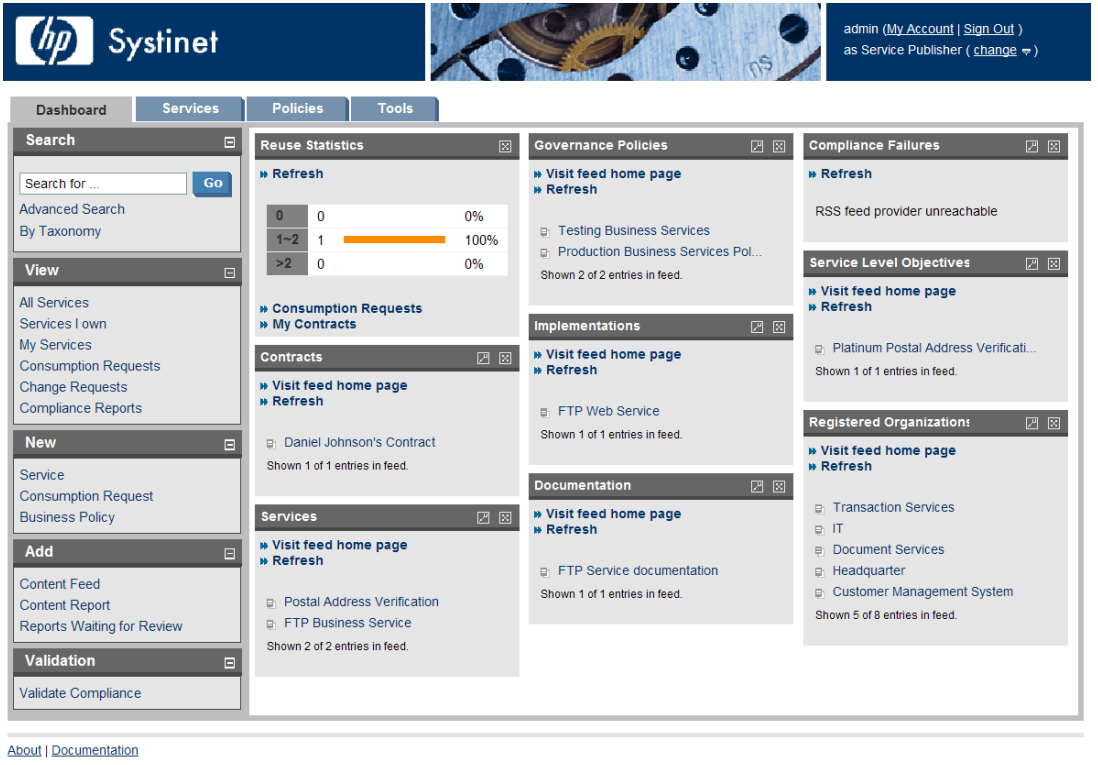
This part contains the following chapters:

- Features of the Dashboard Tab on page 39. The elements of the user interface on the **Dashboard**.
- Adding a Content Feed on page 45. How to add a new RSS feed to the **Dashboard**.
- Adding a Content Report on page 47. How to add new report content to the **Dashboard**.

6 Features of the Dashboard Tab

The **Dashboard** contains a customizable real-time view of your SOA data:

Figure 8. The Dashboard Tab



The Dashboard is split into the menu on the left and a number of **Portlets** in the main section of the page.

Tip: Portlets can be dragged and dropped to customize the look of your dashboard using the mouse. You can also use the keyboard to move portlets.

To move portlets on the Dashboard with the keyboard:

1. Press **F9** to display the movement keypad.
2. Use the **arrow keys** to navigate to the portlet you want to move.
3. Press **Enter** to select the portlet.
4. Use the **arrow keys** to move the portlet into position.
5. Press **Enter** to fix the portlet in place.
6. Press **F9** to exit portlet navigation mode.

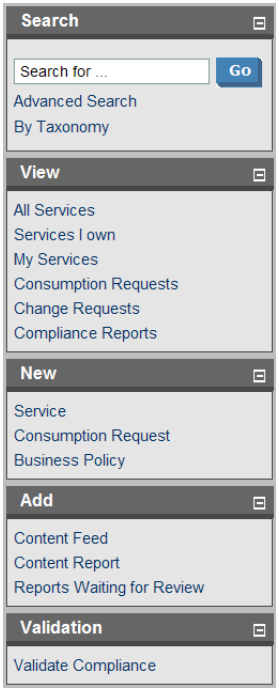
This chapter describes:

- Dashboard Menu on page 40. The items in the dashboard menu.
- RSS Content Feed Portlets on page 42. The RSS content feed portlets on the dashboard.
- Reuse Statistics Portlet on page 43. Displays statistics of service use.

Dashboard Menu

The **Dashboard** menu is split into collapsible sections:

Figure 9. Dashboard Menu



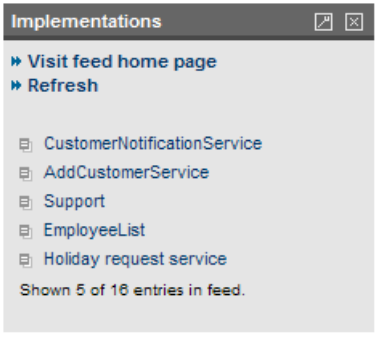
- **Search**. The full text search function described in Full Text Search on page 29.
- **View**. A set of links to **List Views** (see List Views on page 55) showing various aspects of service and contract management.
- **New**. Create new artifacts:
  - **Service**. Create a new business service as described in Creating a New Business Service on page 61.
  - **Consumption Request**. Request the provision of a service as described in Consuming Services on page 87.
  - **Business Policy**. Create a new policy as described in Creating Business Policies on page 121.

- **Add**. Create a new content feed or report to the dashboard, as described in Adding a Content Feed on page 45 and Adding a Content Report on page 47, or restore a portlet to the dashboard.
- **Validation**. Validate the policy compliance of an artifact as described in Validating Documents on page 137.

RSS Content Feed Portlets

The **Dashboard** contains a number of content feeds that use RSS subscription to display up-to-date information from a variety of sources, including the repository:

Figure 10. Implementations RSS Feed Portlet



Visit feed home page takes you to the source of the content in the portlet.

Refresh reloads the content list.

Clicking one of the links in the list takes you to the page showing that item.

The tool icon accesses the feed portlet configuration where you can change the number of list items and the update frequency.

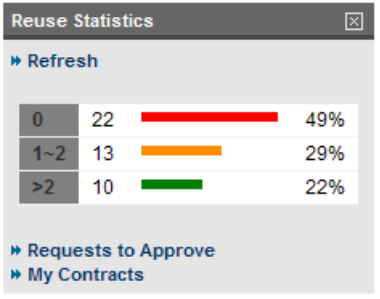
The portlet can be removed from the dashboard by clicking **[X],** and new portlets can be added as described in Adding a Content Feed on page 45.

Closing a portlet in the Dashboard makes it available in the **Add** section of the Dashboard menu.

Reuse Statistics Portlet

Contract Management provides basic statistics of service use in the **Reuse Statistics** portlet on the **Dashboard**.

Figure 11. Reuse Statistics Graph



The statistics show the percentage of services used by a given number of consumers. Basic intervals are less than one, one or two, and more than two.

Refresh reloads the service statistics.

Requests to Approve and **My Contracts** open the relevant **List View** as described in List Views on page 55.

Closing the portlet makes it available in the **Add** section of the Dashboard menu.

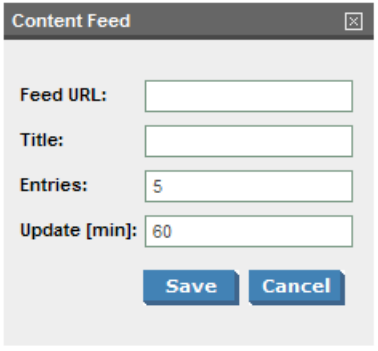
Click one of the graph bars to view the services that fit the selected criteria. For each service the table lists all consumers.

7 Adding a Content Feed

The **Dashboard** can display up-to-date information from external sources and from SOA Systinet.

To add a new RSS feed to the Dashboard:

1 In the **Add** section of the dashboard menu click **Content Feed** to open a new content feed in the **Dashboard**:



2 Complete the form with parameters:

Parameter	Definition
Feed URL	The address of the RSS feed **Note:** To add a feed for repository content use the url from the RSS view accessed from the **Common** context menu in **Browse Artifact** and **detail view** pages (see Browse Artifact Pages on page 167 and Artifact Detail Pages on page 170) or the **RSS of Result** view accessed from the **View** context menu for a stored search.

Parameter	Definition
Title	The heading for the new feed portlet
Entries	The number of items to list
Update [min]	The interval between feed updates

3 Click **Save** to access the feed and load the initial content.

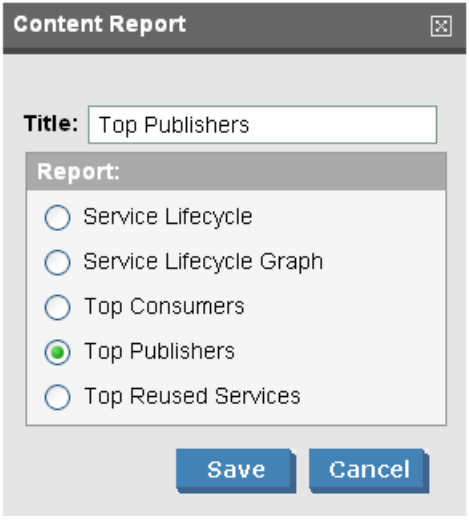
8 Adding a Content Report

The **Dashboard** can display content from specially designed reports.

SOA Systinet contains a standard set of dashboard reports which can be added to using the SOA Systinet Report Editor. See the SOA Systinet Report Editor documentation for more information.

To add a new content report to the Dashboard:

1. In the **Add** section of the dashboard menu click **Content Report** to open a new content report in the **Dashboard**:



2. Input a title for the portlet and select a report from the list.
3. Click **Save** to access the most recent report from the reporting server.

4 **Reload** executes the associated reporting tool to generate a new version of the report.

5 Click the tool icon to change the title or content of the portlet.

Part III. Services

This part explains the features and use of the **Services** tab which is the place to organize and manage your SOA services.

This part contains:

Features of the Services Tab on page 51 describes the user interface elements of the services tab.

Service Pages on page 55 describes the pages for browsing and viewing services and lifecycles in the services tab.

Service Publication on page 61 explains the process of creating services, their implementation, and making them available for use.

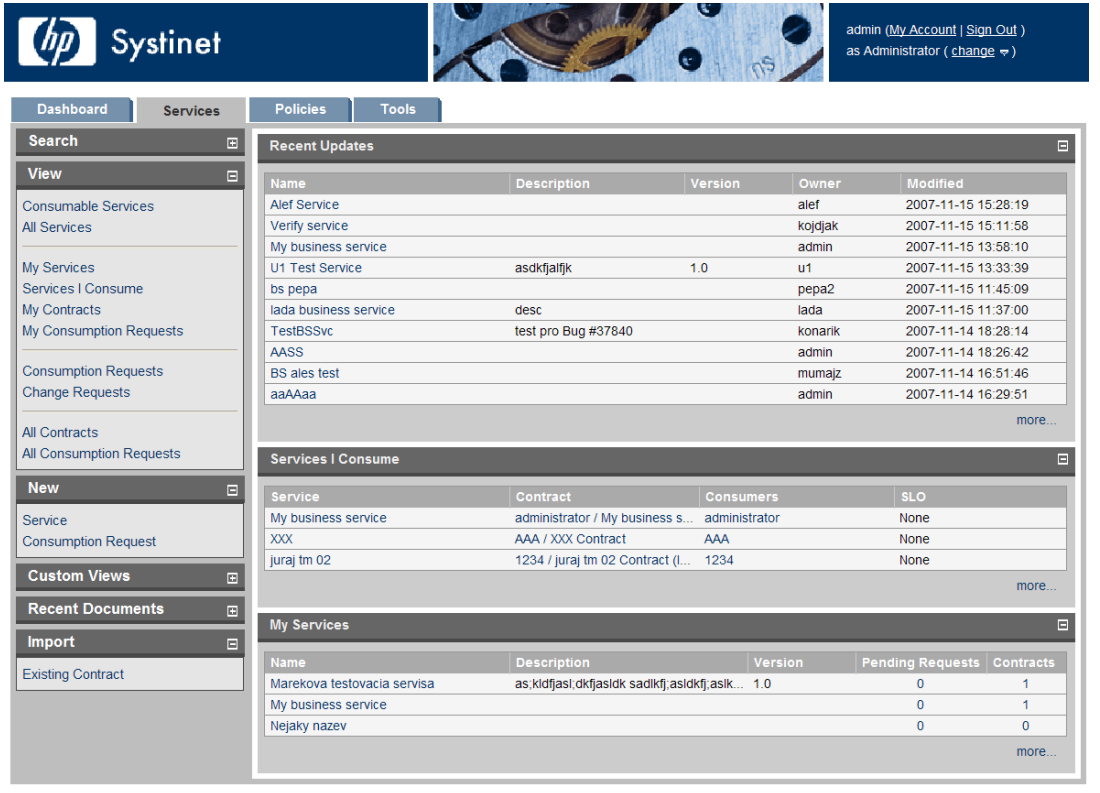
Managing the Service Lifecycle on page 77 explains the process of establishing a lifecycle process for your services.

Managing Contracts on page 87 explains the process of establishing and managing contracts.

9 Features of the Services Tab

The **Services** tab is the central location that shows all information about services and contracts in one place to provide easy access and simple management:

Figure 12. The Services Tab



The **Services** tab is split into the menu on the left and a number of collapsible sections:

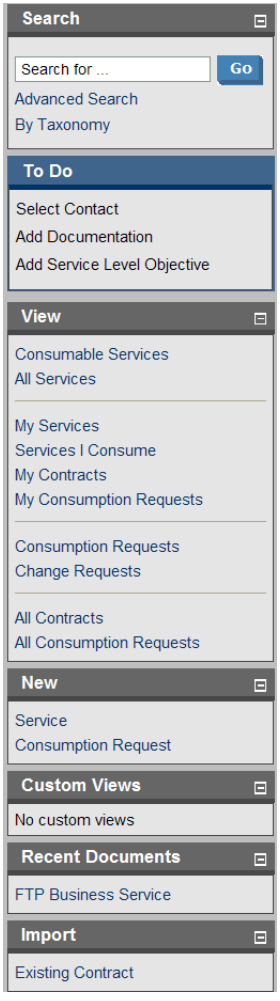
- Services Menu on page 52. A description of the items in the **Services Menu**.
- **My Services**. Shows the services that you provide that are ready for consumption.
- **Services | Consume** displays the services that you use.
- **Recent Updates** shows services that are newly available or modified

Click a service name in these lists to view its details in the **View Service** page or **more...** to open the **List View** for that type of item (see Service View on page 56 or List Views on page 55).

Services Menu

All pages in the **Services** tab include a menu of links:

Figure 13. Services Menu



The **Services** menu is split into sections:

- **Search**. The full text search function described in Full Text Search on page 29.

- **To Do**. When viewing a service, this section shows the recommended steps to make the service ready for consumers as described in Service Publication on page 61.
- **View**. A set of links to **List Views** (see List Views on page 55) showing various aspects of service, contract and lifecycle management.
- **New**. Create new artifacts:
  - **Service**. Create a new business service as described in Creating a New Business Service on page 61.
  - **Consumption Request**. Request the provision of a service as described in Consuming Services on page 87.
- **Custom Views**. Each view is the result of a user specified search as described in Stored Searches on page 205.
- **Recent Documents** displays the last few artifacts you have viewed.
- **Import**. Create a new contract using the details of an existing one as described in Importing an Existing Contract on page 88.

10 Service Pages

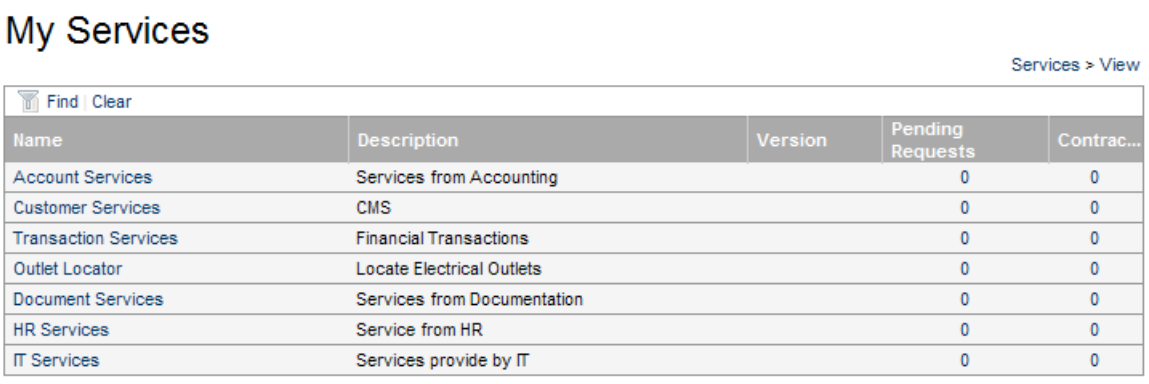
The **Services** tab contains two types of view pages, described in the following sections:

- List Views on page 55 describes the index views of service artifacts.
- Service View on page 56 describes the detailed view of service related artifacts in the Service Catalog.
- Change Requests Page on page 60 describes the lifecycle management page displaying an overview of your approval requests.

List Views

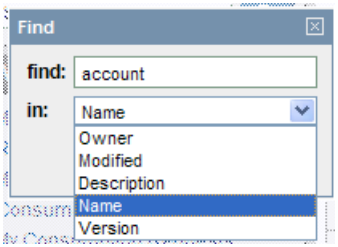
Click one of the links under **View** in the services menu to open a list view of that type of artifact:

Figure 14. My Services List View



These pages have the same functionality as search result pages with the addition of **Find** immediately below the page heading. Click **Find** to open a query window:

Figure 15. List View Filter



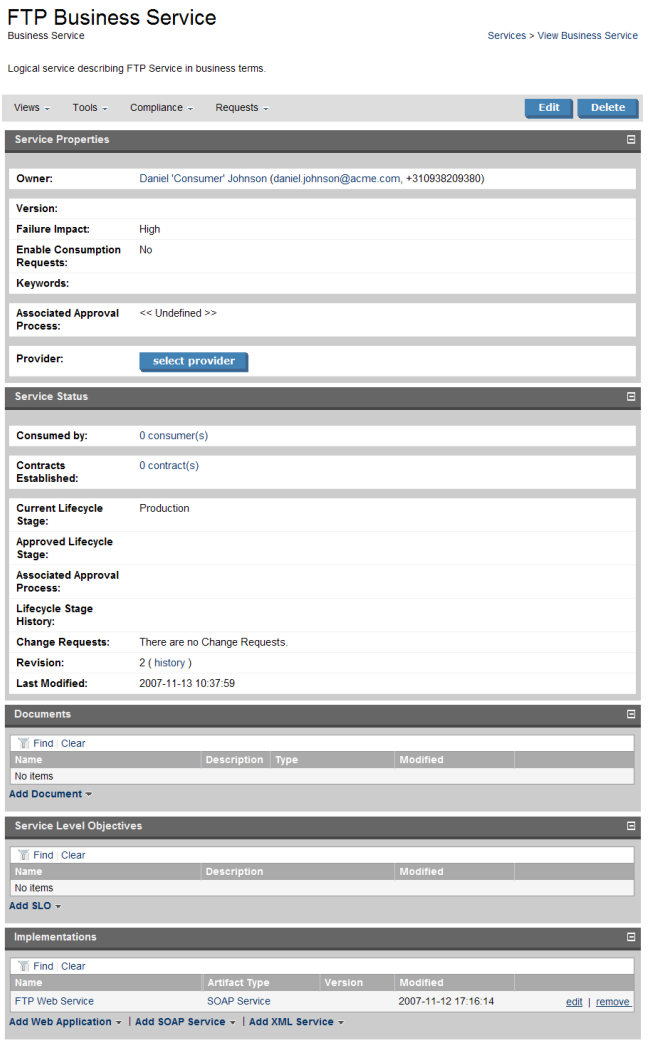
Enter your search parameter, select a column, and then click **Find** to filter the list.

Click **Clear** to remove the filter and restore the list of artifacts.

Service View

Clicking a service name in **Services** opens a service view:

Figure 16. View Service Page



This is the central location for information about the service.

The grey bar contains a set of context action menus containing sets of actions that can alter the view of the service or perform governance actions on the service.

The actions vary depending on the artifact but they include:

- **Views**:
  - **Advanced View** opens the detailed view of the artifact from the **Tools** tab as described in Artifact Detail Pages on page 170.
  - **Navigator View** opens a graphical representation of the artifact and its relationships, as described in Navigator View on page 173.
  - **Revision History** opens the version history of the artifact as described in Revision History on page 175.
  - **Access Rights** opens a view of the access permissions for the artifact.
- **Tools**:
  - **Related Reports** opens a list of the reports related to this artifact as described in Reports on page 203.
  - **Dependency Analysis** and **Impact Analysis** execute the impact management tool on the artifact as described in Impact Tools on page 189.
  - **Change Owner** enables the administrator or owner of the artifact to transfer ownership to a different user, as described in Changing Artifact Ownership on page 180.
- **Compliance**:
  - **Validate Compliance**. Validate the policy compliance of an artifact as described in Validating Documents on page 137.
  - **Compliance Status**. View the results of the last compliance check as described in Report Views on page 107.
  - **Effective Policies**. View the business policies associated with the service.

    - **Reset Compliance Statistics**. Delete all compliance reports associated with the artifact.

- **Related Requests**:
    - **Submit Change Request** starts the procedure described in Submitting a Change Request on page 83.
    - **Submit Consumption Request** starts the procedure described in Consuming Services on page 87.
    - **View Pending Consumption Requests** opens a list view (see List Views on page 55) of consumption requests that require action by the service provider.
    - **View Accepted Consumption Requests** opens a list view (see List Views on page 55) of consumption requests accepted by the service provider.
    - **View Rejected Consumption Requests** opens a list view (see List Views on page 55) of consumption requests rejected by the service provider.

- **Edit** enables you to change the attributes of the service.
- **Delete** removes the service from the repository after confirmation.
- **Submit Change Request** is displayed if the service is associated with a lifecycle approval process and at a stage requiring approval. Click **Submit Change Request** to start the approval process described in Submitting a Change Request on page 83.
- **Approve/Deny** is displayed if the service is associated with a lifecycle approval process and there is an outstanding request for your approval. Click **Approve/Deny** to start the approval process described in Handling Change Requests on page 84.

The **To Do** section of the menu shows the recommended set of steps to make the service complete with appropriate accompanying documentation, an implementation and any service level objectives. Completing these steps is described in Service Publication on page 61.

Service Properties displays key information about the service, the service owner, version, and contact, and also the lifecycle stage with any associated approval process.

Service Status displays contract information, lifecycle approval status and registry integration status (see Registry Synchronization on page 212).

SOA Manager includes a link to view the SOA Manager view of this service if it is also stored there.

The **Documents**, **Service Level Objectives**, and **Implementations** sections enable you to manage the artifacts associated with the service and add new relationships as described in Service Publication on page 61.

Change Requests Page

The **Change Requests** page is part of lifecycle management displaying an overview of all approval requests you are involved with (see Managing the Service Lifecycle on page 77).

Access the page from the **Services** or **Tools** menu with the **Change Requests** link.

The page is split into the following sections displaying different stages of service and lifecycle approvals.

- **Change Requests to Approve** displays a list of change requests that require your attention. These requests are associated with services at a lifecycle stage that you are the approver for. Click a request to review it and approve or reject, as described in Handling Change Requests on page 84.
- **Change Requests | Processed** displays the list of change requests that you either approved or denied.
- **My Pending Change Requests** displays your outstanding change requests that require review by the relevant approvers.
- **Change Requests | Submitted** displays a list of all change requests that you submitted.
- **My Services with a Change Request Needed** displays services you own that require approval because the revision is different to the last approved revision.
- **Services with a Change Request Needed** displays services that require your approval because the revision number is different to the last approved revision.
- **Services with Approvals** displays a list of approved services with links to the last approved revision.

11 Service Publication

Service publication is one of the most important aspects of SOA Systinet.

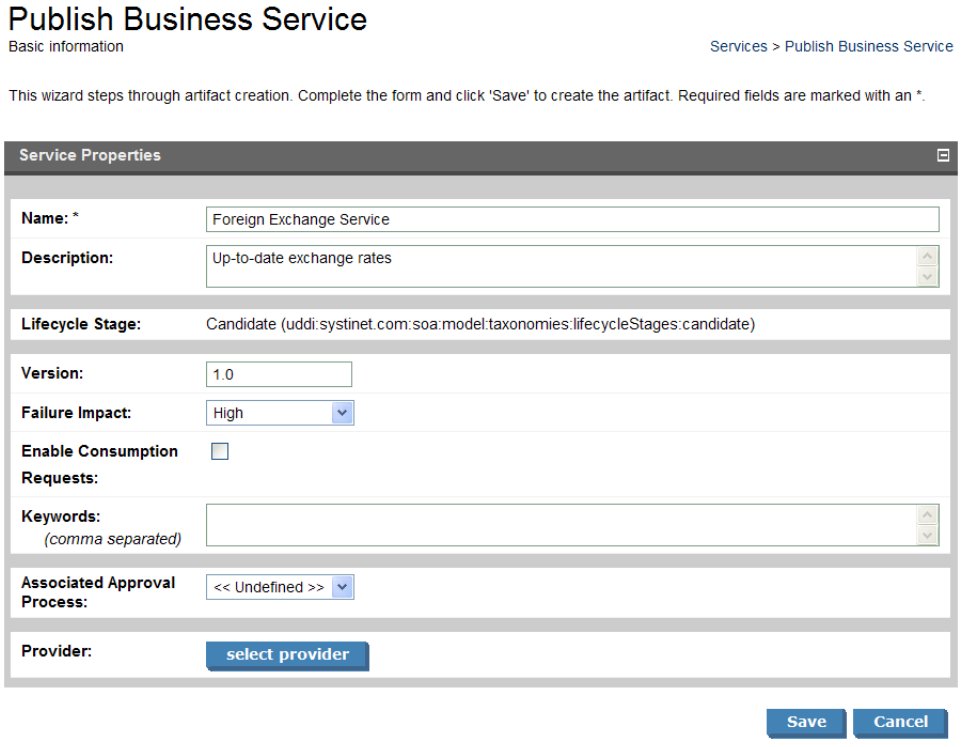
SOA Systinet makes service publication simple by breaking the process down into a set of basic procedures:

Creating a New Business Service

You can publish new business services from the **Services** tab.

To publish a new service:

1 In the **New** section of the services tab menu click **Service** to open the **Publish Business Service** page:



2 Complete the form with parameters:

Parameter	Definition
Name	The name of the new business service
Description	A description of the new service

Parameter	Definition
Lifecycle Stage	Select a status from the drop-down list If a default lifecycle stage is set, as described in Configuring the Default Lifecycle on page 85, then the default status is displayed and cannot be changed.
Version	The version number of the service
Failure Impact	Select an impact from the drop-down list
Enable Consumption Requests	Check this box to make the service available to consumers (not visible in the **General** perspective)
Keywords	Optionally, add search terms for the service
Associated Approval Process	Select the lifecycle approval process to associate with the new service from the drop-down list
Provider	Optionally, click **select provider** to select a provider from the list of available users as described in Setting a Provider on page 63.

3 Click **Save** to create the business service artifact.

Setting a Provider

A business service is usually associated with a particular individual.

To make a particular user responsible for a service:

1 In the service view expand the **Provider** section by clicking **select provider**.

2 Use **Find** to search for the required provider and click **select** to set the provider from the list.

Adding Service Documentation

To add documentation to a service:

In the **service view** place the cursor over **add document** to view the following options:

- **From Local File** – to upload a document from your local filesystem.
- **From Remote File** – to upload a document from a remote location.
- **Link to a Remote File** – to create a link to a document on a remote location.
- **From Catalog** – to select a document from the collection in the repository.

To upload a document from your local filesystem:

1 Click **From Local File** to open the **Local File** dialog.

2 Complete the dialog with parameters:

Parameter	Definition
File	Use **Browse** to locate the file on your local filesystem
Type	Select a document type from the drop-down list
Name	Input a name for the documentation artifact
Description	Input a description of the documentation artifact

3 Click **Save** to import the document, create a new documentation artifact and the relationships between the service and the documentation artifacts.

To upload a document from a remote location:

1 Click **From Remote File** to open the **Remote File** dialog.

2 Complete the dialog with parameters:

Parameter	Definition
URL	Input the url of the remote document
Type	Select a document type from the drop-down list
Name	Input a name for the documentation artifact

Parameter	Definition
Description	Input a description of the documentation artifact

3 Click **Save** to import the document, create a new documentation artifact and the relationships between the service and the documentation artifacts.

To link to a document on a remote location:

1 Click **Link to a Remote File** to open the **Link to a Remote File** dialog.

2 Complete the dialog with parameters:

Parameter	Definition
URL	Input the url of the remote document
Type	Select a document type from the drop-down list
Name	Input a name for the documentation artifact
Description	Input a description of the documentation artifact

3 Click **Save** to create a new documentation artifact with a link to the remote document and the relationships between the service and the documentation artifacts.

To select from the list of the documentation artifacts in the repository:

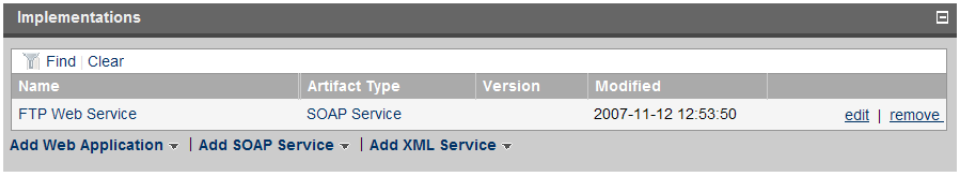
1 Click **From Catalog** to open the **Browse Catalog** dialog.

2 Use **Find** to search for the required documentation artifact and click **add** to select the document from the list.

Implementing a Service

Business services are implemented in the **Services** tab. The **Service View** (see Service View on page 56) contains an **Implementation** section with the following options:

Figure 17. The Implementations Section



- **Add Web Application** as described in Adding a Web Application on page 69.
- **Add SOAP service** as described in Adding a SOAP Service on page 66.
- **Add XML service** as described in Adding an XML Service on page 68.

XML services and web applications also require the creation of an endpoint to make them functioning implementations. See Adding an Endpoint on page 70.

XML services can also be defined with an XML schema document, as described in Adding an XML Service Definition on page 71.

Adding a SOAP Service

A common implementation of a business service is a SOAP service.

To add a SOAP service to a business service:

1 In the **Implementation** section of the service view place the cursor over **Add SOAP service** to view the following options:

- **From Local File**. Select a SOAP service from a local filesystem.
- **From Remote File**. Select a SOAP service from a remote location.
- **From Catalog**. Select a SOAP service already in the repository.

2 Do one of the following:

- **To select a SOAP service from your local filesystem:**

  1. Click **From Local File** to open the **Local File** dialog.
  2. Use **Browse** to locate the WSDL file on your local filesystem.
  3. Click **Save** to start the publication process for the implementations contained in the WSDL file.
  4. Optionally, edit the web service name and description, and then click **Next**.
  5. Click **Finish** to validate the WSDL, and then create the new WSDL and SOAP service artifacts and create the relationships with the business service.

- **To select a SOAP service from a remote location:**

  1. Click **From Remote File** to open the **Remote File** dialog.
  2. Complete the dialog with parameters:

Parameter	Definition
WSDL File	Input the url of the remote WSDL file
Apply Synchronization Policy	Check the box to apply a synchronization policy (see Synchronization Policy on page 196 for more details).
Synchronization Policy Type	Select **Automatic** or **Manual**

  3. Click **Upload** to start the publication process for the implementations contained in the WSDL file.
  4. Optionally, edit the web service name and description, and then click **Next**.
  5. Click **Finish** to create the new WSDL and SOAP service artifacts and create the relationships with the business service.

- **To select a SOAP service from the repository:**

  1. Click **From Catalog** to view a list of SOAP services in the repository.
  2. Click **add** next to the SOAP service you require to associate it with the business service.

Adding an XML Service

You can also associate a business service with an XML service artifact.

To add an XML service to a business service:

1. In the **Implementations** section of the service view, place the cursor over **Add XML Service** to view the following options:
   - **New XML Service**. Create a new XML service.
   - **From Catalog**. Select an XML service already in the repository
2. Do one of the following:
   - **To create a new XML service:**
     1. Click **New XML Service** to open the **Create XML Service** dialog.
     2. Complete the dialog with parameters:

Parameter	Definition
Name	The name of the new XML Service artifact
Description	A description of the XML Service artifact
Version	A version number for the XML Service artifact

     3. Click **Save** to create the new XML service artifact and the relationships with the business service.

Note: This process only creates an XML service artifact. You must add an endpoint to the artifact in the service view of the XML service to make it a functioning implementation, as described in Adding an Endpoint on page 70. An XML schema document can also be added to an XML service as described in Adding an XML Service Definition on page 71.

- **To select a XML service from the repository:**

  1. Click **From Catalog** to view a list of XML services in the repository.
  2. Click **add** next to the XML service you require to associate it with the business service.

Adding a Web Application

You can associate the business service with a web application artifact.

To add a web application to a service:

1. In the **Implementations** section of the service view, place the cursor over the **Add Web Application** to view the following options:
   - **New Web Application**. Create a new web application.
   - **From Catalog**. Select a web application already in the repository
2. Do one of the following:
   - **To create a new web application:**
     1. Click **New Web Application** to open the **Create Web Application** dialog.
     2. Complete the dialog with parameters:

Parameter	Definition
Name	The name of the new web application artifact
Description	A description of the web application artifact
Version	A version number for the web application artifact

3 Click **Save** to create the new web application and the relationships with the business service.

Note: This process only creates an web application artifact. You must add an endpoint to the artifact in the service view of the web application to make it a functioning implementation, as described in Adding an Endpoint on page 70.

- **To select a web application from the repository:**

1 Click **From Catalog** to view a list of web applications in the repository.

2 Click **add** next to the web application you require to associate it with the business service.

Adding an Endpoint

XML service and web application implementations require an endpoint artifact to locate the actual implementation of the service.

To add an endpoint to an XML service or a web application:

1 In the **Endpoints** section of the service view of an XML service or web application, click **Add Endpoint** to open the **Publish Endpoint** page.

2 Complete the dialog with parameters:

Parameter	Definition
Name	The name of the new endpoint

Parameter	Definition
Description	A description of the endpoint
Endpoint Address	The url for the actual implementation of the service

3 Click **Save** to create the new endpoint and the relationships with the XML service or web application.

Adding an XML Service Definition

XML service implementations can be defined by an XML schema document.

To add a definition to an XML service:

1 In the **Definitions** section of the service view of an XML service, place the cursor over **Add Definition** to view the following options:

- **From Local File** – to upload an XSD file from your local filesystem.
- **From Remote File** – to upload an XSD file from a remote location.
- **From Catalog** – to select an XML schema artifact from the collection in the repository.

2 Do one of the following:

- **To upload an XSD file from your local filesystem:**

  1 Click **From Local File** to open the **Local File** dialog.

  2 Use **Browse** to locate the XSD file.

  3 Click **Save** to import the XSD, create a new XML schema artifact and the relationships between the service and the artifact.

- **To upload an XSD file from a remote location:**

  1 Click **From Remote File** to open the **Remote File** dialog.

2 Input the URL for the remote XSD file.

3 Click **Save** to import the XSD, create a new XML schema artifact and the relationships between the service and the artifact.

- **To select an XML schema from the repository:**

  1 Click **From Catalog** to view a list of XML schema artifacts in the repository.

  2 Click **add** next to the XML schema you require to associate it with the XML service.

Adding an SLO

Most services are offered with a set of terms describing the levels of performance the service provider expects to meet.

To add a service level objective to a service:

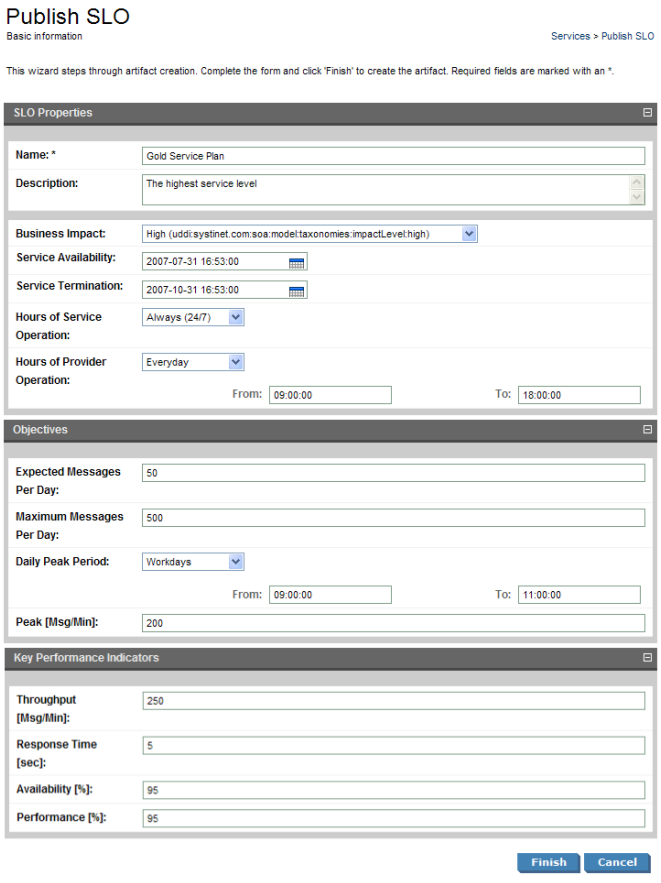
1 In the **Service Level Objectives** section of the service view place the cursor over **Add SLO** to view the following options:

- **New SLO**. Create a new service level objective.
- **From Catalog**. Select a service level objective already in the repository.

2 Do one of the following:

- **To create a new service level objective:**

  1 Click **New SLO** to open the **Publish SLO** dialog:



2 Input the following parameters which are split into sections:

SLO Properties:

Parameter	**Definition**
Name	The name of the new SLO artifact
Description	A description of the SLO artifact
Business Impact	Select an impact from the list

Parameter	Definition
Service Availability	Expected time of service delivery
Service Termination	Expected time of service termination
Hours of Service Operation	Select an option from the list, and then input start and end times if required
Hours of Provider Operation	

Objectives:

Parameter	Definition
Expected Messages Per Day	Number of messages
Maximum Messages Per Day	
Daily Peak Period	Select an option from the list, and then input start and end times if required
Peak [Msg/Min]	Expected messaging capacity

Key Performance Indicators:

Parameter	Definition
Throughput [Msg/Min]	The number of calls to the service per minute
Response Time [sec]	The time for the service to respond
Availability [%]	The availability of the service in its operating hours
Performance [%]	A measure of the performance of the service

3 Click **Save** to create the service level objective and the relationships to the business service.

- **To select a service level objective from the repository:**

1 Click **From Catalog** to view a list of service level objectives in the repository.

2 Click **add** next to the service level objective you require to associate it with the business service.

Making the Service Available

When the service is ready you must make it available for consumption.

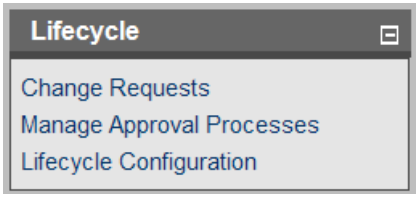
To make the service available to consumers:

1. Switch to the **Service Publisher** perspective.
2. In the service view, click **Edit** to open the **Edit Service** page.
3. Select **Enable Consumption Requests**.
4. Click **Save** to make the service available for consumption.

12 Managing the Service Lifecycle

SOA Systinet provides functionality that enables you to manage your service development lifecycle by creating approval definition processes. Each service can then be associated with a different approval process.

In the **Tools** menu, the **Lifecycle** section gives access to these features:



- **Change Requests Summary** opens the **Change Requests** page, giving an overview of your approvals, as described in Change Requests Page on page 60. This option is also available in the **View** sections of the **Dashboard** and **Services** menus.
- **Manage Approval Process Definitions** opens the browse **Approval Process Definitions** page. From this page you can review, edit, or delete existing processes or create new ones.
- **Lifecycle Configuration** enables you to set the default approval process and lifecycle stage used during business service creation (administrator perspective only).

Note: The lifecycle process described in this chapter is based on the standard lifecycle taxonomy provided with SOA Systinet. The lifecycle taxonomy can be modified using the HP SOA Systinet Taxonomy Editor.

Lifecycle management is enabled by a set of procedures accessed from **Services** and **Tools** pages:

- Creating an Approval Process Definition on page 78

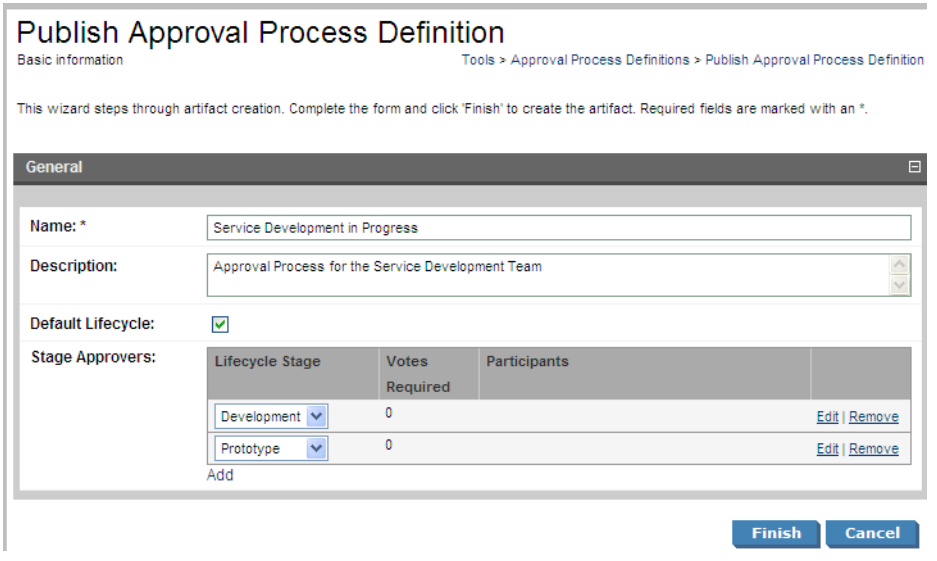
- Submitting a Change Request on page 83
- Handling Change Requests on page 84
- Configuring the Default Lifecycle on page 85

Creating an Approval Process Definition

To manage your service lifecycle, you must first create an approval process definition. The definition sets the users and groups who can approve a lifecycle stage change at one or more lifecycle stagees.

To create an approval process definition:

1 In the browse approval process definitions page, click **New** to open the **Publish Approval Process Definition** page:

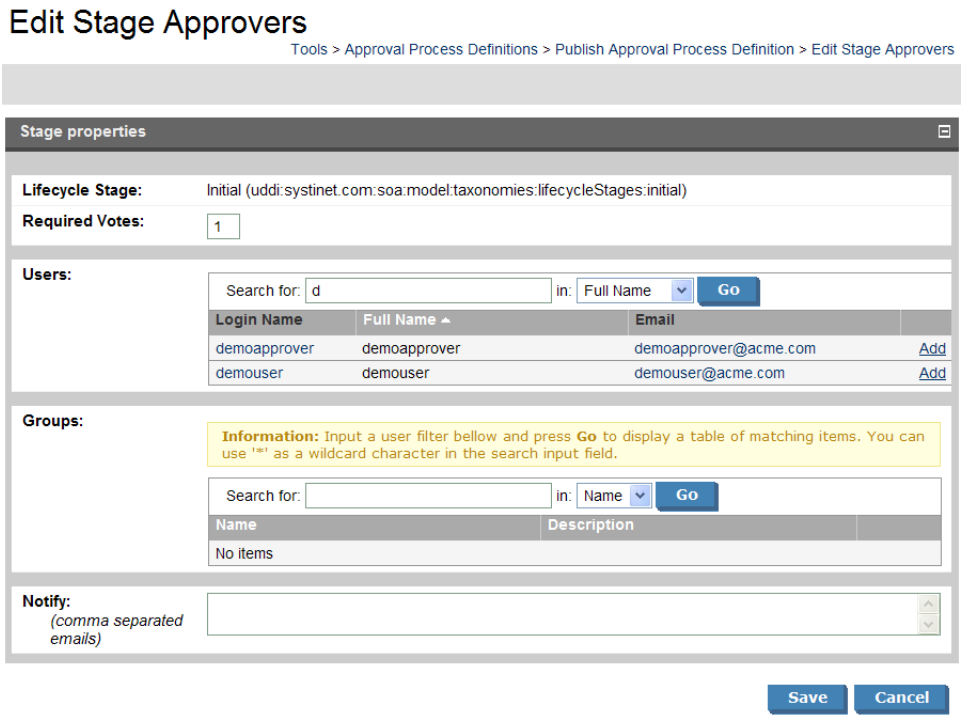


2 Input a name and description for the new process definition.

3 Select **Default Lifecycle** if this lifecycle is the default lifecycle used during service creation, as described in Creating a New Business Service on page 61.

4 In the **Stage Approvers** table, select the lifecycle stage that requires approval. To select additional lifecycle stages, click **Add**.

5 Click **Edit** for a lifecycle stage to open the **Edit Stage Approvers** page:



6 Select a combination of user, group and individual group member votes. The total votes required are calculated automatically from the mandatory user votes and per-group required votes. The stage is approved when the following conditions are met:

- Vote count total votes required.
- All mandatory users have approved and all groups have cast at least their specified amount of positive votes.

An example of group vote selection is given in Selecting Group Votes on page 80.

7 Input a user or group search term and click **Go** to view a list of matching users or groups.

8 Click **Add** to select the user or group to approve this lifecycle stage.

9 If you want additional approval notifications to be sent, type a set of comma-separated e-mail addresses into the **Notify** field.

To send notices to a distribution list email address, add that address here.

10 Click **Save** to set the approvers and return to the approval process page.

11 Repeat Step 4 to Step 10 for as many lifecycle stages as required to define your process.

12 Click **Save** to save the new approval process definition.

Selecting Group Votes

You can specify which user votes are required and how many votes of a group's members are required. The total number of required votes adds up automatically in the **Required Votes** field.

For example, consider a scenario where there is an architect, "architect1," who analyzed a feature. Then someone designed a solution. To approve the design stage of that solution, you require a review from the original architect (architect1), another architect from the "architects" group, the team leader (manager1) and someone from the "accessibility" group. You want notices sent to the distribution group email addresses, `architects@company.com` and `accessibility@company.com`. In summary, you have the following users and groups in this scenario:

- Users 'architect1', 'architect2', other members of the "architects" group
- User "manager1," the team leader
- Group "accessibility," consisting of users who review design ergonomy and accessibility

You need a total of 4 votes to approve the design stage, divided up between the users and groups as follows:

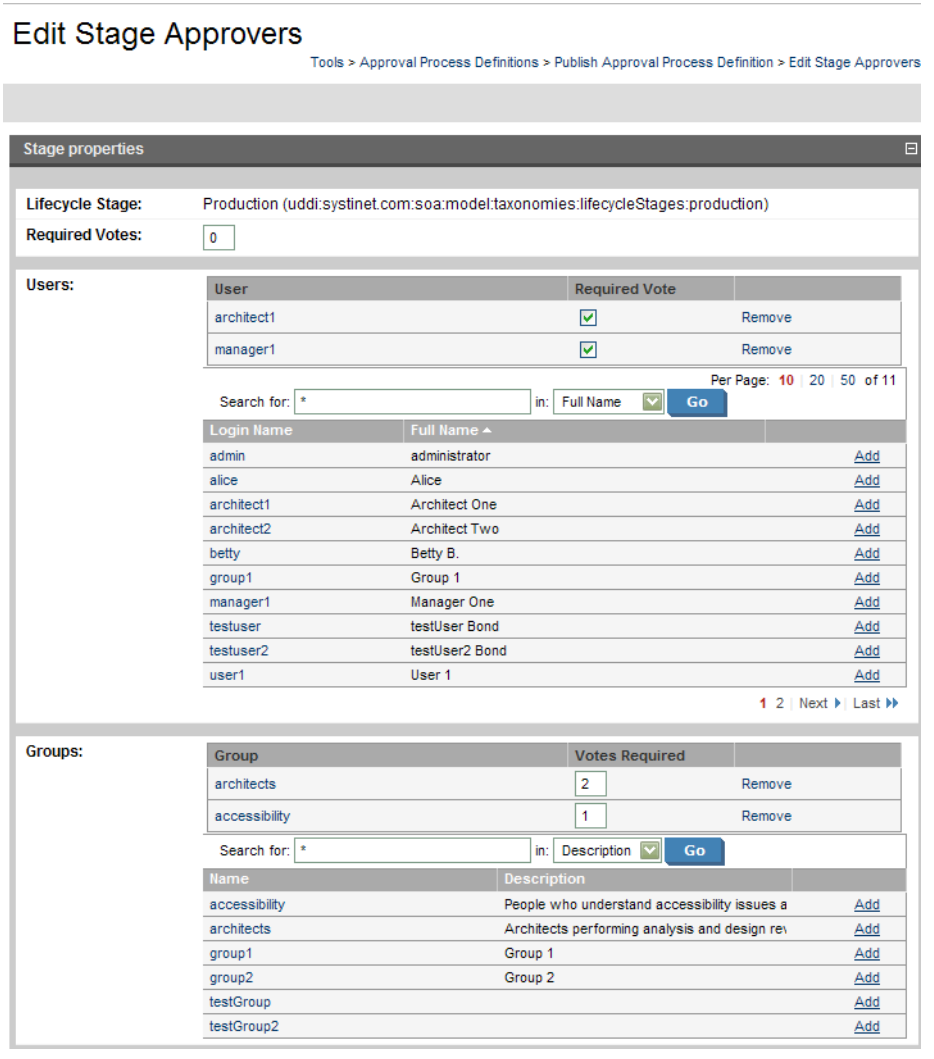
- Users

    - architect1, required vote
    - manager1, required vote

- Groups
    - architects, 2 required votes (including architect1)
    - accessibility, 1 required vote

To specify these votes, you fill in the **Edit Stage Approvers** page as shown in Figure 18.

Figure 18. Setting Group and User Approvers



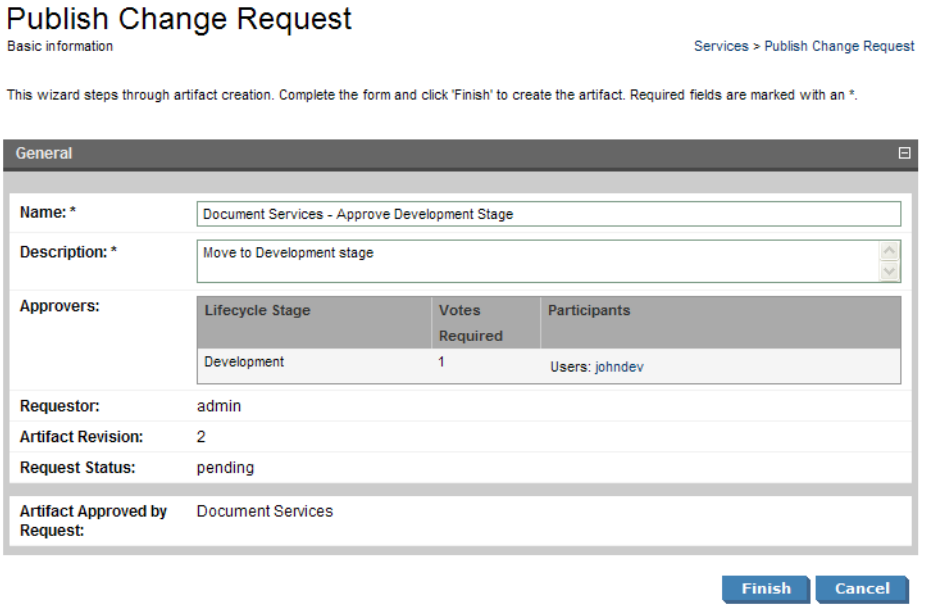
To send email notifications to the architect and accessibility group distribution lists, you type `architects@company.com` and `accessibility@company.com` in the **Notify** field.

Submitting a Change Request

When a service with an associated approval process definition requires amendment you must request approval.

To request approval:

1. Edit the service, as described in Editing an Artifact on page 178, and amend the service as required.
2. In the service view of a service at a lifecycle stage requiring approval, click **Submit Change Request** to open the **Publish Approval Request** page:



3. Amend the name of the request and input a description.
4. Click **Save** to send the approval request to the users and groups listed in the **Approvers** section for the current lifecycle stage. Notifications are also sent to the specified e-mail addresses added in the approval definition creation.

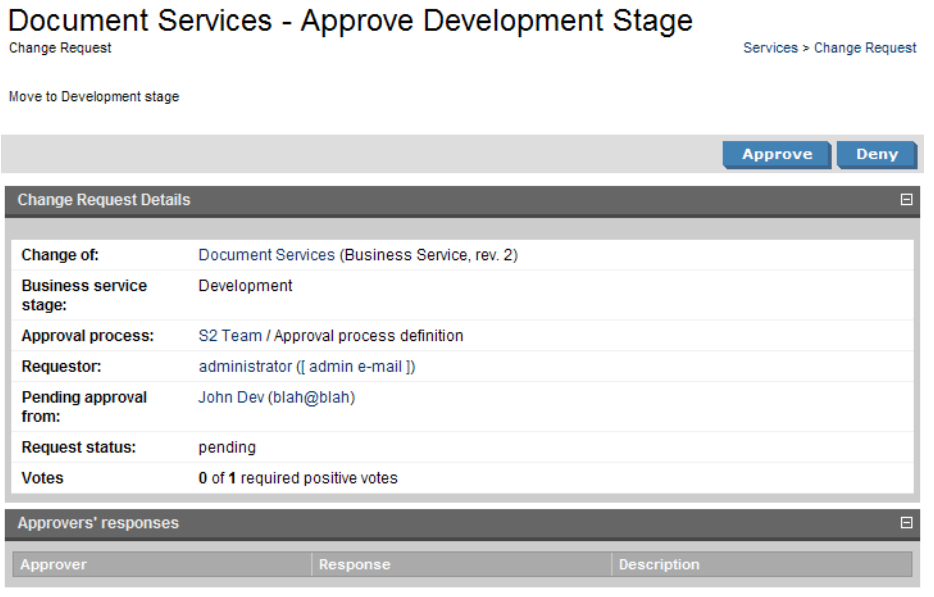
Note: A service with a pending approval request cannot be edited.

Handling Change Requests

A request requiring your approval appears in the **Change Requests to Approve** section of the **Approval Requests** page.

To approve or deny a change request:

1 Click the name of the request in the **Requests to Approve** section to open the **Change Request** page:



2 Review the request and any responses made by other approvers.

3 Click **Approve** or **Deny** based on your decision and input your comments.

4 Click **Save** to complete the approval process.

E-mails are sent to the requester, and the other specified e-mails for that approval stage when the required number of votes for that stage are made.

Configuring the Default Lifecycle

The default lifecycle and lifecycle stage used during business service creation can be configured.

To configure the default lifecycle and stage:

1. In the **Tools** menu **Lifecycle** section, click **Lifecycle Configuration** to open the **Lifecycle Configuration** page.
2. Use the drop-down lists to select the **Default Approval Process** and **Default Lifecycle Stage** used during business service creation, as described in Creating a New Business Service on page 61.
3. Click **Save** to confirm your changes.

Lifecycle Reports

A number of lifecycle reports are provided with SOA Systinet:

- In the **Tools** tab **Report Launcher**, **Services by Lifecycle Stage with Pending Requests** gives details of services with an associated approval process at a lifecycle stage requiring approval and with an outstanding change request.
- In the **Tools** tab **Report Launcher**, **Services in Unapproved Stages** gives details of services with an associated approval process at a lifecycle stage requiring approval but with no change requests.
- In the **Tools** tab **Report Launcher**, **Service Lifecycle Statistics** gives a summary of all services regardless of whether there is an approval process associated with them.

13 Managing Contracts

SOA Systinet provides contract management to enable providers and consumers to establish contracts.

Contract management is enabled by a set of procedures accessed from the **Services** tab:

Consuming Services on page 87 describes how consumers request the provision of a service.

Processing Consumption Requests on page 88 describes how providers manage these consumption requests.

Importing an Existing Contract on page 88 describes how a consumer can use an existing contract instead of the request process.

Revoking an Active Contract on page 89 describes how a provider can cancel an active contract.

Consuming Services

To consume a service you must make a request to the provider.

To request the provision of a service:

1 Do one of the following:

- In the **New** section of the services menu click **Submit Consumption Request**.
- Alternatively, in the service view of a service that is available for consumption click **Request Consumption**.

The **New Consumption Request** page appears.

2 If the default service is not the service required, use **Find** to search for the service to consume. Check the radio button to select the service from the list and click **Next**.

3 If the default consumer is not the consumer required, use **Find** to search for the consumer that is requesting the service. Check the radio button to select the consumer from the list and click **Next**.

4 If required, check **select specific SLO** and select one from the list. Click **Next**.

5 Optionally, modify the name and description of your consumption request and click **Next**.

6 Confirm the request details and click **Finish** to place your request.

Processing Consumption Requests

When consumers request provision of a service you must either approve or reject their request.

To process consumption requests:

1 In the **View** section of the services menu click **Consumption Requests** to display the list view of requests that require your attention.

2 Click the request name to open a view of that request.

3 To accept or reject a request, click **Accept** or **Reject** and confirm your decision.

4 SOA Systinet informs the consumer and any stakeholders in the service of the decision. In the case of acceptance the request becomes a contract between the consumer and provider.

Importing an Existing Contract

As there are usually existing contracts between a provider and their consumers which were previously created (and still valid), SOA Systinet allows consumers to import such contracts and avoid the request approval process.

To import an existing contract:

1 In the **Import** section of the services menu click **Existing Contract** to start the **Enter Existing Contract** process.

2 Use **Find** function to search for the service to consume. Check the radio button to select the service from the list and click **Next**.

3 If the default consumer is not the required consumer, use **Find** function to search for the consumer that is requesting the service. Select the consumer from the list, and then click **Next**.

4 If required, select **select specific SLO**, and then select one from the list. Click **Next**.

5 Optionally, modify the name and description of your contract, and then click **Next**.

6 Confirm the details and click **Finish**.

Revoking an Active Contract

A provider may need to cancel an active contract.

To revoke a contract:

1 In the **View** section of the services menu, click **My Contracts** to display the list view of active contracts for services that you provide.

2 Click the contract name to open a view of that contract.

3 Click **Revoke** to cancel the contract, and then confirm.

4 SOA Systinet informs the consumer and any stakeholders in the service of the decision.

Part IV. Policies

This part explains the most common uses of Policy Manager, accessible from the **Policies** tab of SOA Systinet. It includes the following sections:

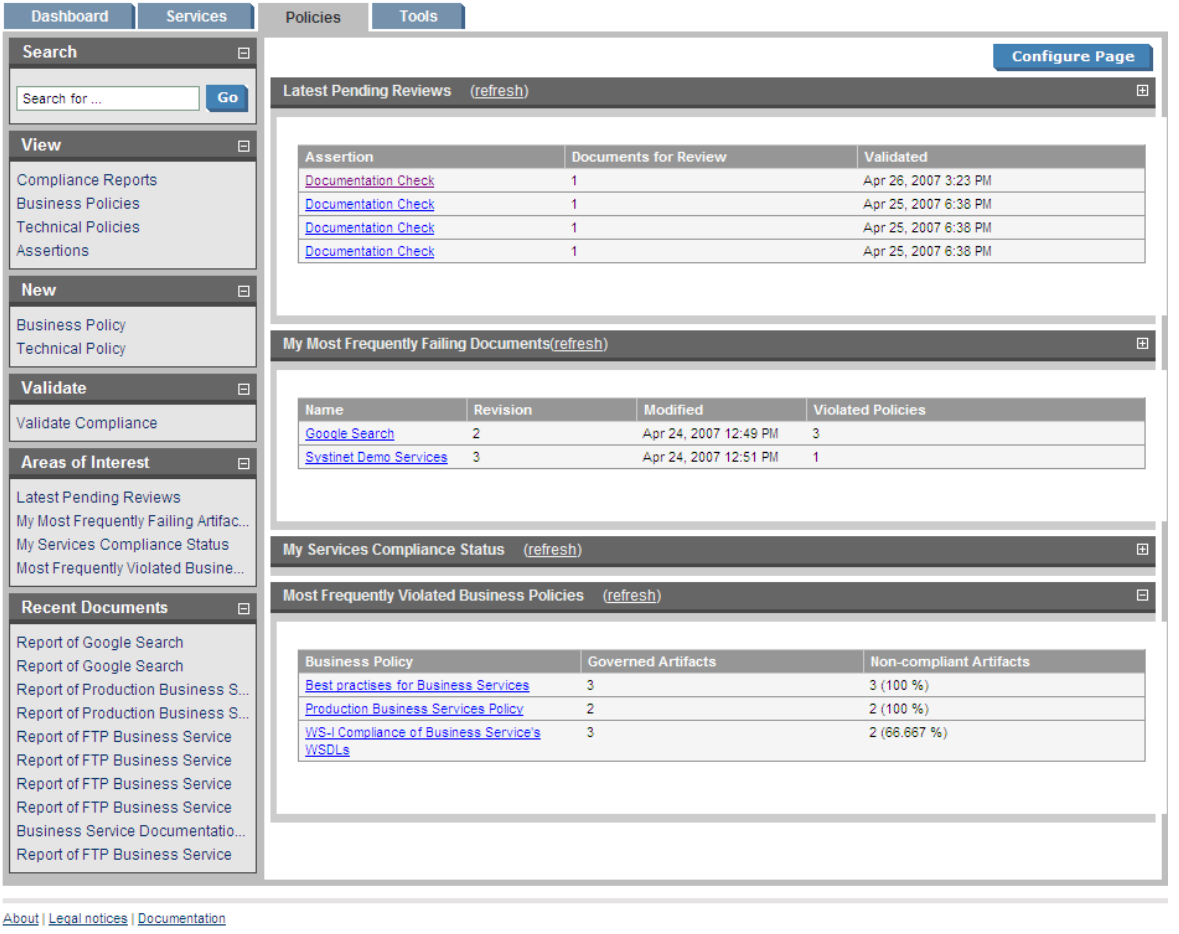
- Features of the Policies Tab on page 93. Navigating the **Policies** tab.
- Creating Business Policies on page 121. Creating and modifying business policies.
- Managing Technical Policies on page 129. Creating, browsing and modifying technical policies.
- Validating Documents on page 137. Validating documents.
- Assertion View on page 118. Browsing assertions and creating new ones.

The User's Guide describes how to operate HP SOA Systinet Policy Manager through the GUI or command line. Both interfaces replicate HTTP POST and GET calls made to REST API endpoints. These endpoints and calls are listed in the REST Interface chapter of the Developer Guide.

14 Features of the Policies Tab

The **Policies** tab is the central location which shows all information about policies and compliance reports in one place to provide easy access and simple management. The policies tab is shown in Figure 19.

Figure 19. Policies Tab



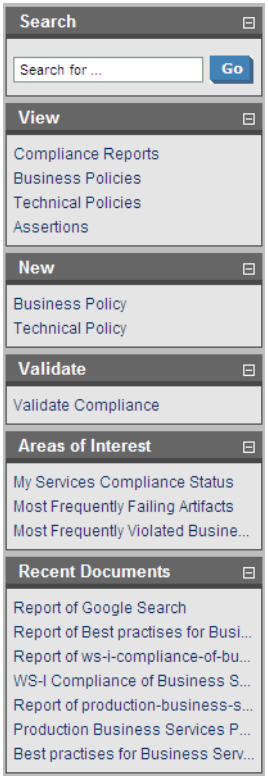
The **Policies** tab is split into the menu on the left and the main view pane, as described in these sections:

- Policies Menu on page 95
- Areas of Interest on page 96

Policies Menu

All pages in the **Policies** tab include a menu of links on the left side, such as that in Figure 20. These links let you view compliance reports, policies and assertions, create new policies or validate documents. There are also links to your most recently edited documents and your chosen **Areas of Interest**. Several of these links are also available on other tabs.

Figure 20. Policies Menu



The **Policies** menu is split into sections:

- **Search**. The full text search function described in Full Text Search on page 29.

- **View**. List business policies, technical policies, compliance reports or assertions (see Policy and Report List Views on page 101).
- **New**. Create a new technical policy or business policy.
- **Validate Compliance**. Validate the compliance of a single resource against one or more technical policies (see Resource Compliance on page 138).
- **Recent Documents**. Reopen one of the last few pages you have viewed.

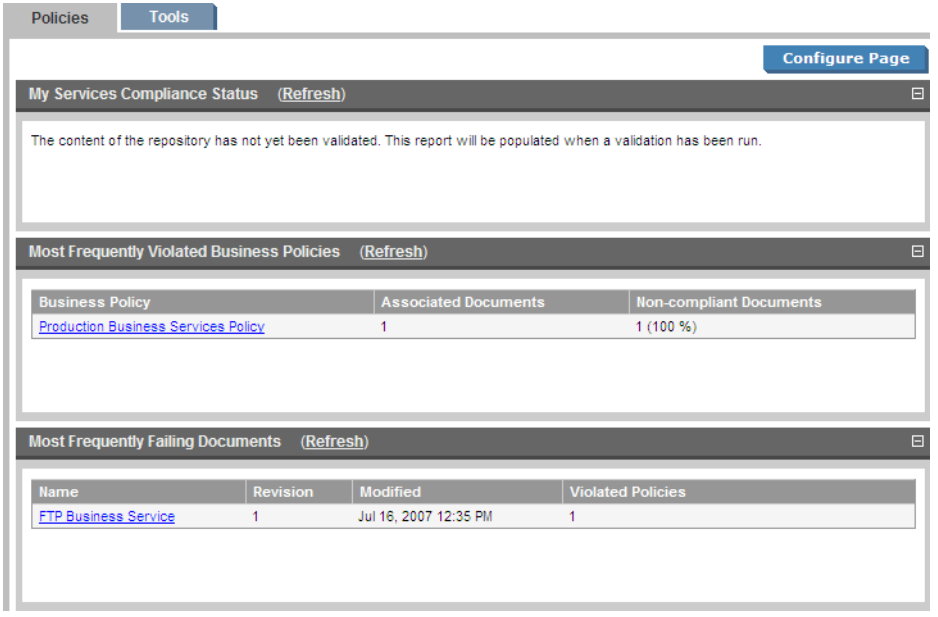
Areas of Interest

When you open the **Policies** tab, you see your areas of interest in the main view. Figure 21 shows **My Most Frequently Failing Documents**, **My Services Compliance Status** and **Most Frequently Violated Business Policies**. You can view an area of interest at any time by clicking it under **Areas of Interest** in the **Policies** menu (see Policies Menu on page 95). However, the Area of Interest does not update when you open it. To see an up-to-date Area of Interest, click **Refresh** after you open it. You might have to refresh the Area of Interest more than once to show the results of a recent action.

Resetting statistics. After policy violating problems have been fixed, you can reset the statistics for the Areas of Interest. Each Business Policy detail page (Business Policy View on page 103) and Assertion detail page (Assertion View on page 118) has a **Reset Compliance Statistics** tool in the **Tools** dropdown menu. This tool deletes all reports for that policy or assertion. You can also delete all compliance reports in the SOA Systinet repository with the command-line `resetvalidationdata` tool, located in `POLICYMGR_HOME/bin`.

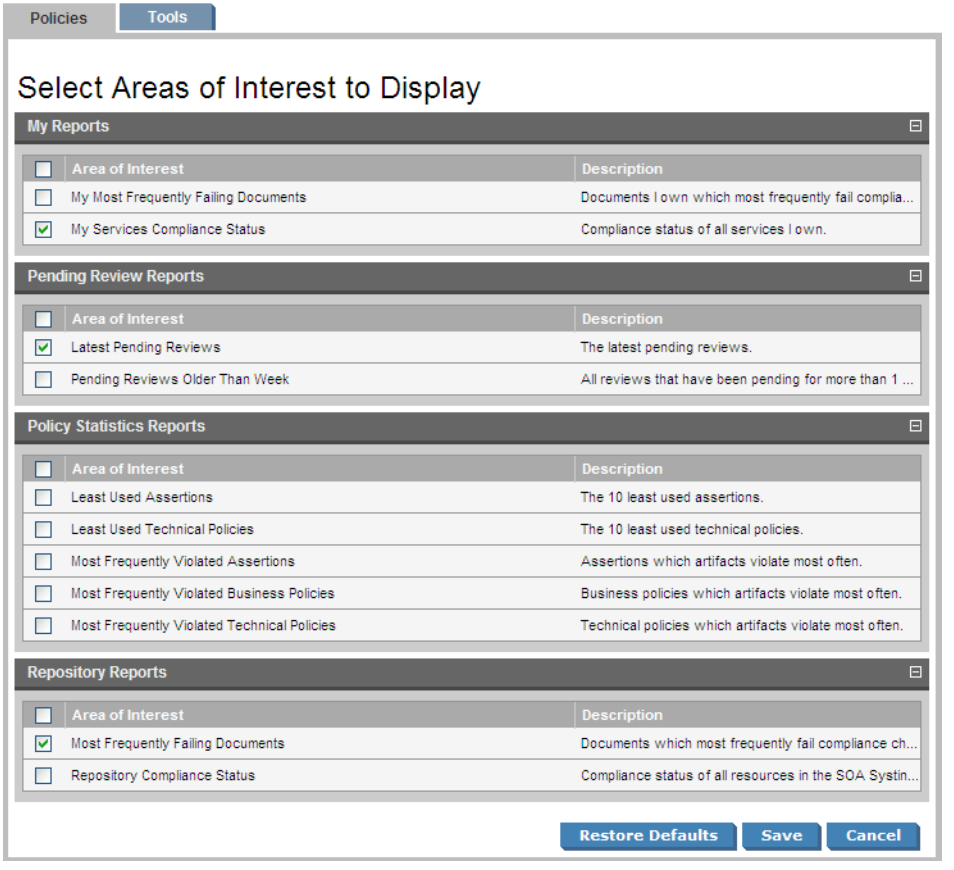
Tip: HP Systinet recommend scheduling a task using the **AOI Preparation Tool** to perform a daily update of all areas of interest. As this task is memory intensive, it should be scheduled for a non-peak period. See Creating a Task on page 200.

Figure 21. Policies Tab Showing Areas of Interest



You can select the areas of interest to display. Click **Configure Page** to view a list of possible areas of interest as shown in Figure 22. Select those you want displayed and click **Save**.

Figure 22. Select Areas of Interest to Display



Some notes about the Areas of Interest:

- **"My" Documents**. A report, policy, service etc. is 'yours' if you own it.
- **Pending Reviews**. Some assertions cannot be enforced by XML tools but require manual review. These areas of interest list all reports whose final status is pending until such manual validation is performed. Please see Reviewing Documents Manually on page 142 for full details.

15 Policy Pages

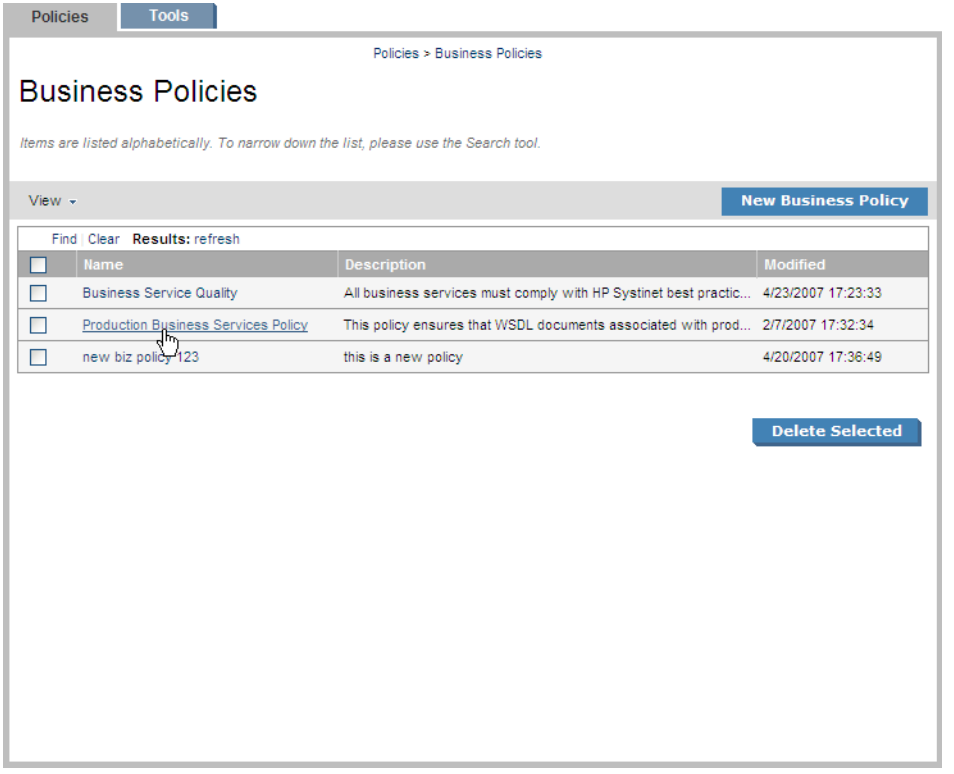
The **Policies** tab includes several view pages, described in the following sections:

- Policy and Report List Views on page 101 describes the index views of policies, reports and assertions.
- Business Policy View on page 103 describes the business policy detail page.
- Technical Policy View on page 106 describes the technical policy detail page.
- Report Views on page 107 describes the various reports Policy Manager generates.
- Assertion View on page 118 describes the assertion detail page.

Policy and Report List Views

Click one of the **View** links in the **Policies** menu (see Policies Menu on page 95) to open a list view of that type of document. Figure 23 is a list view for business policies.

Figure 23. List of Business Policies

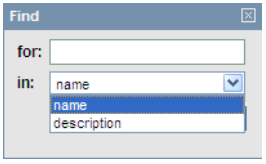


List views are broadly similar, differing only in providing the following functionality:

- **Compliance Reports**. Has a **Validate Compliance** button for running compliance checks. You can select reports and delete them on this page. See Validating Documents on page 137.
- **Business/Technical Policies**. Have **New Business Policy**/**New Technical Policy** buttons for creating new policies. See Creating Business Policies on page 121 and Creating Technical Policies on page 129. You can also delete selected policies from the lists. See Deleting Business Policies on page 128 and Deleting Technical Policies on page 136.
- **Assertions**. Delete selected assertions from the list.

List views have the same functionality as search result pages with the addition of **Find** immediately below the page heading. Click **Find** to open a search/filter dialog box. The business policy search/filter is shown in Figure 24.

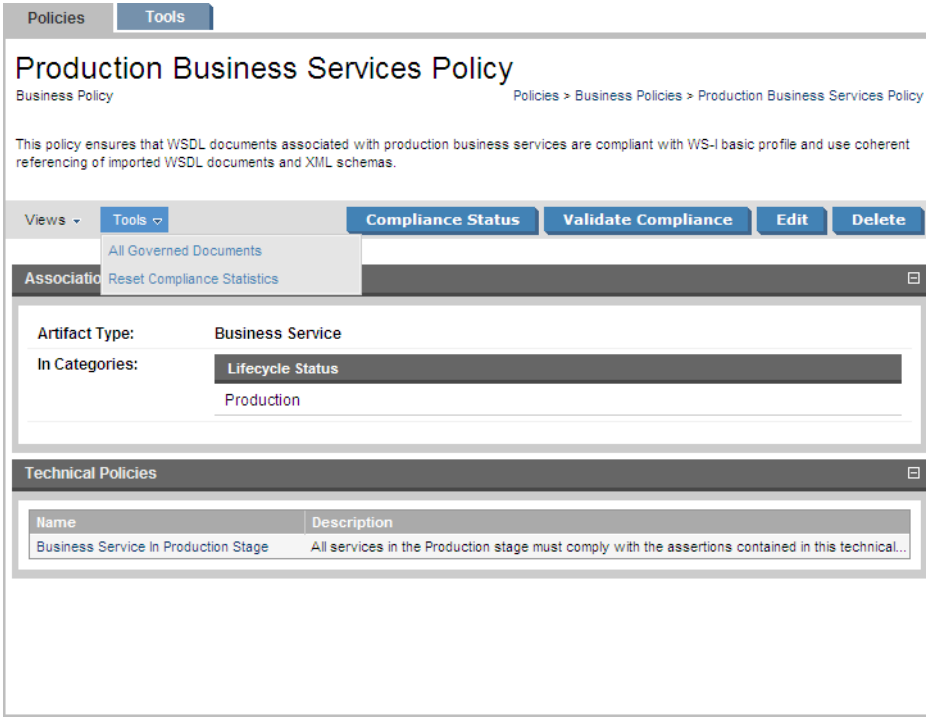
Figure 24. Policies List View Filter



Business Policy View

Click the name of a business policy in the list view (see Policy and Report List Views on page 101) to open the business policy detail view, shown in Figure 25. The detail view lists the technical policies and association rules of the business policy. In addition, you may edit the policy (opening the creation wizard) or Validate Compliance, which validates all the business policy's documents against all its technical policies.

Figure 25. Business Policy Details



Business policy detail views include a toolbar with the following buttons and context action menus:

- **Compliance Status**. Opens a view of the results of the most recent validation of the business policy. See Business Policy Summary Reports on page 108 for details.
- **Validate Compliance**. Runs a compliance check of the business policy against its associated documents. See Business Policy Validation on page 138 for details.

Important: If any of the documents associated with the business policy are missing from the repository, you will be warned of this in the detail view. Validations performed on such a policy will automatically fail.

- **Edit**. Opens a pane in which you edit the business policy. See Editing Business Policies on page 126 for details.
- **Delete**. Deletes the business policy. Deleted policies are *unrecoverable*.
- **Views**. The options in this menu are to see the **Revision History** or the **Advanced View**. The Advanced View is the policy's detail page in the **Tools** tab, as described in Artifact Detail Pages on page 170. The business policy detail reopens in the last view you selected for it.
- **Tools**. Select one of the following tools:
  - **All Governed Documents**. Lists all documents associated with the business policy. You can run a business policy validation (see Business Policy Validation on page 138) from that list.
  - **Reset Compliance Statistics**. Deletes compliance reports for this policy, which resets the relevant Area of Interest statistics.

The **Association Rules** section includes the information in Table 4 on page 105.

Table 4. Association Rules

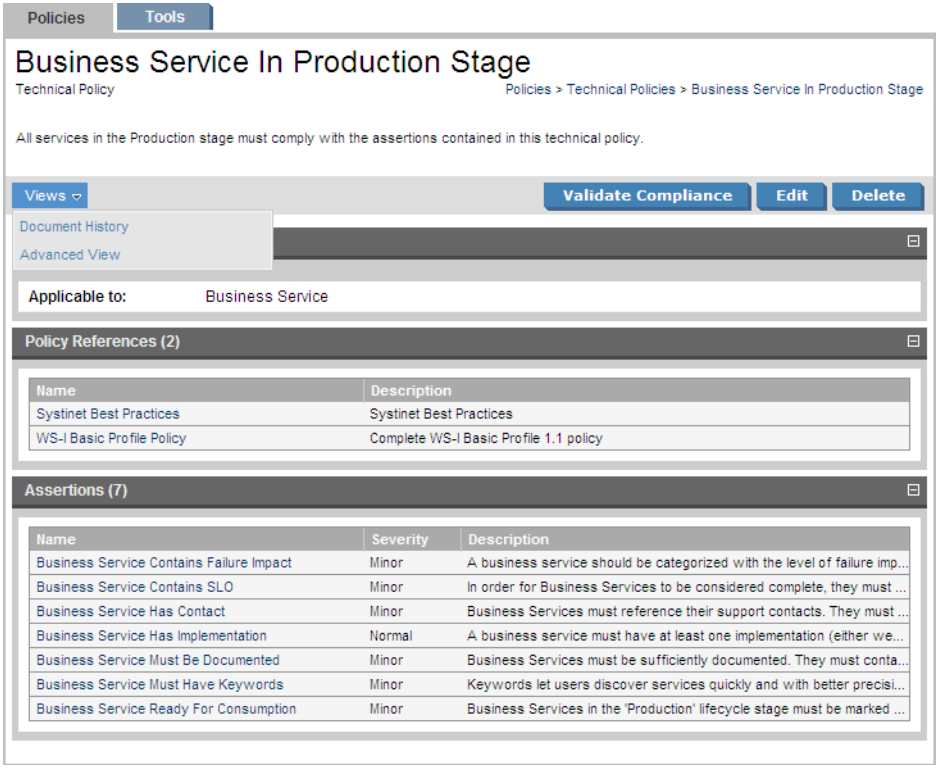
Document Type	The type of document to which the policy applies.
In Categories	The business policy applies to only those documents with the selected values in the selected categories. In Figure 25, the policy applies only to documents with a failure impact of "Low" and lifecycle stage "Prototype" or "Development."
Not In Category	As **In Categories**, except the business policy *does not* apply to those documents with the selected values in the selected category.
Exclude	The business policy does not apply to these specific documents.
Additional documents	The business policy applies to these specific documents even if the category rules would exclude them.

The **Technical Policies** section lists all technical policies associated with a document. Click the name of a technical policy to open its detail view.

Technical Policy View

Click the name of a technical policy in the list view (see Policy and Report List Views on page 101) to open the technical policy detail view, shown in Figure 26. The detail view lists the policy's assertions and policy references.

Figure 26. Technical Policy Details



Technical policy detail views include a toolbar with the following buttons and context action menus:

- **Validate Compliance**. Runs a compliance check of the technical policy against a document. The document types to which the policy may apply are listed under **Applicable to**. See Resource Compliance on page 138 for details.
- **Edit**. Opens a pane in which you can edit the technical policy. See Editing Technical Policies on page 134 for details.
- **Delete**. Deletes the business policy. Deleted policies are *unrecoverable*.
- **Views**. The options in this menu are to see the **Document History** or the **Advanced View**. The Advanced View is the policy's detail page in the **Tools** tab, as described in Artifact Detail Pages on page 170.

The **Applicable to** field shows the source types of documents to which the technical policy applies.

Technical policy detail views include a table of all assertions included in the technical policy, the severity of their violation, and their descriptions. Click the name of an assertion to open its detail view.

Report Views

Compliance checks generate the following reports:

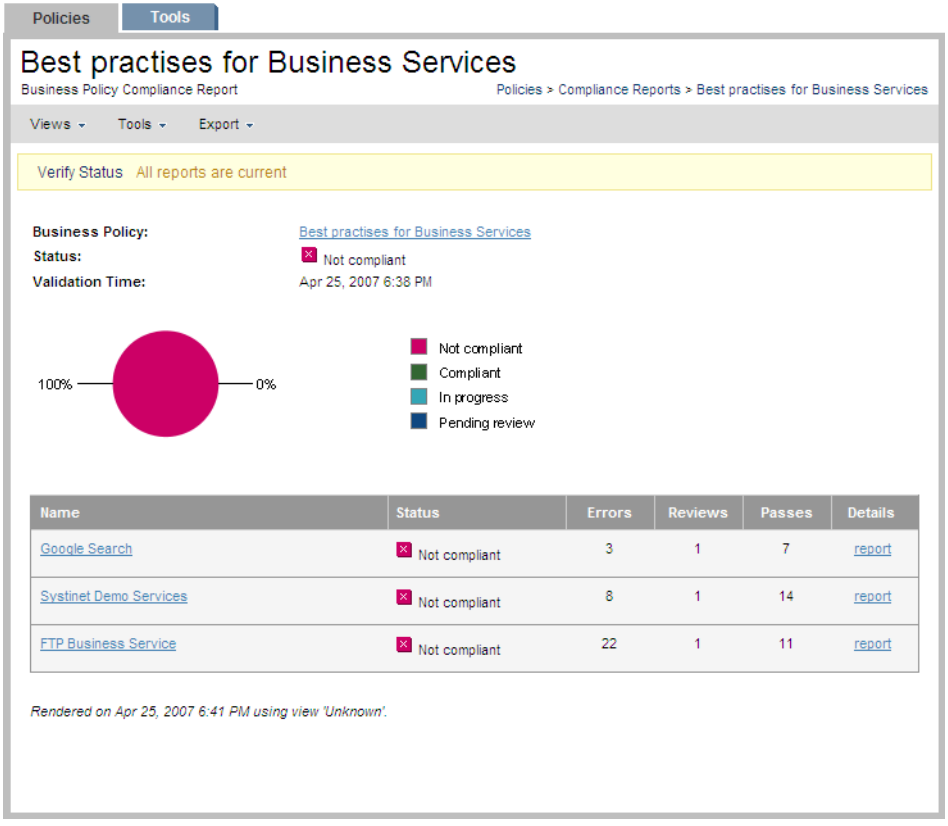
- **Business policy summary report**. Running a business policy validation (see Business Policy Validation on page 138) generates a business policy summary report. This report lists a business policy's associated documents, says whether they complied with all of the associated technical policies, and gives a breakdown of how many assertions the document complied with, how many it violated and how many require manual review. It includes links to reports for each document. See Business Policy Summary Reports on page 108.
- **Document summary report**. Validating a document against its associated business policies generates a document summary report. This lists a document's governing business policies, says whether the document complied with them, and gives a breakdown of how many assertions the document complied with, how many it violated and how many require manual review. It includes links to reports for each business policy. See Document Summary Reports on page 110
- **Document report**. A document report describes the compliance of an document and its documents with the assertions contained in the policies used to validate the document. See Document Reports on page 112.

- **Business policy report**. A business policy report describes the compliance of all documents associated with a business policy with the policy's constituent assertions. See Business Policy Reports on page 118.

Business Policy Summary Reports

A business policy validation, where all associated documents are validated against the business policy (see Business Policy Validation on page 138), produces a business policy summary report. Business policy summary reports show how many of the business policy's associated documents complied with all of its technical policies at the time of validation. Figure 27 shows the summary report for a business policy with three associated documents.

Figure 27. Best Practices for Business Services Summary Report



Business policy summary reports feature the name of the business policy, the compliance status of its documents, the time of validation and a pie chart with the percentage of tested documents that complied with all the technical policies. The name of the policy is a link to its detail view. If the business policy was altered after the compliance validation was run, the version used for the validation is next to the name.

Business policy summary reports include a toolbar with the following buttons and context menus:

- **Views**. The **Standard View** only lists business policies. The **Detailed View** lists all violated and pending assertions for each business policy. The **Responsibilities View** shows the owner and the last modifier

of each validated document. When you select a view and then close and reopen a report, it reopens displaying the last view you selected.

- **Tools**. Only the **Revalidate** tool is available. This tool validates the document against all associated business policies.
- **Export**. You can export the report as a PDF or CSV file.
- **Delete**. Deletes the report.

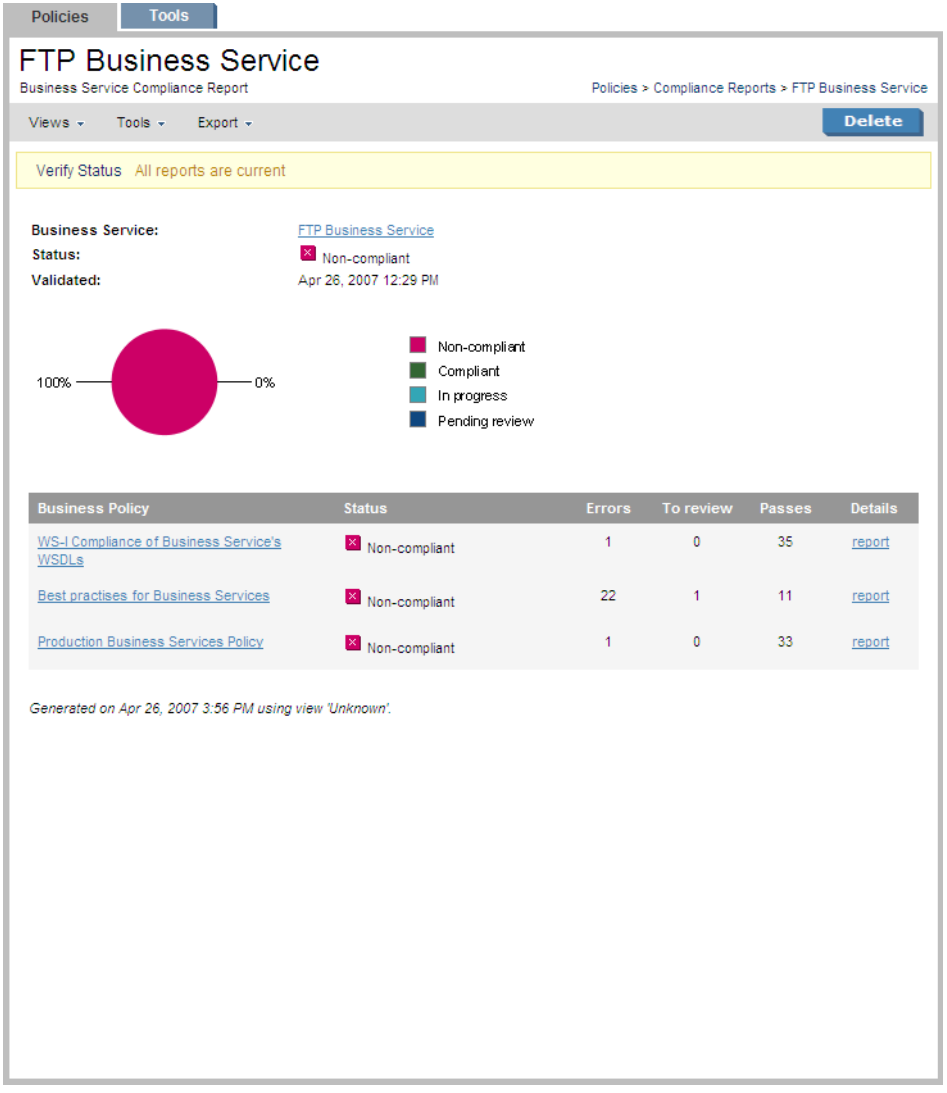
A table of tested documents occupies the bottom of business policy reports. The name of each document is a link to its detail page (see Artifact Detail Pages on page 170). You can see whether a document passed the latest validation, how many assertions it violated (**Failed**), how many it complied with (**Passed**) and how many still require manual validation (**To review**). Clicking **report** for a document opens its document report.

If the documents or policies changed since the validation generating the report was run, the report is no longer up to date. Click **Verify Status**, between the toolbar and the pie chart, to make sure the report is current.

Document Summary Reports

Validating a document against its associated business policies produces a document summary report. Document summary reports show how many business policies the document complied with at the time of validation. Figure 28 shows the summary report for a document validated against three business policies.

Figure 28. FTP Business Service Summary Report



Document summary reports feature the name of the document, its compliance status, the time of validation and a pie chart with the percentage of business policies with which it complies. The name of the document is a link to its detail view (see Artifact Detail Pages on page 170). If the document was altered after the compliance validation was run, the version used for the validation is next to the name.

Document summary reports include a toolbar with the following buttons and context menus:

- **Views**. The **Standard View** only lists business policies. The **Detailed View** lists all violated and pending assertions for each business policy. Business policy validation reports also have a **Responsibilities View**, which shows the owner and the last modifier of each validated document. When you select a view and then close and reopen a report, it reopens displaying the last view you selected.
- **Tools**. Only the **Revalidate** tool is available. This tool validates the document against all associated business policies.
- **Export**. You can export the report as a PDF or .csv file.
- **Delete**. Deletes the report.

Document summary reports include a table of business policies. (In the **Detailed View**, the violated and pending assertions are also listed under each policy.) The name of each policy is a link to its detail page (see Business Policy View on page 103). You can see whether the document complied with each policy, and for each policy how many assertions it violated (**Failed**), how many it complied with (**Passed**) and how many still require manual validation (**To review**). Clicking **report** for a business policy opens its detail report.

If the documents or policies changed since the validation generating the report was run, the report is no longer up to date. Click **Verify Status** to make sure the report is current.

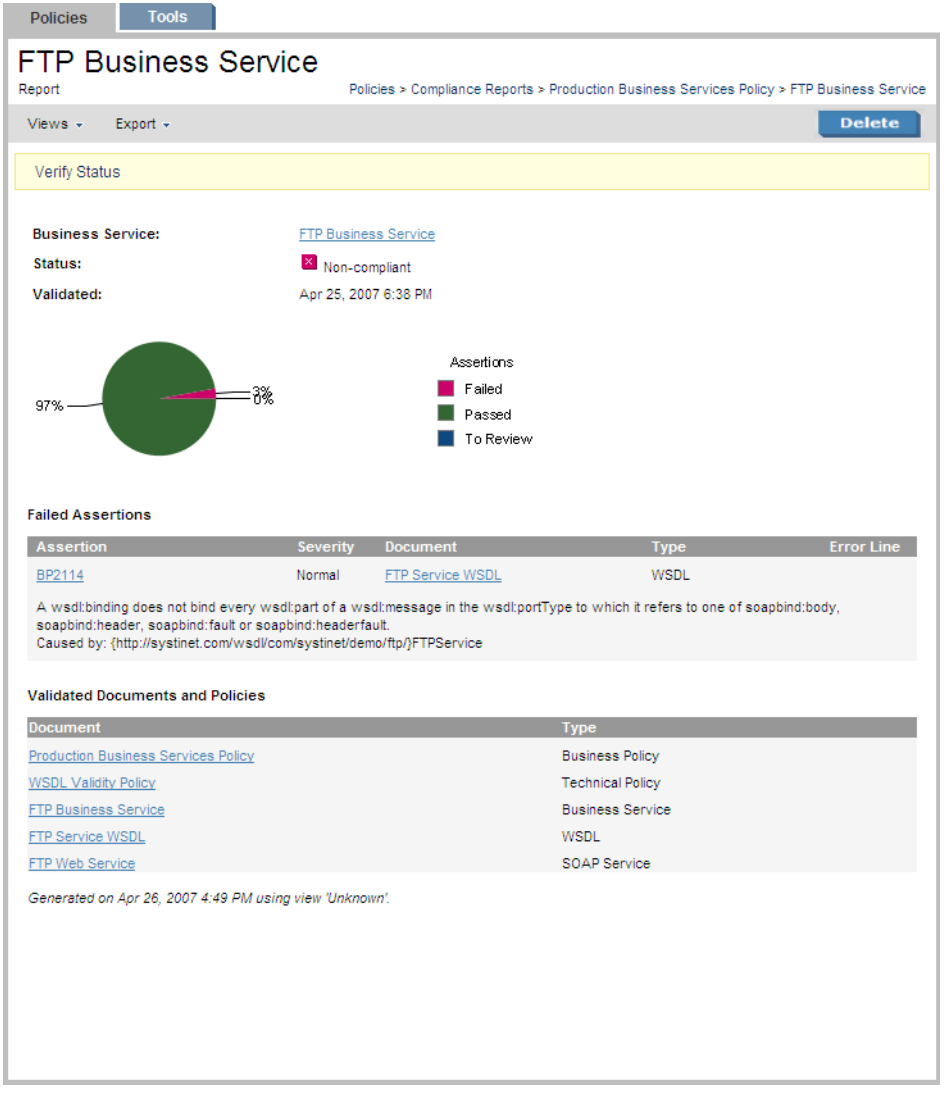
Document Reports

A document report describes the compliance of a document with business and/or technical policies. Document reports are generated in the following cases:

- During business policy validation. They are listed in the business policy summary report (see Business Policy Summary Reports on page 108).
- When a single resource is validated.

The report in Figure 29 was generated by a business policy validation using the Production Business Services Policy. It is listed in the business policy summary report for that validation.

Figure 29. FTP Business Service Report



Document reports feature the name of the document, its compliance status, the time of validation and a pie chart with the percentage of assertions with which it complies. (Compare to the document summary report, Figure 28, which gives the percentage of business policies with which it complies.) The name of the document is a link to its detail page (see Artifact Detail Pages on page 170). If the document was altered after the compliance validation was run, the version used for the validation is next to the name.

Above the pie chart is a toolbar with the following buttons and context menus:

- **Views**. The **Standard View** only lists failed and pending assertions. The **Full View** lists all assertions for each business policy. When you select a view and then close and reopen a report, it reopens displaying the last view you selected.
- **Tools**. Only the **Revalidate** tool is available. This tool validates the document against all associated business policies.
- **Export**. You can export the report as a PDF or .csv file.
- **Delete**. Deletes the report.

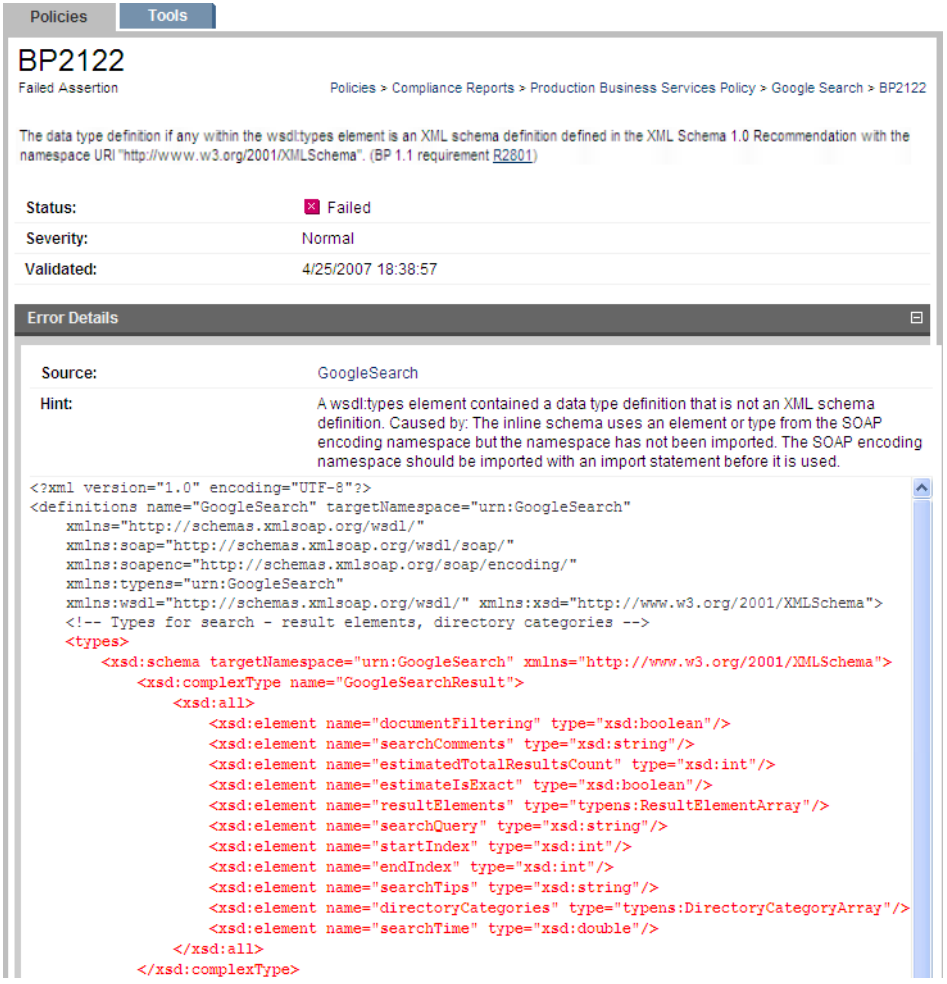
All violated and pending assertions are listed in a table beneath the pie chart. (In the **Full View**, passed assertions are listed as well.) For each assertion, the table shows:

- The name of the assertion. Clicking this opens the compliance status view of the assertion. Figure 30 shows the compliance status of the BP 2122 assertion when validating the GoogleSearch WSDL. It includes a copy of the WSDL document with the violation highlighted in red.
- The severity of the assertion.
- The specific document that violated the assertion.
- The type of document that violated the assertion.
- The line in the document where the violation occurred. Due to length, this appears beneath the other entries in the row.

The policies used to validate the document are listed in the **Validated Documents and Policies** table. Each name is a link to the policy, document or document detail page. The order in which these items is listed is, from top to bottom:

- Business policy used for validation, if applicable.
- Technical policies. If validation used a business policy, these technical policies are associated with that business policy.
- The document's name and type.
- Any other documents associated with the document and their types.

Figure 30. BP 2122 Compliance Status View



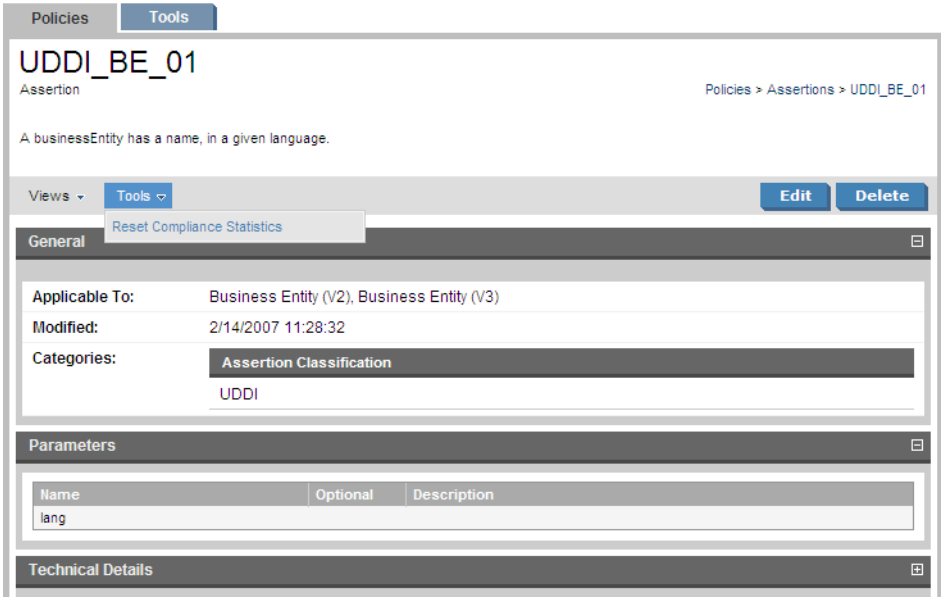
Business Policy Reports

A business policy report describes the degree to which a business policy's associated documents violate its constituent assertions. Business policy reports are generated when an document is validated against the business policies which govern it. In all other respects business policy reports are identical to document reports. See Document Reports on page 112 for details.

Assertion View

Click the name of an assertion in the **Assertions** list to open that assertion's detail view, shown in Figure 31.

Figure 31. UDDI BE 01 Assertion

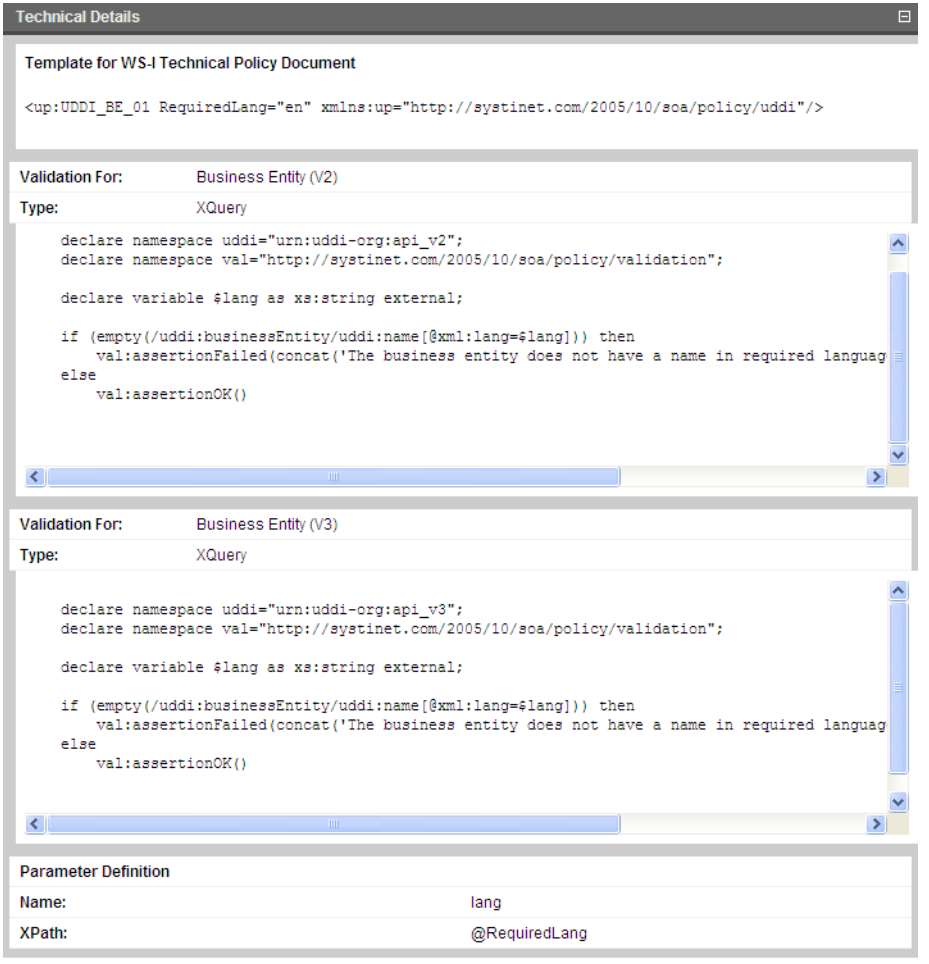


An assertion detail view shows what types of document the assertion applies to, when it was last modified, and the categories to which it belongs. Assertion detail views include a toolbar with the following buttons and context action menus:

- **Edit**. Click this to change the assertion's name or description. You cannot change any of the assertion's technical details in SOA Systinet. HP provides the HP SOA Systinet Assertion Editor tool for this purpose.
- **Delete**. Click this to delete the assertion. Deleted assertions are *unrecoverable*.
- **Views**. The options in this menu are to see the **Revision History** or the **Advanced View**. The Advanced View is the assertion's detail page in the **Tools** tab, as described in Artifact Detail Pages on page 170. The assertion detail reopens in the last view you selected.
- **Tools**. The only available tool is **Reset Compliance Statistics**. This deletes compliance reports for this assertion, which resets the relevant Area of Interest statistics.

The **Technical Details** of an assertion include the reference template, validation handlers, and parameter definitions. Figure 32 are the technical details of the UDDI BE 01 assertion. These details are explained in the Assertion Schema chapter of the Reference Guide.

Figure 32. UDDI BE 01 Technical Details



16 Managing Business Policies

Business policies are sets of documents with the technical policies with which they must comply. The procedures for managing business policies are covered in the following sections:

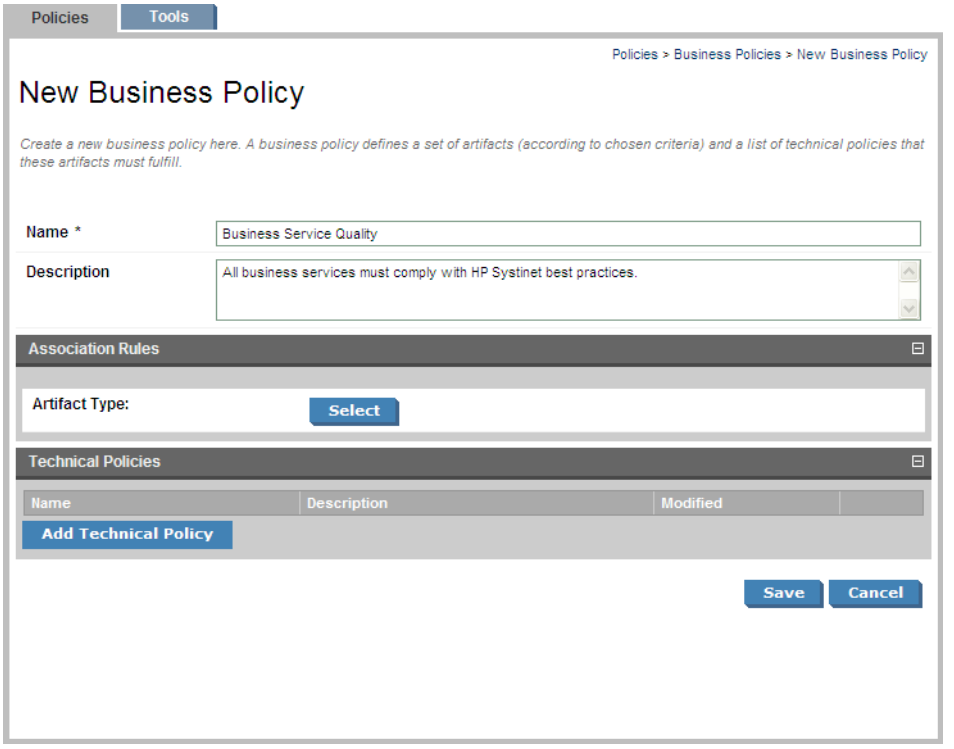
- Creating Business Policies on page 121
- Editing Business Policies on page 126
- Deleting Business Policies on page 128

Creating Business Policies

Business policies can be created from the menu on the left side of the **Dashboard** and **Policies** tabs and from the business policy list view (see Policy and Report List Views on page 101).

To create a business policy:

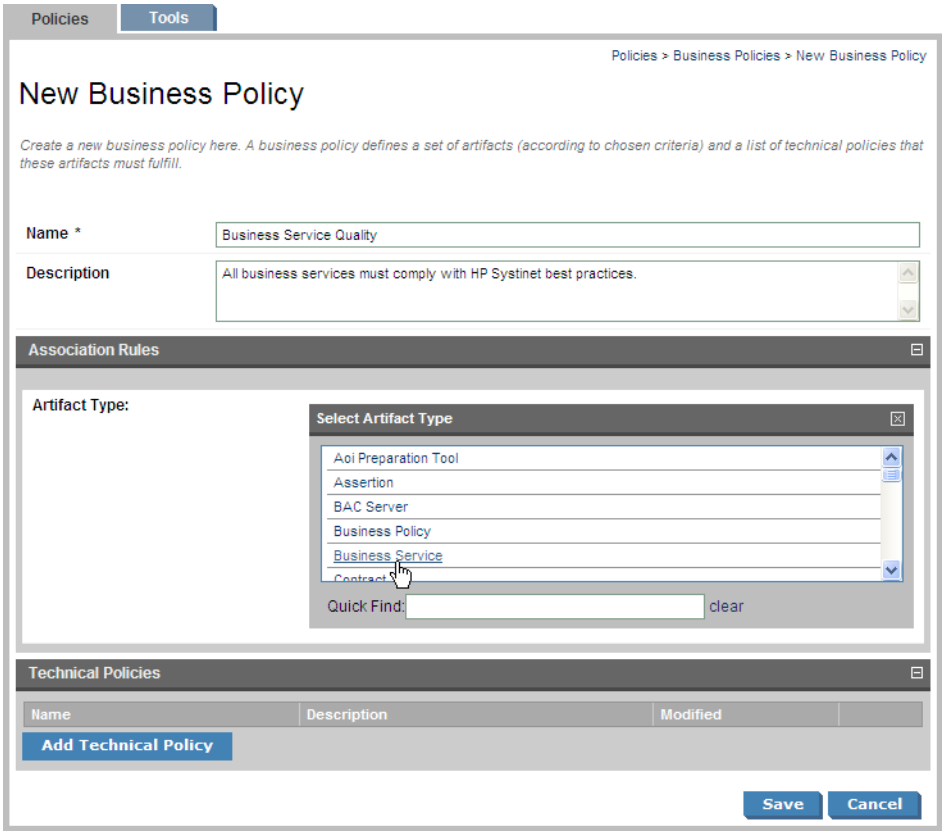
1 Click **Business Policy** in the **New** section of the **Policies** menu (see Policies Menu on page 95). The **New Business Policy** wizard opens.



2 Type a name for the business policy. This name should give an idea of the function of the policy. For example, a policy requiring that all business services comply with SOA Systinet Best Policies (a technical policy) could be called Business Service Quality. You can give further details in the optional **Description** field.

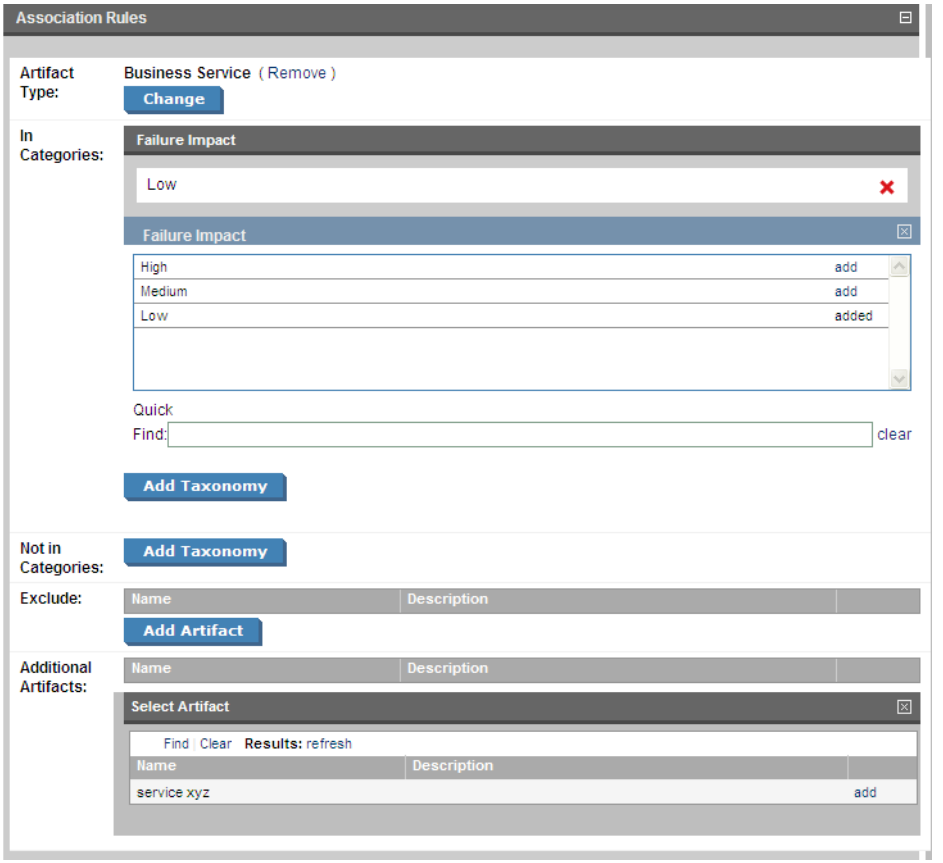
At this point in creating a business policy, click **Save** to create a draft policy. You can add association rules and technical policies at any future time by editing the policy.

3 Click **Artifact Type: Select** in the **Association Rules** section. A list of document types appears.



4 Select the type of document to which the business policy applies. By default the policy applies to all documents of this type.

5 You can narrow the scope of documents to which the policy applies. Under **Association Rules** you see a number of options:



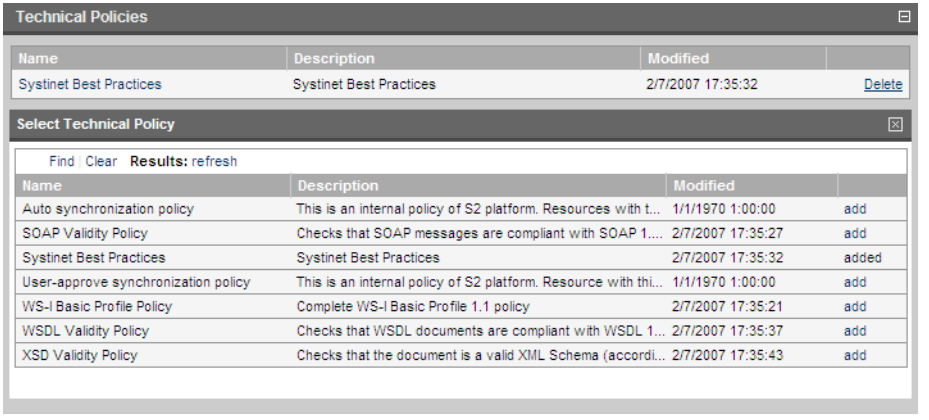
Use these options as follows:

Option	Use
Document Type	Click **Change** and a list of document types appears. Select one and change the type of document to which the policy applies.

Option	Use
In Categories	Click **Add Taxonomy** and a list of categories appears. Click a category and a list of category values appears. Click **add** next to the desired values. The business policy applies to only those documents with the selected values in the selected category. **Note:** Custom taxonomies added to the repository are propagated to Policy Manager after approximately 10 minutes. See SOA Definition Model in the Reference Guide for a description of taxonomies, document types and categories.
Not In Category	Click **Add Taxonomy** and a list of categories appears. Click a category and a list of category values appears. Click **Add** next to the undesired values. The business policy does not apply to those documents with the selected values in the selected category. **Note:** Custom taxonomies added to the repository are propagated to Policy Manager after approximately 10 minutes. Please see SOA Definition Model in the Reference Guide for a description of taxonomies, document types and categories.
Exclude	Click **Add Document**. A list appears of all documents of the type to which the business policy applies. Click **add** next to the documents you wish to exclude. The business policy does not apply to these documents. **Note:** Custom taxonomies added to the repository are propagated to Policy Manager after approximately 10 minutes. Please see SOA Definition Model in the Reference Guide for a description of taxonomies, document types and categories.

Option	Use
Additional documents	After using the **In Category** and **Not In Category** rules to narrow the scope of the business policy, you can reinclude individual documents of the excluded categories. Click **Add Document**. A list appears of all documents of the type to which the business policy applies. Click **add** next to the documents you wish to include even though other association rules would exclude them.

6 Click **Add Technical Policy** under **Technical Policies**. A list of technical policies appears.



7 Click **add** next to all technical polices you wish to associate with the business policy.

8 Click **Save**.

Editing Business Policies

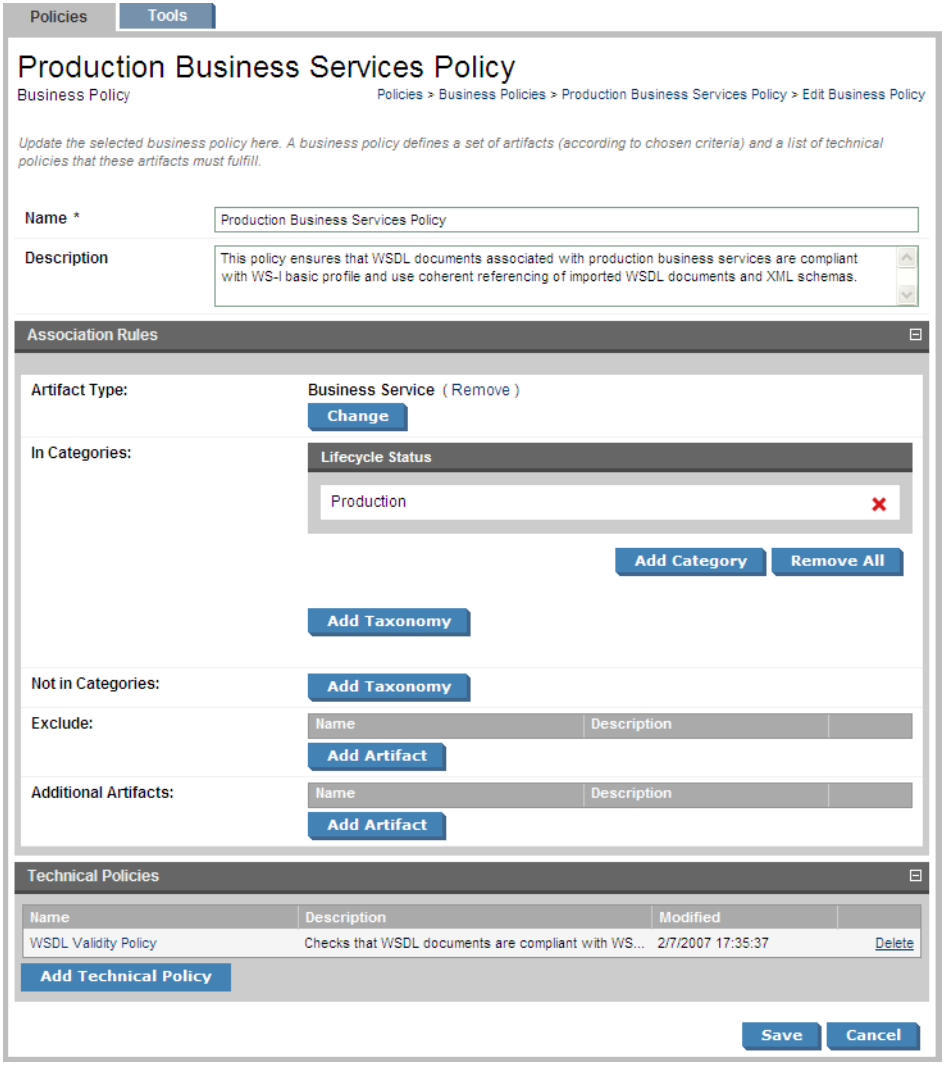
Business policies can be edited from their detail views, described in Business Policy View on page 103.

To edit an existing business policy:

1 In the business policies list view (see Business Policy View on page 103), find the business policy.

2 Click the name of the policy to open its detail view.

3 Click **Edit** in the detail view. The **Edit** page for that business policy opens.



4 You can now change the name, association rules and technical policies of the business policy. The procedure is identical to creating a business policy. See Creating Business Policies on page 121, starting at Step 2.

The **Revision History** records all changes made to a business policy. The **Revision History** can be viewed from a context action in the business policy's detail view. See Business Policy View on page 103.

Deleting Business Policies

You can delete a business policy either from the business policy list view or the policy's detail view (see Policy and Report List Views on page 101 and Business Policy View on page 103).

- In the business policy list view, select the business policies you wish to delete and click **Delete Selected**.
- In the business policy's detail view, click **Delete** in the toolbar.

Warning: Deleted policies are *unrecoverable*! (Equivalent to `--purge` on the command line)

17 Managing Technical Policies

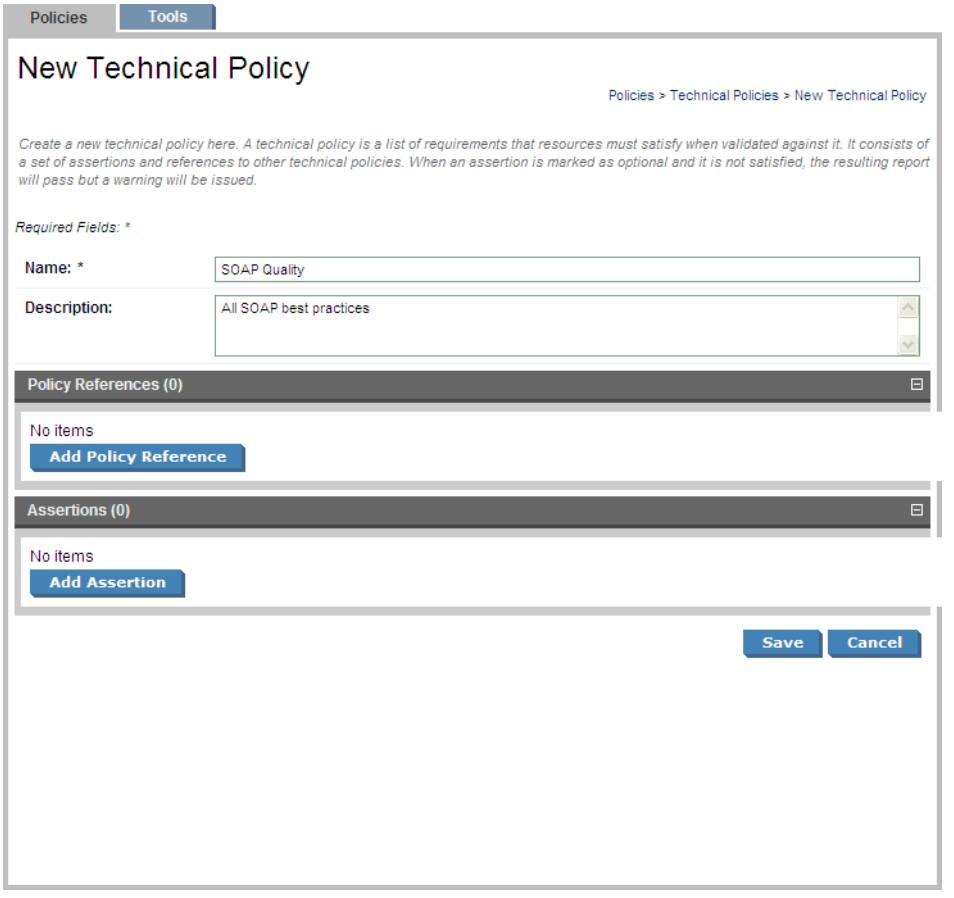
The procedures for managing technical policies are covered in the following sections:

Creating Technical Policies

You can create technical policies from the menu on the left side of the **Policies** tab and from the technical policy list view (see Policy and Report List Views on page 101).

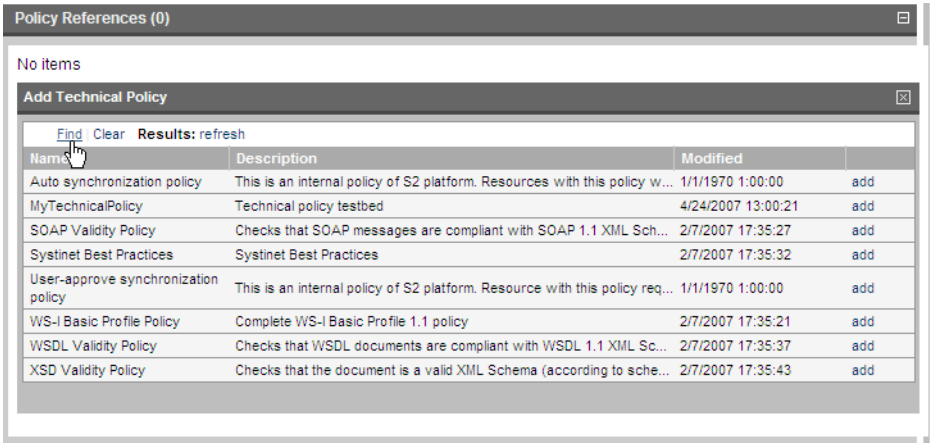
To create a technical policy:

1 Click **Technical Policy** in the **New** section of the **Policies** menu (see Policies Menu on page 95). The **New Technical Policy** wizard opens.



2 Type a name for the technical policy. This name should give some idea of the function of the policy. Further details can be given in the optional **Description** field. You can save a technical policy that includes only a name and description and edit it in a later production stage to include policy references and assertions.

3 To include references to another technical policy, click **Add Policy Reference**. A list appears of all technical policies. (If you are not including policy references, go to Step 6.)

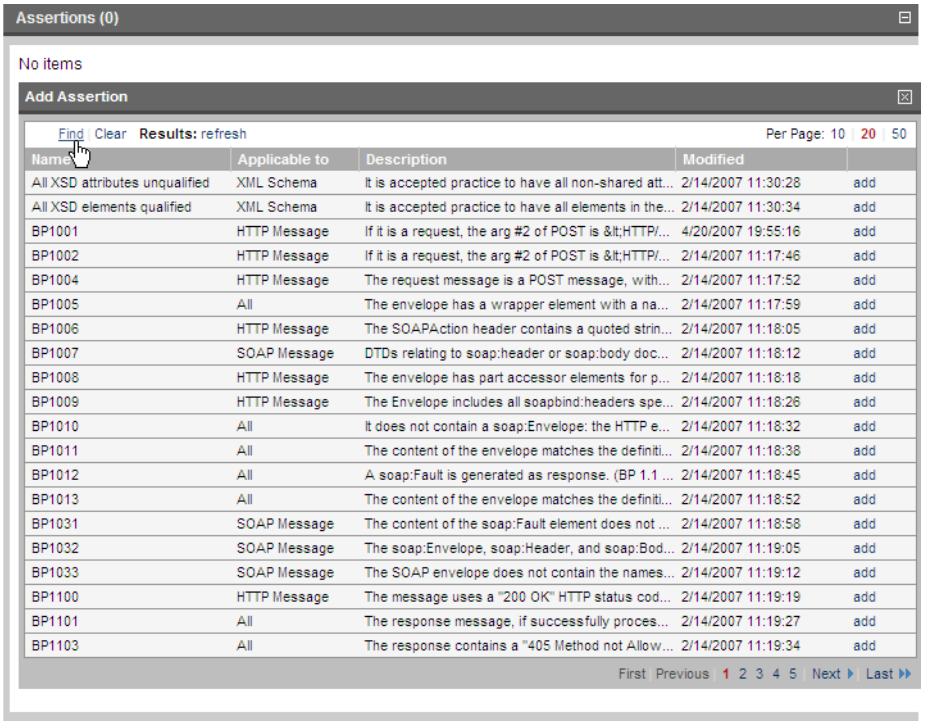


4 To filter the list or search for a specific policy, click **Find**.

5 Click **Add** by each policy you wish to reference. The technical policy you are creating enforces all the referenced policies' assertions.

Note: A technical policy cannot refer to itself. The UI will not allow you to include such a circular reference.

6 To include assertions in the technical policy, click **Add Assertions**. A list of all assertions appears.



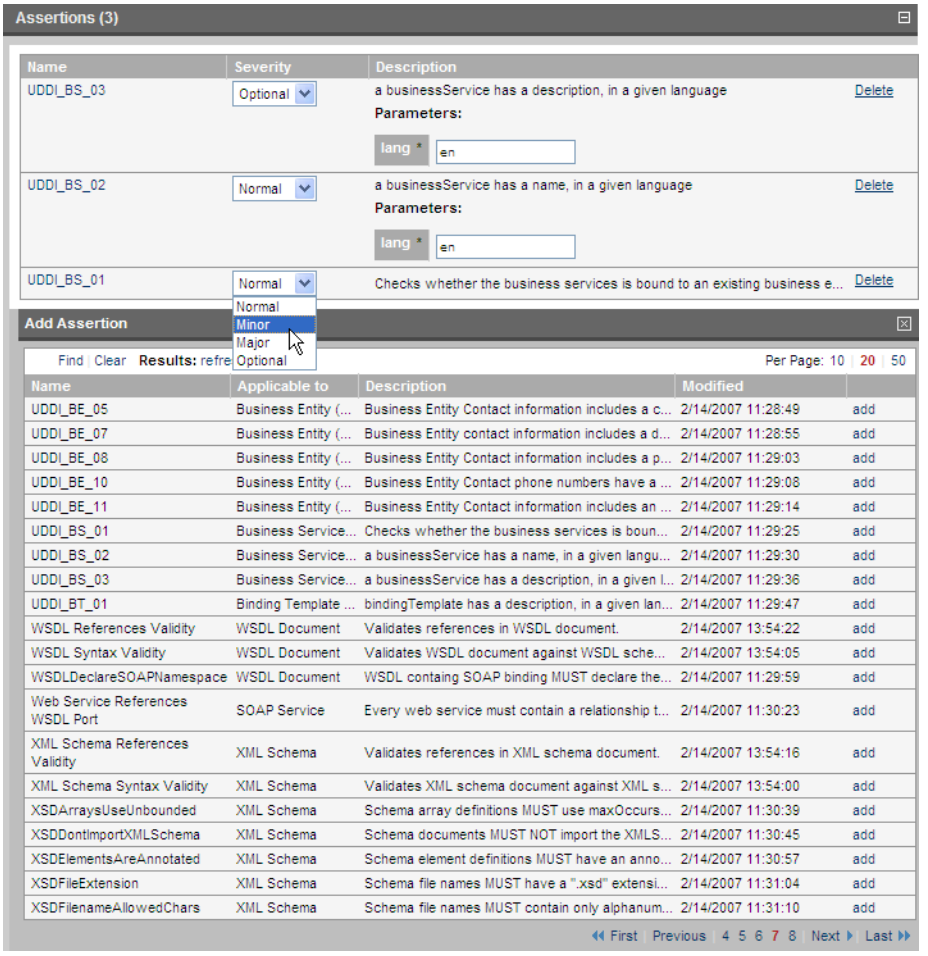
7 To filter the list or search for a specific assertion, click **Find**.

8 Click **add** by each assertion you wish this technical policy to enforce.

9 After adding an assertion, you can click the assertion's name and see its detail view.

10 Select a value in the added assertion's **Severity** field to set the severity of its violation.

11 If the assertion includes parameters, you can set or change their values. Parameters inherit default values from the assertion template if their values are set in the template. Non-optional parameters must have a value. (See SOA Definition Model in the Reference Guide for more information about assertion schema and parameters.)



Warning: Do not create technical policies that directly enforce more than 100 assertions. Instead, create multiple smaller technical policies and include them into a master technical policy through policy references. See Step 3.

12 Click **Save**.

Editing Technical Policies

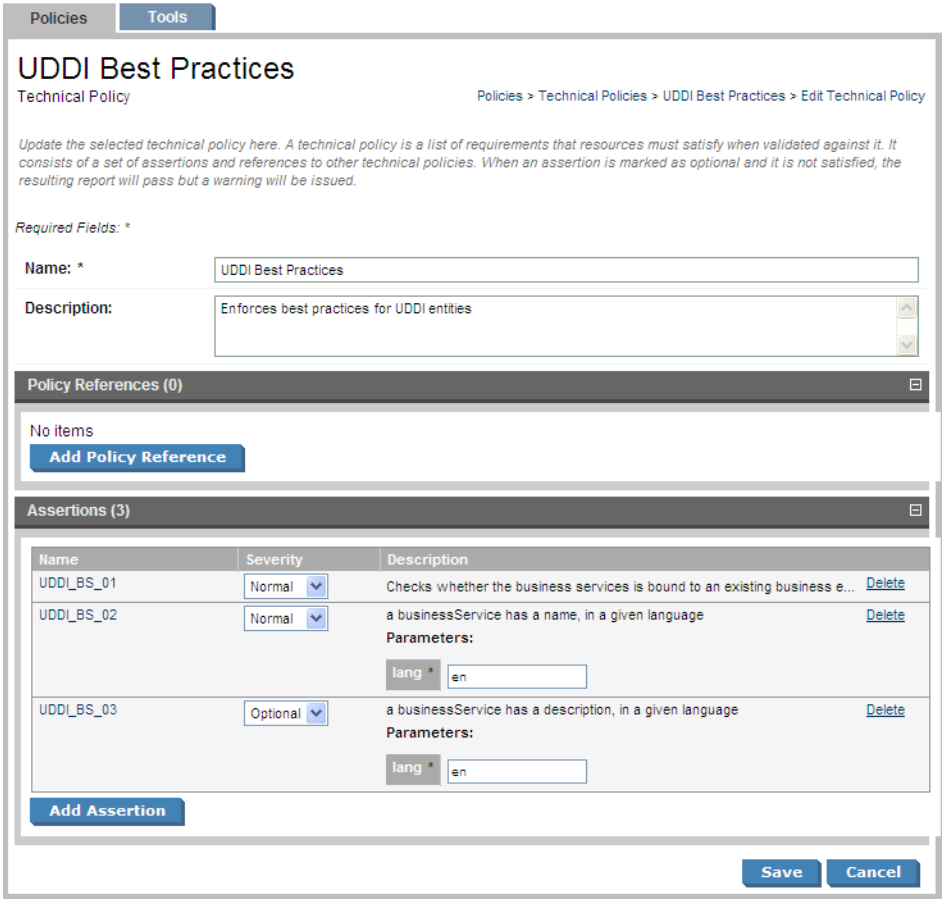
Edit a technical policy to add or delete assertions and policy references or set the value of assertion parameters.

To edit a technical policy:

1 Find the technical policy in the list view of technical policies (see Policy and Report List Views on page 101).

2 Click the name of the policy to open its detail view.

3 Click **Edit** in the detail view (see Technical Policy View on page 106). The **Edit** page for that technical policy opens.



4 Add or delete policy references and assertions (see Creating Technical Policies on page 129).

5 To view an assertion's detail view, click its name (see Assertion View on page 118).

6 Change the severity level of an assertion and/or the value of any parameters it has as when creating a technical policy, described in Creating Technical Policies on page 129.

7 Click **Save**.

Deleting Technical Policies

You can delete a technical policy either from the technical policy list view or the policy's detail view (see Policy and Report List Views on page 101 and Technical Policy View on page 106).

- In the technical policy list view, select the technical policies you wish to delete and click **Delete Selected**.
- In the technical policy's detail view, click **Delete** in the toolbar.

Warning: Deleted policies are *unrecoverable*! (Equivalent to `--purge` on the command line)

18 Validating Documents

Validation is the process of checking one or more documents to see if they comply with the requirements of one or more policies. Reports are generated when you run a compliance validation. These reports can be viewed by clicking **Compliance Reports** under **View** in the left-margin menu.

Policy Manager provides three types of document validation, which along with other validation features are described in the following sections:

- Document Validation on page 137. Validation of a document against all business policies associated with it.
- Business Policy Validation on page 138. Validation of all documents associated with a business policy.
- Resource Compliance on page 138. Validation of a single document against one or more technical policies, for test purposes.
- Reviewing Documents Manually on page 142. Some assertions require a manual review of the document to determine its compliance.
- Deleting Compliance Reports on page 146. Deleting reports.
- Validation Client on page 146. Running validation with a command-line client.

Document Validation

To validate a document against all associated business policies:

1 Do one of the following:

- From the **Services** tab, open the document's view page (see Service View on page 56)
- From the **Tools** tab, open the document's detail page (see Artifact Detail Pages on page 170).

2 Open the **Compliance** context action menu and select **Validate Compliance**.

3 Validation runs automatically, generating a document summary report as described in Document Summary Reports on page 110.

You can schedule document validation to run automatically as a SOA Systinet task. Create a new task, select the **Validate Compliance** tool and select the document or documents to be the subject of the validation. See Creating a Task on page 200 for details. Scheduled validations always have a lower priority than ones you run at the moment.

Business Policy Validation

You can validate the compliance of all a business policy's associated documents against all its technical policies. The result is a business policy summary report as described in Business Policy Summary Reports on page 108. To run a business policy validation, click **Validate Compliance** in the policy's detail page, as described in Business Policy View on page 103. No further user input is needed.

You may also schedule regular business policy validations as a SOA Systinet task. Create a new task, select the **Validate Compliance** tool and select the business policy to be used for the validation. See Creating a Task on page 200 for details. Scheduled validations always have a lower priority than ones you run at the moment.

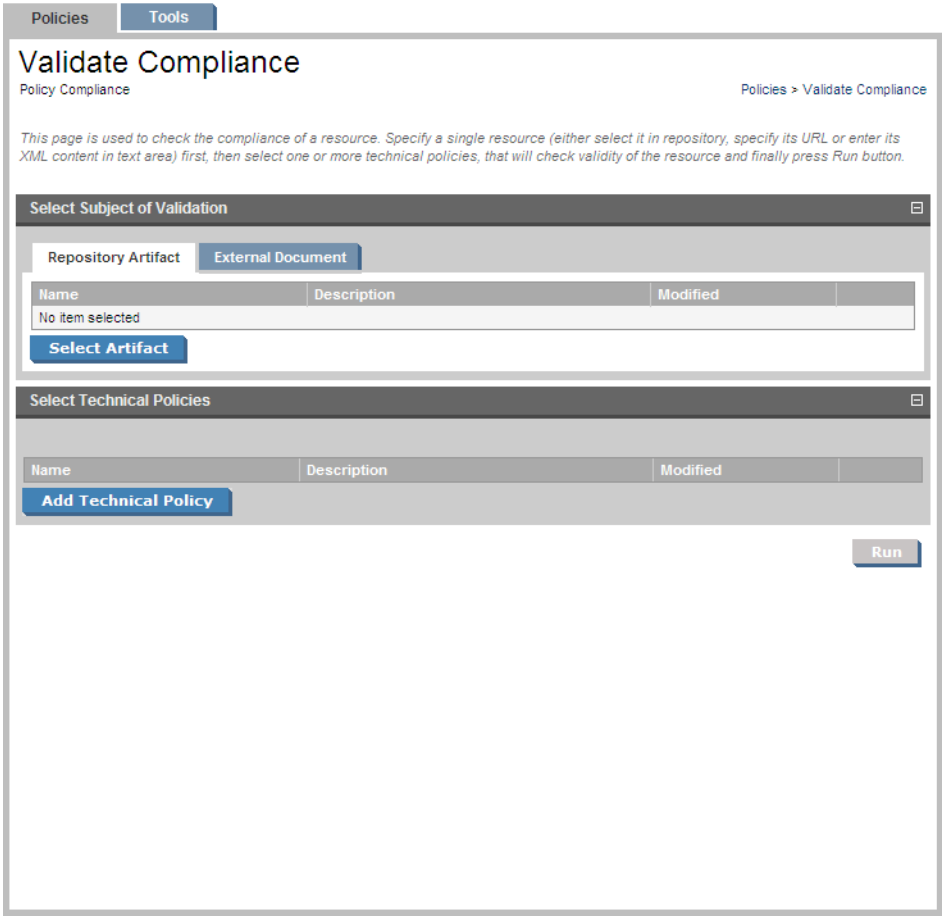
You can run a business policy validation from a remote client with the client `server-validate` tool. See Validating Against Policy On Server (server-validate) on page 151 for details.

Resource Compliance

Select a single resource to check for compliance against one or more technical policies. This can be useful for testing purposes during resource or policy development.

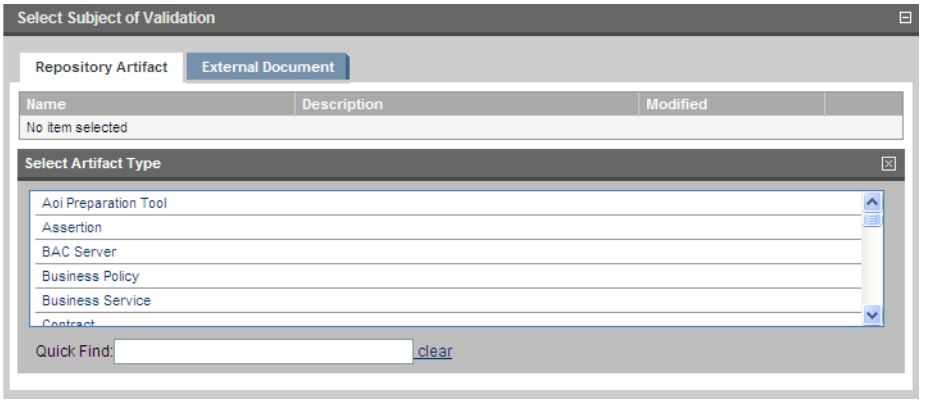
To check the compliance of a single resource:

1 From the **Policies** or **Dashboard** tab menu, or from a technical policy's detail view (see Technical Policy View on page 106), click **Validate Compliance**. The **Validate Compliance** page opens.

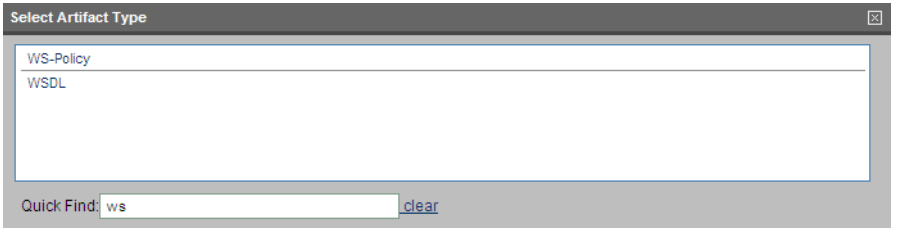


2 Select the subject of validation. This can be either a repository document or an external document. To select a repository document:

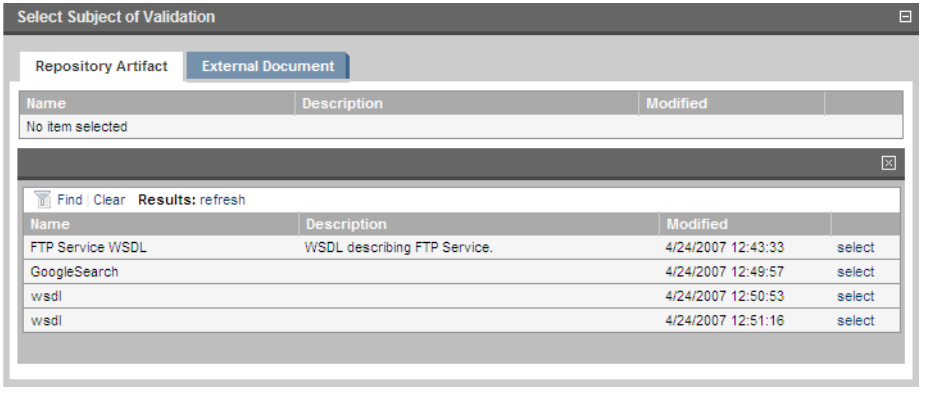
a Click **Select Artifact** in the **Repository Artifact** tab. A list of document types appears.



b You can narrow the list by typing part of the artifact type's name in the **Quick Find** field.



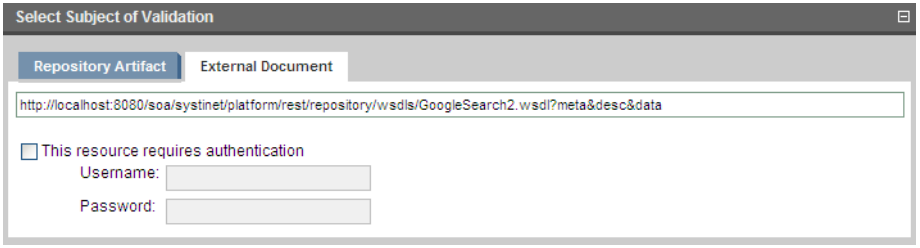
c Select an artifact type by clicking on it. A list appears of artifacts of this type. You can narrow down this list by clicking **Find**, which opens a filter dialog box, and typing a partial name.



d Click **select** by the artifact you want to validate. Only one artifact can be selected.

To select an external document:

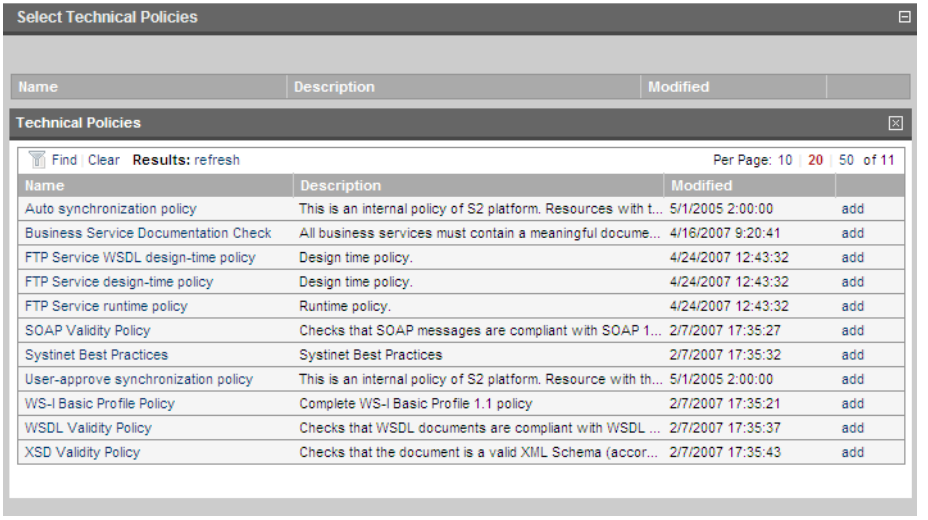
a Click the **External Document** tab to open it.



b Type or paste the document URL.

c If the document is secure, select **This resource requires authentication** and type the username and password.

3 Select the technical policies to be used for the validation. To select a technical policy, click **Add Technical Policy**. A list of technical policies appears. You can narrow down this list by clicking **Find**, which opens a filter dialog box, and typing a partial name or selecting a category. If you launched the validation from a technical policy's detail page in Step 1, that technical policy is already selected.



4 Click **add** by the technical policies you want to use.

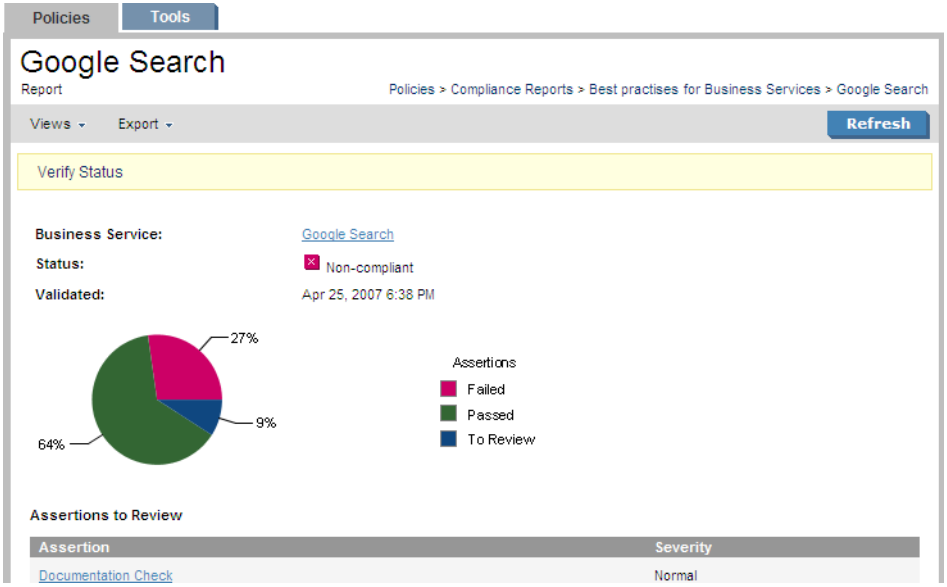
5 Click **Run**. Validation generates a document report as described in Document Reports on page 112.

Reviewing Documents Manually

Some assertions cannot be enforced programatically but require a human to review the document being validated. When a validation is run that involves such an assertion, Policy Manager informs you in these ways:

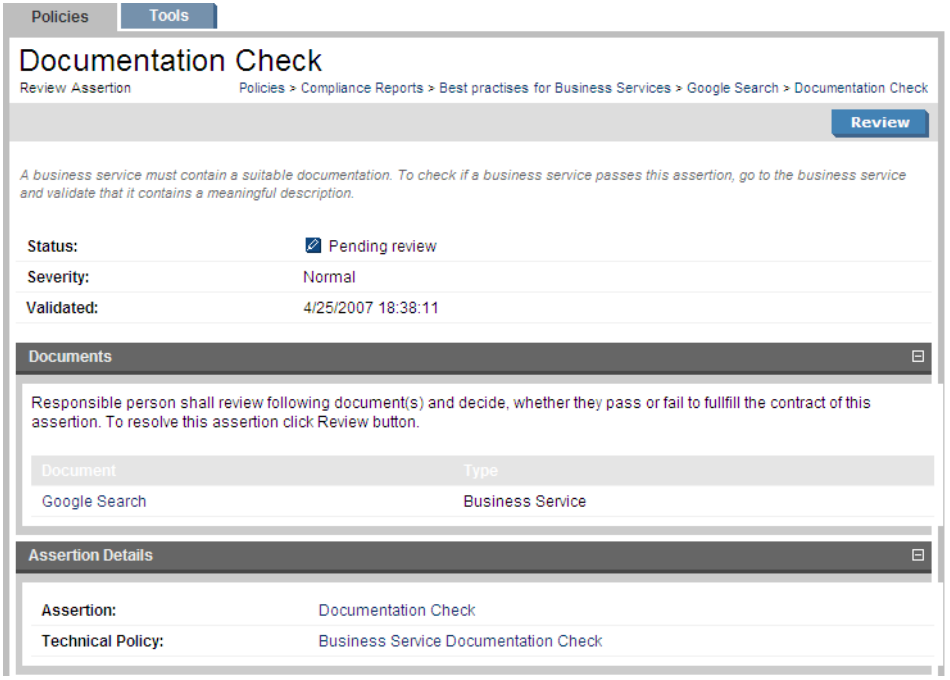
- The **Latest Pending Reviews** and **Pending Reviews Older than Week** areas of interest list the assertions requiring manual document review. See Areas of Interest on page 96.
- The document reports (see Document Reports on page 112) or business policy reports (see Business Policy Reports on page 118) that include the assertion list it under **Assertions to Review**. Figure 33 is from a document report with an assertion pending review.

Figure 33. Google Search Document Report Awaiting Review



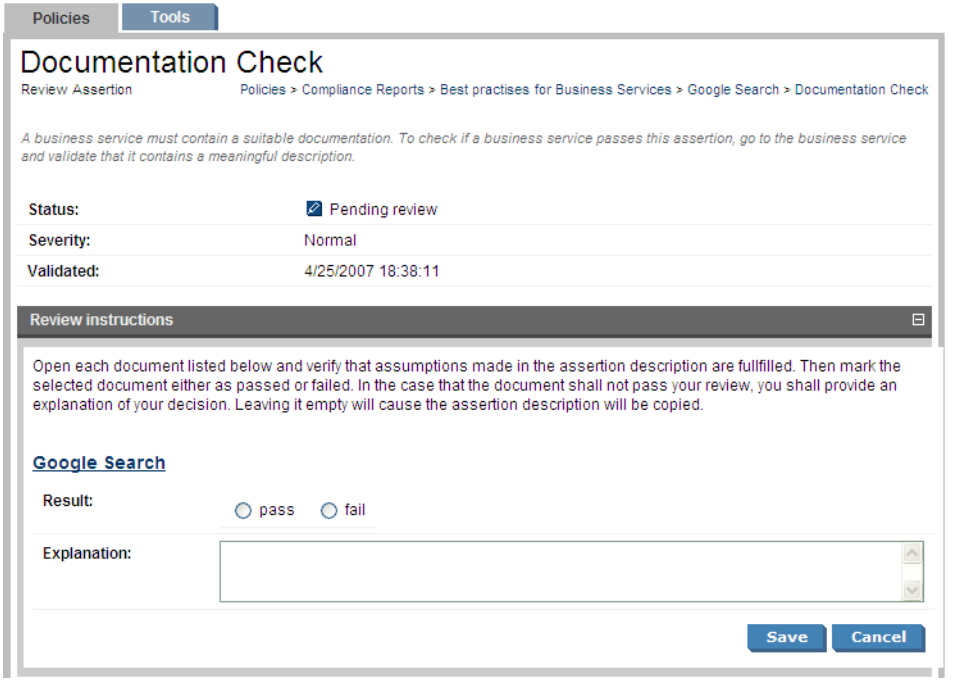
To manually review a document:

1 In either the report (see Figure 33) or the **Pending Reviews** area of interest, click the assertion name. The assertion's compliance status page opens.



2 To open the detail page of a document under review (see Artifact Detail Pages on page 170 and Service View on page 56), click its name under **Documents**. You can also read the assertion or technical policy detail pages by clicking their names under **Assertion Details**.

3 To perform the review, click **Review**. The assertion's review page opens.



4 To open the detail page of a document under review (see Artifact Detail Pages on page 170 and Service View on page 56), click its name under **Review Instructions**

Tip: Depending on the conditions of the assertion, you may want to see the **Advanced View** of the detail page. From the **Advanced View** you can open the **XML View**. All views are accessible from the **Views** context action menu.

5 After reviewing the document, select **Pass** or **Fail** in the assertion's review page. If you select **Fail**, type in an explanation of why the document fails validation in the **Explanation** field.

6 Click **Save**. The document or business policy report page opens.

Deleting Compliance Reports

On the **Compliance Reports** view page, you can select and delete individual reports. Every summary report and document report also has a **Delete** button for deleting that report.

Each Business Policy detail page (Business Policy View on page 103) and Assertion detail page (Assertion View on page 118) has a **Reset Compliance Statistics** link in the **Tools** dropdown menu. This tool deletes all reports for that policy or assertion. Similarly, every artifact in the **Tools** tab except technical policies has a **Reset Compliance Statistics** link in its **Tools** dropdown menu. Click this link to delete all reports for that artifact.

You can also delete all compliance reports in the SOA Systinet repository with the command-line `resetvalidationdata` tool, located in `POLICYMGR_HOME/bin`.

Validation Client

Policy Manager includes a command-line validation client that you can copy to another computer on the network. The validation client is designed for the following uses:

- Validating local and/or remote documents against local policies. These validations run on the client.
- Validating local and/or remote documents against policies located on a server. These validations run on the server.

The validation client is located at `POLICYMGR_HOME/client`. To install the client, copy this folder to the location of your choice.

The validation client command-line tools are located in `POLICYMGR_HOME/client/bin`. The tools and their functions are described in the following sections:

Downloading Policies and Assertions (sync)

To perform validations locally, you need local copies of the policies and assertions in the SOA Systinet repository. To download these policies and assertions, run the `sync` tool. Your computer has to be connected to the SOA Systinet server/cluster when you run `sync`.

To run `sync`, simply enter **sync.bat|.sh -u *`SOA Systinet username`* -p *`SOA Systinet password`***. If SOA Systinet does not require any credentials, enter **sync.bat|.sh -noauth**. The `sync` tool gets the hostname and port of the SOA Systinet host from the `.../client/bin/sync.properties` file, created automatically when Policy Manager is installed.

Local Validations (validate)

Validate documents against local copies of technical policies by running the `validate` tool. The syntax is `validate.bat|.sh` [OPTIONS] {--policy local_technical_policy_name,_file_or_uri...} {--source source_file_or_uri...}
. For a full list of options and examples of commands, enter **validate.bat|.sh --help**.

Local documents must exist before you can validate them. Download a set of documents with the `sync` tool before running `validate`.

Policy Formats

You can write technical policies in the following formats:

- As the plain text name of the policy, in quotation marks. For example, `"Systinet Best Practices"`.
- As the file name (full or relative) of the policy file. For example, `C:/opt/systinet/policymgr/client/data/policies/systinet-best-practices.xml`.
- As the full URI of the policy. For example, `file:///opt/systinet/policymgr/client/data/policies/systinet-best-practices.xml`.

Source Formats

You can write source document locations in the following formats:

- As the file name (full or relative) of the document. For example, `C:/tmp/services/service1.wsdl`.

- As the full URI of the document. For example, `http://localhost:8080/services/service1.wsdl`.

To validate one source against one policy it is not necessary to include any options in the command line. For example, to validate a local copy of `service1.wsdl` against a local copy of the **Systinet Best Practices** technical policy, you can run **validate.sh "Systinet Best Practices" C:/tmp/services/service1.wsdl**.

Validating Multiple Sources With Multiple Policies

You can validate multiple source documents and/or use multiple technical policies. In this case, it is mandatory to use the `-p|--policy` and `-d|--source` options. For example, **validate.bat -p "Systinet Best Practices" -p file:///opt/systinet/policymgr/client/data/policies/wsdl-validity.xml -d C:/tmp/services/service1.wsdl -d C:/tmp/services/service2.wsdl** validates `service1.wsdl` and `service2.wsdl` against the **Systinet Best Practices** and **WSDL Validity** technical policies.

You can make the validation stop the first time a policy is violated. Use the `-c/--stop` option. For example, the validation launched by **validate.sh --stop -p "WSDL Validity" -p "Systinet Best Practices" -d C:/tmp/services/service1.wsdl -d C:/tmp/services/service2.wsdl** would stop when either `service1.wsdl` or `service2.wsdl` violated either **Systinet Best Practices** or **WSDL Validity**.

Selecting Sources By Wildcard

Instead of specifying every source document to be validated, you can specify a directory of documents and pass a wildcard so all matching documents in that directory will be validated. Specify the directory with the `-d|--source` option and use the `-e|--pattern` to pass the wildcard. For example, **validate.bat -p "Systinet Best Practices" -d C:/tmp/services -e service*.wsdl** would validate `service1.wsdl`, `service2.wsdl`, etc, against the **Systinet Best Practices** technical policy.

Setting Up Output

By default, validation reports are created in text format and printed in the console window. You can save the report as a file by using the `-o|-outputDir` option and the file location. For example, **validate.sh -o C:/tmp/reports "Systinet Best Practices" C:/tmp/services/service1.wsdl** would create the file `C:/tmp/reports/service1.txt`.

Report names are based on source names by default. To give a report a different name, use the `-n|--name` option.

You can produce output in HTML or XML format instead of text. Use the `--format html` or `--format xml` option, respectively. When producing HTML or XML output, specify an output location with the `-o|-outputDir` option. Otherwise the raw HTML or XML is only printed out to the console.

If you produce a report in XML format, you can use it to produce any number of HTML reports with the `render` tool. See Rendering Output from XML Reports (render) on page 152.

When the `validate` tool produces HTML output, it uses a template combining XSL and graphics. The validation client comes with a default template that reproduces the Policy Manager report style. You can add additional templates by saving them in the `../client/templates` folder. Specify the template to be used by using the `-m|--template` option. For example, if you saved a custom template in `.../client/templates/MyCustomTemplate`, use it to produce HTML output by running **validate.sh --format html --template MyCustomTemplate [-p policy] [-d source]**. If you do not specify a template, the default template is used.

ANT Task Automation of `validate`

You can automate the execution of the `validate` tool as an ANT task. Write an ANT script to launch `validate` and save the script in `.../client/bin`. Launch it with the **ant** command. For example, if you create an ANT script called `/client/bin/validatetask.xml`, launch it with **ant -f validatetask.xml**.

The elements of the ANT task are given in Table 5 on page 150. Example 1 on page 151 is an example of an ANT task script for launching `validate`.

Table 5. `validate` ANT Task Elements

Element name	Attributes	
`taskdef`	`name`	Must be `validate`.
	`classname`	Must be `com.systinet.policy.tools.ant.ValidateTask`
`validate` (Child of `target`)	`format`	Output format. Takes one of `xml`, `html`, or `txt`
	`policyPropsFile`	Specifies Policy Manager properties file. Usually `../conf/policy-manager.properties`
	`output`	Output file path, such as `C:/opt/reports/` or `C:/tmp/myreport.html`. If file name is not specified, it will match the validated source's name or `summary.txt|xml|html` if it is a summary report.
	`cancel`	Boolean. `true` stops the validation at the first failure.
`policies` (Child of `validate`)	No attributes. Contains a list of all policies to be used for the validation, in nested ANT elements (`fileset/include`).	
`sources` (Child of `validate`)	No attributes. Contains a list of sources to be validated, in nested ANT elements (`uri`, `fileset/include`).	

Example 1: `validate` ANT Task

```
<?xml version="1.0"?>
<project name="validatetool" default="main">
  <taskdef name="validate" classname="com.systinet.policy.tools.ant.ValidateTask"/>
  <target name="main">
    <validate format="html" policyPropsFile="../conf/policy-manager.properties" output="C:/tmp/out">
      <policies>
        <fileset dir="../data/policies/">
          <include name="wsdl-validity.xml"/>
          <include name="systinet-best-practices.xml"/>
        </fileset>
      </policies>
      <sources>
        <uri value="http://api.google.com/GoogleSearch.wsdl"/>
        <fileset dir="../data/policies/">
          <include name="wsdl-validity.xml"/>
        </fileset>
      </sources>
    </validate>
  </target>
</project>
```

Validating Against Policy On Server (server-validate)

Validate a document against a technical policy in an SOA Systinet repository, or remotely run a business policy validation, by running the `server-validate` tool. The tool publishes a report in the same SOA Systinet repository that contains the policy. The URL of the report is printed on the command-line console.

The syntax for validating a document against a technical policy is
`server-validate.bat|.sh` [OPTION] {-u *`SOA Systinet username`*} {-p *`SOA Systinet password`*} [-s *`SOA Systinet server URL`*] { *`POLICY_URI`* } {SOURCE_FILE_OR_URI}
. The syntax for running a business policy validation is
`server-validate.bat|.sh` [OPTION] {-u *`SOA Systinet username`*} {-p *`SOA Systinet password`*} [-s *`SOA Systinet server URL`*] {-b *`BUSINESS_POLICY_URI`*}
For a full list of options and examples of commands, enter **server-validate.bat|.sh --help**.

Policy URIs

Policy URIs are in the following formats:

- Technical policy URI: `http|https:`*`hostname:port`*`/soa/systinet/platform/rest/repository/wsPolicies/`*`policy-name`*
- Business policy URI: `http|https:`*`hostname:port`*`/soa/systinet/platform/rest/repository/businessPolicies/`*`policy-name`*

Policy names in URIs are in lower case, have hyphens instead of whitespaces, and do not include the word "policy." For example, the **WSDL Validity** technical policy URI ends in `../wsdl-validity`, and the **Testing Business Services** business policy URI ends in `../testing-business-services`.

Source Formats

Only specify a source document if you are validating one against a technical policy. You can write source document locations in the following formats:

- As the full file name of the document. For example, `C:/tmp/services/service1.wsdl`.
- As the full URI of the document. For example, `http://api.google.com/GoogleSearch.wsdl`.

Selecting the SOA Systinet Server

By default, the `server-validate` tool communicates with the installation of SOA Systinet from which the validation client was copied. It can use a policy in a different SOA Systinet repository. Specify the SOA Systinet repository with the `-s|--server` option and the URL of the SOA Systinet host. Be careful to use the authorization credentials for that server.

Rendering Output from XML Reports (render)

If you have a report in XML, you can use it to generate HTML reports by running the `render` tool. The syntax is
`render.bat|.sh` {--input *`full_path_to_XML_report`*} {--outDir *`output_directory`*} [OPTIONS]
. For a full list of options and examples of commands, enter **render.bat|.sh --help**.

Overwriting Reports

The `render` tool cannot overwrite existing reports of the same name in the same directory. By default, `render` gives the output file the same name as the input file. If a file of the default name already exists and you want to generate a report in the same location, give it a different name by using the `-n|--name` option.

Selecting Output Template

The `render` tool uses a template combining XSL and graphics. The validation client comes with a default template that reproduces the Policy Manager report style. You can add additional templates by saving them in the `../client/templates` folder. Specify the template to be used by using the `-m|--template` option. For example, if you saved a custom template in `../client/templates/MyCustomTemplate`, use it to produce HTML output by running **render.sh [-i XML_input_file] [-o output_directory] -m MyCustomTemplate**. If you do not specify a template, the default template is used.

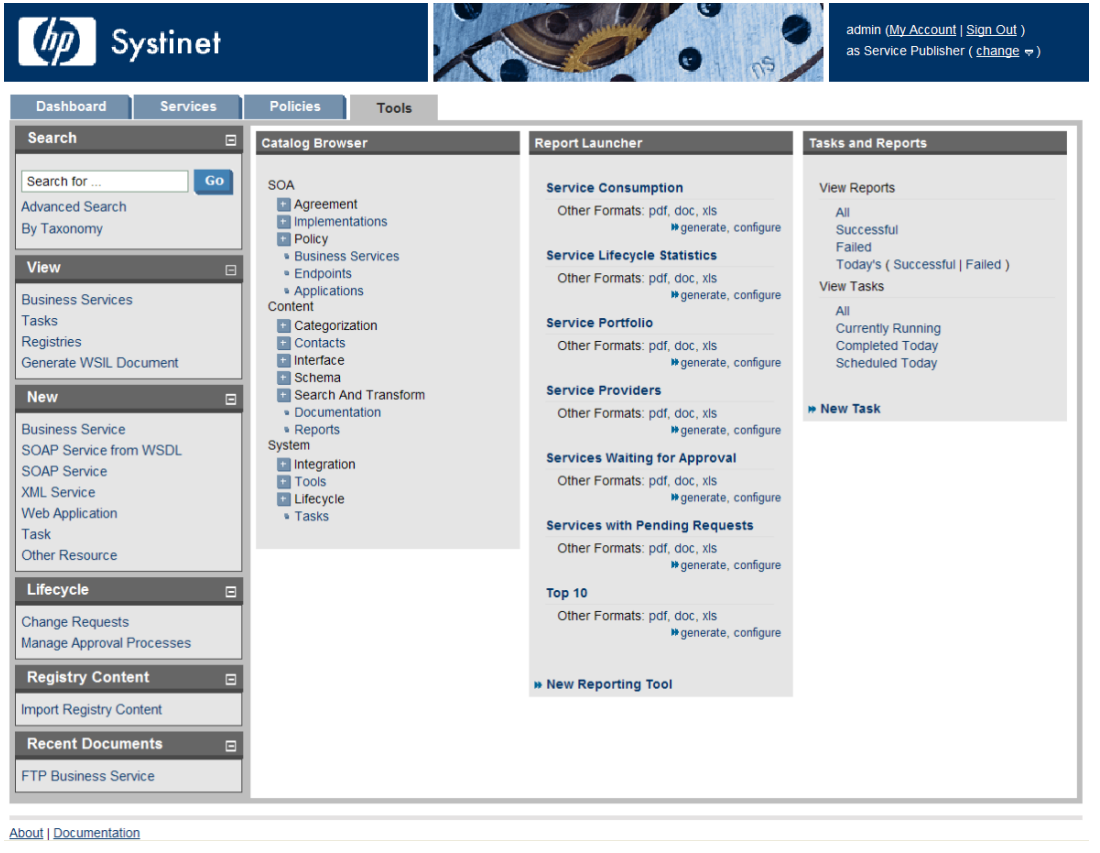
Part V. Tools

- This part explains the features and use of the **Tools** tab, which is the place to organise and manage your SOA content. It includes the following sections:
- Features of the Tools Tab on page 157 describes the user interface elements of the **Tools** tab.
- Tools Pages on page 167 describes the pages for browsing and viewing artifacts in the **Tools** tab.
- Managing Content on page 177 explains the procedures for managing the content of SOA Systinet.
- SOA Utilities on page 189 describes the use of SOA Systinet governance tools, tasks and reports.
- Stored Searches on page 205 describes the advanced search facilities of SOA Systinet.
- Registry Integration on page 209 explains how to integrate SOA Systinet with a UDDI registry.
- Business Availability Center Integration on page 217 describes how to integrate SOA Systinet with HP Business Availability Center.
- SOA Manager Integration on page 221 describes how to integrate SOA Systinet with HP SOA Manager.

19 Features of the Tools Tab

The **Tools** tab gives access to Information Management offering a generic view of the content of SOA Systinet and access to administration and governance tools:

Figure 34. The Tools Tab



The **Tools** tab is split into the menu on the left, the **Catalog Browser** and a number of portlets in the main section of the page.

Each feature is explained in detail in the following sections:

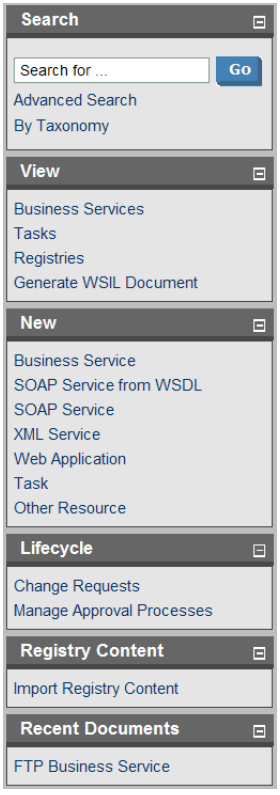
- Tools Menu on page 158. A description of the items in the **Tools Menu**.
- Catalog Browser on page 160. The index portlet of artifact types in the repository.
- Tasks and Reports Portlet on page 162. A portlet to access tasks and the reports on the results of those tasks.
- Report Launcher Portlet on page 163. An access portlet for customized reporting tools.

The portlets in the **Tools** tab can be moved in the same way as described in Features of the Dashboard Tab on page 39.

Tools Menu

The **Tools** menu is split into sections:

Figure 35. Tools Menu



- **Search**. The full text search function described in Full Text Search on page 29.
- **View**. A set of links to Browse Views showing an index of the artifacts in the repository.
- **New**. A set of links to create new artifacts:
  - **Business Service**. Create a new business service as described in Creating a New Business Service on page 61.
  - **SOAP Service from WSDL**. Create a new SOAP implementation using a WSDL document as described in Publishing a SOAP Service from WSDL on page 186.

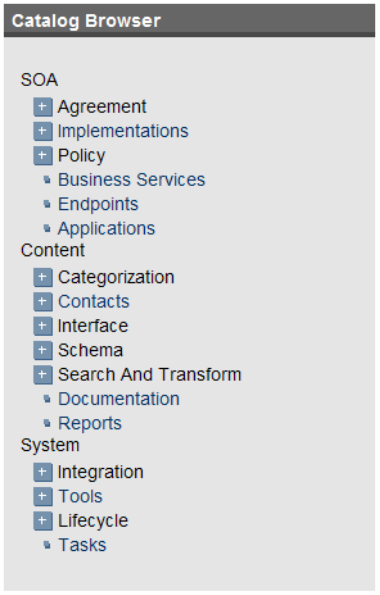
- **SOAP Service**. Create a new SOAP service artifact.
- **XML Service**. Create a new XML service artifact as described in Adding an XML Service on page 68.
- **Web Application**. Create a new web application artifact as described in Adding a Web Application on page 69.
- **Task**. Create a new governance task as described in Creating a Task on page 200
- **Other Resource**. Create a new resource artifact as described in Publishing Definition Resources on page 184.

- **Lifecycle**. Accesses the lifecycle features described in Managing the Service Lifecycle on page 77.
- **Registry Content**. Import entities from a UDDI registry as described in Importing Data From a Registry on page 210.
- **Recent Documents**. Links to the last few viewed artifacts.

Catalog Browser

The **Catalog Browser** is the entry point to the repository. From here all artifacts in the repository can be viewed:

Figure 36. Catalog Browser Portlet



The browser is split into the following sections matching the structure of the SDM described in the Artifacts Taxonomy section in the HP SOA Systinet Reference Guide:

- **SOA** contains the artifact types for business services, their implementation and policies.
- **Content** contains the artifact types normally associated with services such as documentation and metadata.
- **System** contains the artifact types related to integration and governance tools and tasks.

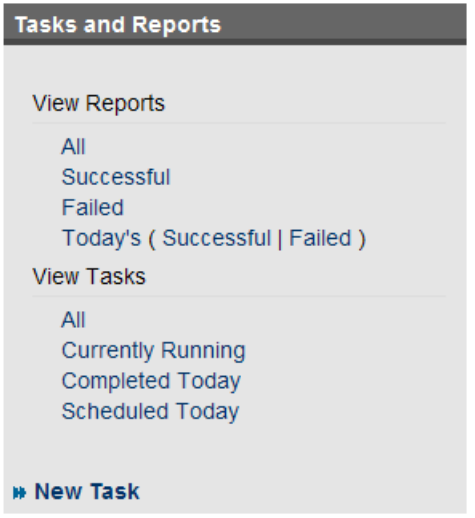
To expand branches in the browser, click **[+]**.

Double-click an artifact type to open its browse page.

Tasks and Reports Portlet

The **Tasks and Reports** portlet on the **Tools** and **Dashboard** (administrator perspective only) tabs is the quickest access point to your SOA governance tasks and the results of their execution.

Figure 37. Tasks and Reports Portlet



The portlet includes the following sections:

- **View Reports** enables you to view reports according to the following categories:
  - **All** displays all the reports in the repository, as described in Reports on page 203.
  - **Successful** opens a browse view of all successful reports.
  - **Failed** opens a browse view of all failed reports.
  - **Today's** opens a browse view of all reports created today, today's successful reports, or today's failed reports.

- **View Tasks** enables you to view tasks according to the following categories:
  - **All** opens a browse view of all tasks in the repository.
  - **Currently Running** opens a browse view of tasks currently being executed.
  - **Completed Today** opens a browse view of all tasks completed today.
  - **Scheduled Today** opens a browse view of all tasks scheduled today.
- **New Task**. Click to create a new governance task, as described in Creating a Task on page 200.

Closing the portlet in the **Dashboard** adds a link to the **Add** section of the dashboard menu enabling you to restore the portlet to the **Dashboard** at any time.

Report Launcher Portlet

The **Tools** tab contains a portlet specifically for reports generated by reporting tools. It contains default tools created by HP Systinet and user created tools with valid URIs.

Figure 38. Report Launcher Portlet

Click the report name to open the last report of its execution in html format.

Click **pdf**, **doc** or **xls** to view the report in that format.

generate executes the tool and switches to a view of the newly generated report.

configure opens the detail view of the associated reporting tool. Click **Edit** to make changes.

The default reporting tools are:

- **Service Consumption** generates an overview of the service consumption in the repository.
- **Service Lifecycle Statistics** generates a summary of how many services are at which stage in the service lifecycle.
- **Service Portfolio** generates an overview of the services in the repository.
- **Service Providers** generates an overview of the service providers in the repository.
- **Services Waiting for Approval** generates a summary of the services for which approval requests are required for current lifecycle stages, but no request has been sent.
- **Services with Pending Requests** generates a summary of the services by lifecycle stage with pending approval requests.
- **Top 10** generates a summary of the top consumers and publishers of services and the services with the most users.

Click **New Reporting Tool** to create a new reporting tool as described in Creating a Reporting Tool on page 194.

20 Tools Pages

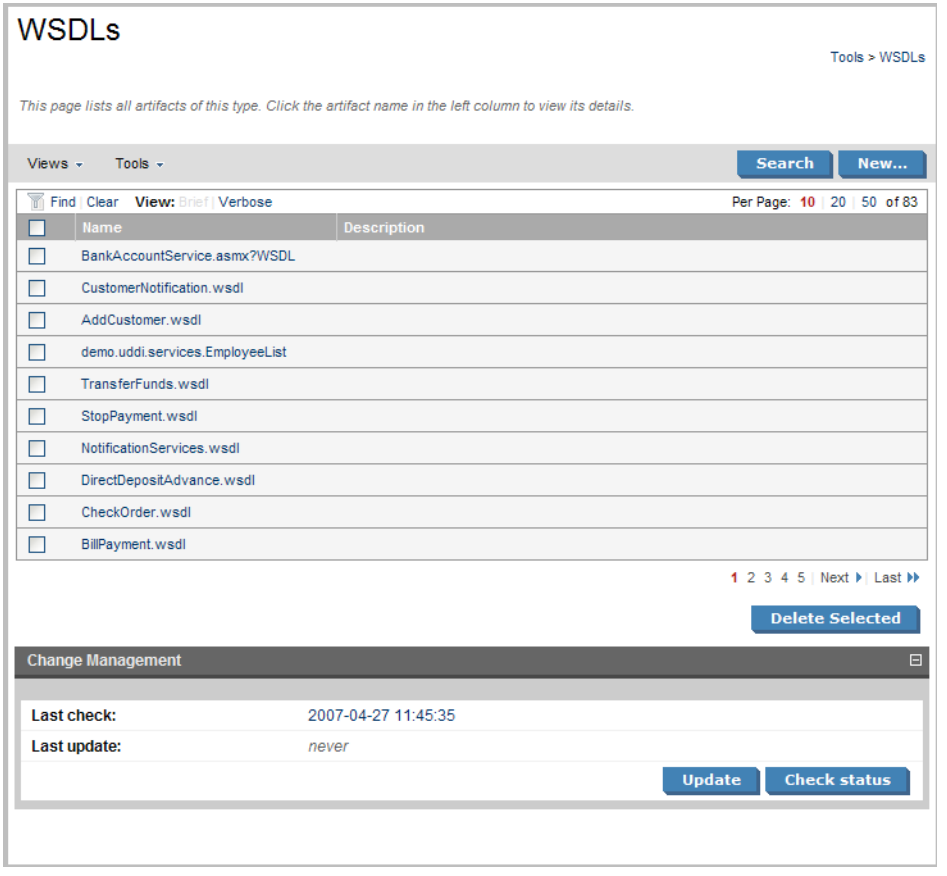
In the **Tools** tab there are a number of different pages describing the artifacts in the repository. This chapter describes:

- Browse Artifact Pages on page 167 are the index views of artifacts.
- Artifact Detail Pages on page 170 are the detailed view of artifacts in the repository.
- Navigator View on page 173 displays a graphical representation of an artifact and its relationships.
- Revision History on page 175 displays previous revisions of artifacts.

Browse Artifact Pages

Clicking an artifact type in the **Catalog Browser** in the **Tools** tab opens a browse artifact page:

Figure 39. Browse WSDLs Page



These pages list all the artifacts of the selected artifact type.

Click **New** to open a page allowing the creation of a new artifact or **Search** to start the advanced search page described in Stored Searches on page 205.

The grey bar contains a set of context action menus containing sets of actions that can alter the view of the collection or perform actions on the collection.

The actions may vary depending on the artifact but they include:

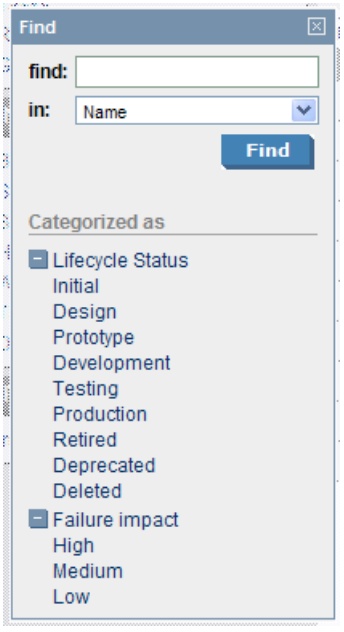
- **Views**:
  - **XML View** opens a XML view of the page in the REST interface.
  - **RSS View** opens an RSS view of the page that can be used to create an RSS content feed for the dashboard.
  - **Access Rights** opens a view of the access permissions for the artifact.
- **Tools**:
  - **Look for Deleted Artifacts** opens a browse view of deleted artifacts of this type with options to **Purge** or **Undelete** selected items.
- **Search** enables you to perform an advanced search within the artifact type, as described in Creating a Stored Search on page 205.
- **New** enables you to create a new artifact of this type as described in Creating an Artifact on page 178.

Each artifact has a checkbox which is used to select services for deletion using **Delete Selected**.

Click an artifact to open its detail view (see Artifact Detail Pages on page 170).

Click **Find** to filter the list by column headings or artifact categories:

Figure 40. Implementations Filter



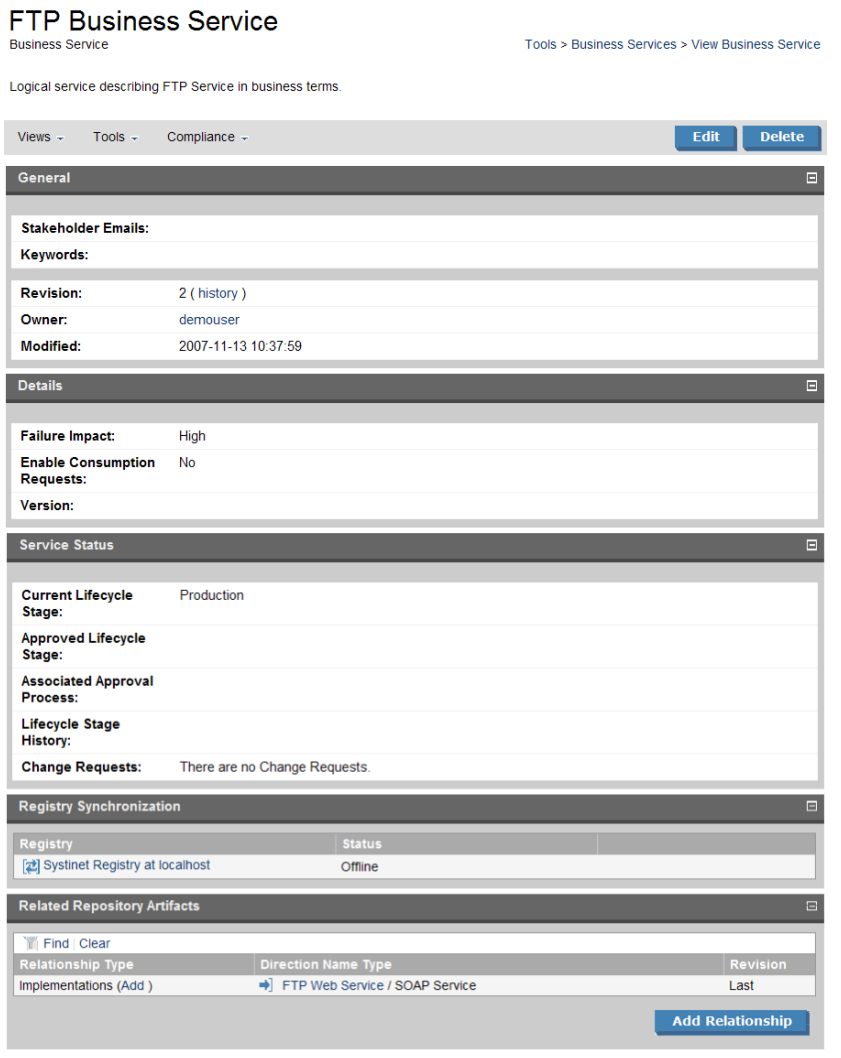
There are also clickable options to change the display settings of the page. You can switch between **Brief** or **Verbose** descriptions and change the number of artifacts to be displayed on each page.

Pages for artifacts linked to external documents have a **Change Management** section allowing you to synchronize your repository artifacts with the external documents. See Running the Change Management Tool on page 196 for more details.

Artifact Detail Pages

Clicking an artifact name opens a detailed artifact view containing all the information about that artifact with options to edit, delete and add relationships:

Figure 41. FTP Business Service Details



The grey bar contains a set of context action menus containing sets of actions that can alter the view of the artifact or perform governance actions.

The actions may vary depending on the artifact but they include:

- **Views**:
  - **Services View** opens a view of the artifact from the **Services** tab as described in Service View on page 56.
  - **Navigator View** opens a graphical representation of the artifact and its relationships, as described in Navigator View on page 173.
  - **Revisions** displays a list of the previous versions of the artifact as described in Revision History on page 175.
  - **Access Rights** opens a view of the access permissions for the artifact.
  - **XML View** opens a XML view of the page in the REST interface.
  - **RSS View** opens an RSS view of the page that can be used to create an RSS content feed for the dashboard.
- **Tools**:
  - **Associated Reports** views the reports related to this artifact as described in Reports on page 203.
  - **Dependency Analysis** and **Impact Analysis** execute the impact management tool on the artifact as described in Impact Tools on page 189.
  - **Add Documentation** creates a document relationship as described in Attaching Documentation to Artifacts on page 183.
  - **Change Owner** enables the administrator or owner of the artifact to transfer ownership to a different user, as described in Changing Artifact Ownership on page 180.
- **Compliance**:
  - **Validate Compliance** validates the artifact against all its associated business policies, generating an artifact index report as described in Document Summary Reports on page 110.

    - **Compliance Status** opens the results of the last compliance check as described in Report Views on page 107.
    - **Effective Policies**. View the business policies associated with the artifact.
    - **Reset Compliance Statistics** deletes the compliance reports associated with the artifact.

- **Edit** opens an edit view of the artifact enabling you to change it
- **Delete** gives the option to mark the artifact as deleted or to purge it completely from the repository..

Other information on the page varies, depending on the artifact type. Information categories include:

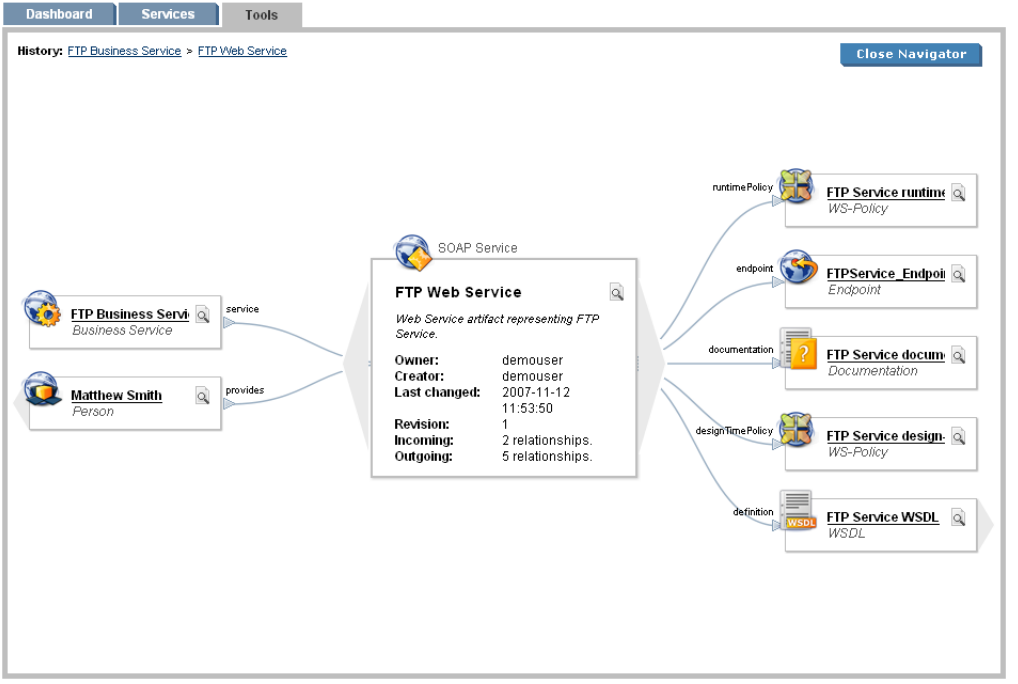
- **General** displays the taxonomic categories of the artifact, the version with a link to the revision history, the owner of the artifact and its last modified date.
- **Details** and **Service Status** contain lifecycle and failure impact information for service artifacts.
- **Data** is an extra section for artifacts associated with external documents. It contains a cached version of the external document and can be viewed by clicking the name of the external document.
- **Change Management** is an extra section for artifacts associated with external documents allowing you to synchronize the artifact with the external document. See Running the Change Management Tool on page 196 for more details.
- **Performance and Availability** is an extra section for service implementations showing service statistics from HP Business Availability Center and is described in BAC Integration Features on page 219.
- **Related Repository Artifacts** shows the relationships that the artifact has with other repository content. **Add Relationship** allows you to associate the artifact with another in the repository as described in Adding a Relationship on page 179.

Navigator View

The navigator view displays a graphical representation of an artifact and its relationships to other artifacts.

Access the navigator view from the service or tools view of an artifact. Select **Navigator View** from the **Views** menu.

Figure 42. Navigator View



The main section in the middle of the view displays details of the artifact. On the left are parent artifacts that the artifact depends on, and on the right are child artifacts that the artifact impacts on.

Click an artifact name to switch the navigator view to that artifact.

Click the magnifying glass icon of an artifact to switch to the detailed view of the artifact.

Click **Close Navigator** to go back to the detail view of the original artifact.

History displays the navigation history within the navigator view. Click an artifact name to switch to that artifact.

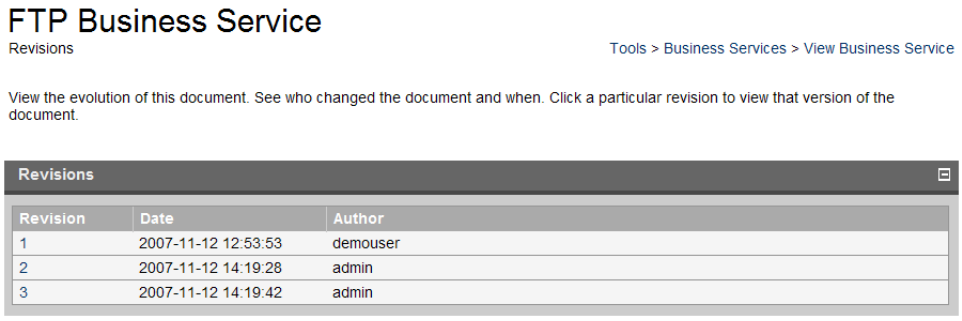
Revision History

During the lifecycle of resources and artifacts stored in the database, their properties or content may change. SOA Systinet supports revisions. Any update of a resource automatically increments its revision number. A resource may be updated by the Change Management Tool or by a user changing any property such as the name, description, etc.

To view the revision history of an artifact:

- In the detail view of an artifact click **history**, next to the revision number, in the **General** section or **Revision History** in the **View** context menu.
- Alternatively, in the service view of an artifact click **Revision History** in the **View** context menu.

Figure 43. FTP Business Service Revision History



To view the content of a past revision, click the revision number.

Click **Latest Revision** to view the latest revision of the artifact.

If you need to restore the artifact to this past revision, the context action **Copy as New Revision** is available in the **Views** menu. A new revision of the resource will be created with the content of the old revision you are viewing.

21 Managing Content

There are four main types of content in SOA Systinet

- **Artifacts**. All entities in the repository are artifacts and there are generic procedures for most artifacts described in Managing Artifacts on page 177.
- **Documentation**. Many artifacts require additional documents describing their purpose or use. Managing Documentation on page 181 describes the procedures for adding and using documentation.
- **Metadata**. Information about the structure and format of the data in your repository can also be published as described in Managing Definition Data on page 184.
- **Taxonomies**. Using categorization groups allows you to further organize the content of your repository. The SOA Systinet UI can be used to manage taxonomies in the same way as other artifacts but we recommend using HP SOA Systinet Taxonomy Editor.

Publishing a SOAP Service from WSDL on page 186 is a procedure describing the creation of a service implementation using a WSDL specification document.

Managing Artifacts

The main artifact management procedures are:

- Create a new artifact as described in Creating an Artifact on page 178.
- Edit an artifact as described in Editing an Artifact on page 178.
- Delete an artifact as described in Deleting an Artifact on page 179.
- Add a relationship to another artifact as described in Adding a Relationship on page 179.
- Change the ownership of an artifact as described in Changing Artifact Ownership on page 180.

Creating an Artifact

The process of creating an artifact is very similar for most artifact types.

To create an artifact:

1. From the browse page of any artifact type, click **New** to start the artifact creation process.
2. The exact details for each artifact type will differ, but in general, there are two types of artifact:
   - Representational artifacts are those that are created for the purpose of managing your SOA such as the business service artifact.
   - Imported artifacts are those created with an association with an external document such as WSDL artifacts.

   Input the artifact details, and then click **Finish** to create a representational artifact or **Next** to create an imported artifact with an associated external document.
3. Choose the data attachment method, and then click **Next**.
4. For **Upload file from your local filesystem** use **Browse** to select the file from your system.

   For **Download the file from a URL** input the URL location of the file.
5. Click **Save** to create the new artifact and upload the external document.

Editing an Artifact

To edit an artifact:

1. In the detail view of an artifact, click **Edit** to open the edit view of the artifact.
2. Change any parameters and use the functionality in the **Related Repository Artifacts** section to manage relationships.
3. Click **Save** to commit your changes and create a new revision of the artifact. See Revision History on page 175 for details.

Deleting an Artifact

Artifacts can be deleted either from the **Browse Page** or from the **detail view** (see Browse Artifact Pages on page 167 or Artifact Detail Pages on page 170):

- In browse pages select the artifacts to delete and click **Delete Selected**.
- In detail views, click **Delete**.

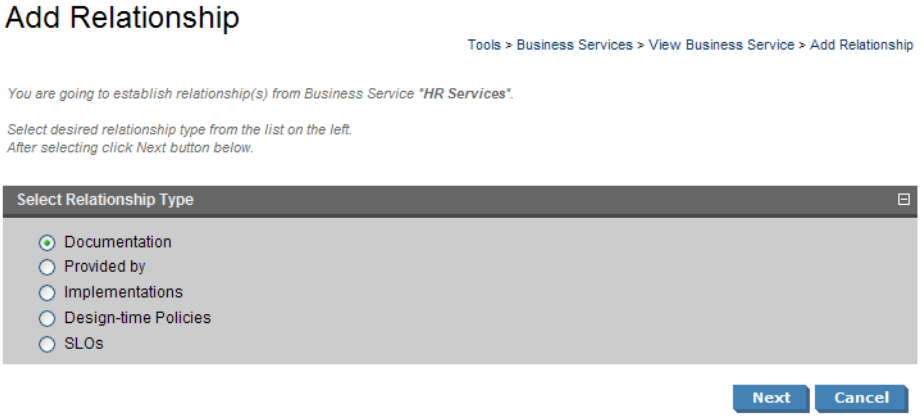
Both options open a confirmation page with options to **Delete** or **Purge** the artifact. Purge removes the artifact from the repository, whereas delete marks the artifact as deleted, allowing you to restore it at a later date.

Adding a Relationship

At the heart of SOA Systinet is the ability to link artifacts together with relationships.

To add a relationship to an artifact:

1 Click **Add Relationship** in any detail view to open the **Add Relationship** page:



There are numerous types of relationships, the choices available depend on the particular artifact type.

2 Select the relationship type and click **Next**.

3 The format of this choice will depend on the artifact and relationship type.

Do one of the following:

- Select an option from the drop-down list.
- Use **Find** function to search for the required artifact. Check the box next to the artifact name to select it.
- Click **New** to create a new artifact to be the object of the relationship as described in Creating an Artifact on page 178.

Click **Next** to continue.

4 Review the details and click **Finish** to create both the relationship and the inverse relationship.

Changing Artifact Ownership

An administrator or the owner of an artifact can change the ownership to another user.

To change the owner of an artifact:

1 In the **Tools** detail view or the **Services** view of an artifact, select **Change Owner** from the **Tools** context menu.

The **Change Owner** page appears.

2 For business services there is an extra option to change the ownership of related artifacts. For other artifact types skip to Step 3. Expand the tree of artifacts and de-select any related artifacts that do not require the ownership change.

Note: Artifact owners are only shown related artifacts that they own.

Click **Next** to continue.

3 Use the search feature to generate a list of users.

4 Select a user from the list, and then click **Next**.

5 Review the details and click **Finish** to confirm the artifact ownership change. If **Send Notification E-Mails** is selected then you, the original owner, and the new owner are notified of the change.

Managing Documentation

The main document management procedures are:

- Add a new document to the repository as described in Adding Documentation on page 181.
- Attach documentation to an artifact as described in Attaching Documentation to Artifacts on page 183.
- Edit the source document as described in Editing Documentation on page 183.

Adding Documentation

You may want to store documents in the SOA Systinet repository or create documentation artifacts linked to external documents.

To create a new documentation artifact:

1 In the **Catalog Browser** click **Documentation** to open the **Browse Documentation** page.

2 Click **New** to start the publish documentation dialog.

3 There are the following options:

- **From Local File** – to upload a document from your local filesystem.
- **From Remote File** – to upload a document from a remote location.
- **Link to a remote file** – to create a link to a document on a remote location.
- **Empty Documentation** – to create a documentation artifact without cached content or a link to an external document.

Select an option and click **Next**.

4 For the local file option complete the form with parameters:

Parameter	Definition
File	Use **Browse** to specify the document on your local system
Type	Select a document type from the drop-down list
Name	Input a name for the documentation artifact
Description	Input a description for the documentation artifact

For the remote file option complete the form with parameters:

Parameter	Definition
URLs	A list of locations of documents to add to the repository
Apply Synchronization Policy	Check the box to apply a synchronization policy (see Synchronization Policy on page 196 for more details).
Synchronization Policy Type	Select **Automatic** or **Manual**

For the link to remote file option complete the form with parameters:

Parameter	Definition
URL	The locations of document to link the new artifact to
Type	Select a document type from the drop-down list
Name	The name of the new artifact
Description	A description for the new artifact

The empty documentation option creates a documentation artifact without any associated external document. Complete the page with parameters:

Parameter	Definition
Name	The name for the new documentation artifact
Description	A description of the new documentation artifact
Type	Select a document type from the drop-down list
Categories	Click **add category** to select a category from the available taxonomies (administrator perspective only)

5 Click **Save** to create the new documentation artifact.

Attaching Documentation to Artifacts

Once a documentation item is stored in the repository it can be attached to other repository resources with a documentation relationship.

To attach a document to an artifact:

1 In the detail view of the artifact click **Add Relationship**.

2 Select **Documentation** and click **Next**.

Note: Not all artifacts have **Documentation** as an available relationship type.

3 Use **Find** to search for the required document or click **New** to import a new document as described in Adding Documentation on page 181. Select the document and click **Next**.

4 Review the relationship and click **Finish** to create it.

If you later want to detach documentation from the artifact, edit the artifact and remove the relationship as described in Editing an Artifact on page 178.

Note: This procedure can be used to add documentation to a business service but an alternative is provided in the **Services** tab as described in Adding Service Documentation on page 63.

Editing Documentation

Both the properties and the source of a documentation artifact can be edited.

To edit a documentation artifact:

1 In the detail view of the documentation artifact click **Edit**.

2 Change any artifact attributes as required.

To change the external source document:

1. In the **Data** section click **change**.
2. Use **Browse** to select a new source document.
3. Click **Save** to upload the new document.

3. Click **Save** to confirm your changes.

Managing Definition Data

SOA Systinet includes extended support for SOA specific resources, such as WSDL documents and XML schemas. This support includes features such as automatic import resolution during publishing and updates, and change management support based on synchronization policies.

Supported metadata formats are:

- WSDL documents
- XML schema documents
- DTD documents
- XSLT stylesheets

This section describes:

- Adding definition documents to the repository in Publishing Definition Resources on page 184.
- Updating definition attributes or their source in Updating Published Metadata on page 186.

Publishing Definition Resources

SOA Systinet includes functionality to make use of the definition data contained in resources such as WSDL documents.

To publish a resource artifact:

1 In the **New** section of the tools menu click **Other Resource** to open the **Publish WSDL, XSLT, XSD or DTD documents** dialog.

2 Complete the dialog with parameters:

Parameter	Definition
URLs	A list of locations of documents to add to the repository
Apply Synchronization Policy	Check the box if you want to set a synchronization policy
Synchronization Policy Type	Set **Automatic** or **Manual** (see Synchronization Policy on page 196 for more details)

3 Click **Finish** to start the publishing process for each resource in the list.

The resource document publishing process then performs the following steps:

1 Each document downloads from its original location URL.

2 The type of document is assessed based on the content of the document and the appropriate type of artifact is created.

3 The repository is searched for a document of the same type with the same value origin URL, if such a document is found it is checked for changes and if changed it is updated.

4 The content of the document is searched for possible references (WSDL, schema includes/imports or other referenced data) to other documents, each referenced document downloads and processes with the same sequence of steps.

5 Finally, the document is stored in the repository, and a relationship is created for each referenced resource.

The name of the stored document is set to the last part of its URL and the origin URL attribute is populated.

Note: An alternative process is to upload a metadata document in the same way as described in Adding Documentation on page 181. In the procedure replace documentation with the relevant metadata artifact type.

Updating Published Metadata

Metadata documents are updated and edited in the same way as documents as described in Editing Documentation on page 183. In the procedure replace documentation with the relevant metadata artifact type.

Publishing a SOAP Service from WSDL

SOA Systinet enables you to uses a WSDL document to publish a SOAP service.

To publish a SOAP service from a WSDL:

1 In the **New** section of the tools menu click **SOAP Service from WSDL**.

2 Select one of the **Upload from** options:

- Local File
- Remote File

3 Do one of the following:

Note: You can specify a `.zip` folder containing multiple files. Publication resolves and uploads all WSDLs and related files.

- For the local filesystem option use **Browse** to specify the WSDL on your local system.
- For the URL option complete the form with parameters:

Parameter	Definition
URL	The location of the WSDL document to add to the repository

Parameter	Definition
Apply Synchronization Policy	Check the box to apply a synchronization policy (see Synchronization Policy on page 196 for more details).
Synchronization Policy Type	Select **Automatic** or **Manual**

4 Click **Next** to continue.

5 Optionally, amend the new service name and description and click **Next**.

6 Confirm the items to be created, and then click **Finish**.

After confirmation SOA Systinet displays a list of the newly created artifacts. Click an artifact name to view its details.

22 SOA Utilities

SOA utilities in the **Tools** tab consist of three elements:

- Tools on page 189 are the basic utilities for performing governance actions.
- Tasks and Scheduling on page 200 enable the use of a tool on an artifact or set of artifacts with the option of periodic or scheduled execution.
- Reports on page 203 are the result of a task or tool execution.

Tools

SOA Systinet provides the following types of utility in the **Tools** tab:

- Impact Tools on page 189 report the potential impact of a change to an artifact on the other artifacts it depends on or impacts.
- Job Tools on page 192 are customized tools created to perform miscellaneous tasks.
- Reporting Tools on page 193 use customized reports to query the repository.
- Sync Tools on page 195 update the repository with the latest versions of externally sourced documents.
- Policy Compliance Tools on page 200 verify whether artifacts conform to business policy.

Impact Tools

Impact tools enable you to report on all the related artifacts that may be impacted by a change to a specific artifact. Using impact tools, you can check the dependency trees or impact trees of an artifact.

In SOA Systinet, a dependency between artifacts is represented by a relationship. Each relationship represents a dependency between two related artifacts: a source artifact and a target artifact. A relationship is a unidirectional concept. Each relationship contains references to the source artifact, target artifact, type of

relationship and several other attributes. For example, consider relationship R which has references to source artifact A and target artifact B. This would mean that artifact A depends on artifact B and that artifact B has impact on artifact A. Accordingly, there are two types of relationship tree: the impact tree and the dependency tree. The impact tree of an artifact shows the artifacts that it has impact on. The dependency tree shows the artifacts on which this artifact depends.

You can create new impact tools or use the **Impact Management** tool provided with SOA Systinet.

This section describes:

Running the Impact Management Tool

The context action for the Impact Management Tool is available in the detail view and service view of artifacts (see Artifact Detail Pages on page 170 or Service View on page 56).

To assess the impact of a change to an artifact:

- In the detail view or service view of the artifact, move the cursor over the **Tools** context menu and select **Impact Analysis** or **Dependency Analysis** depending on which tool you want to execute.

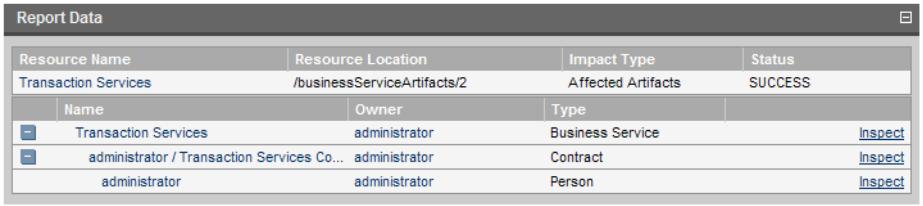
Impact Reports

Impact reports are generated by running the impact tool as described in Running the Impact Management Tool on page 190 or the result of automated tasks as described in Tasks and Scheduling on page 200.

To access impact reports, browse the reports as described in Reports on page 203 and filter for report category **Impact Management**.

The most important part of the impact report is the **Report Data** section:

Figure 44. Impact Report Data



The first part of the report data section displays the source resource of the impact report, the location of the raw report data, the type of report and the report status.

The second part of the report displays a hierarchy of affected artifacts, either impacted or dependent artifacts according to the report type.

Creating an Impact Tool

Impact tools enable you to assess the potential impact of a change to an artifact.

To create a new impact tool artifact:

1 In the **Catalog Browser**, click **[+]** next to **Tools** to expand it and show the list of tool types.

2 Click **Impact Tools** to open the **Browse Impact Tools** page.

3 Click **New** to open the **Publish Impact Tool** dialog.

4 Input the following parameters:

Parameter	Definition
Name	The name for the new impact tool
Description	A description of the impact tool
Choose impact type	Select one of the available impact types

5 Click **Save** to create the new impact tool.

This new impact tool is now available for selection when creating a task, as described in Creating a Task on page 200.

Job Tools

Job tools enable you to use customized Java class implementations to perform a variety of actions.

You can create new job tools or use the **Report Cleaner Job Tool** provided with SOA Systinet.

This section describes:

Creating a Job Tool

SOA Systinet enables you to create miscellaneous tools in association with your own Java classes.

To create a new job tool artifact:

1. In the **Catalog Browser**, click **[+]** next to **Tools** to expand it and show the list of tool types.
2. Click **Job Tools** to open the **Browse Job Tools** page.
3. Click **New** to open the **Publish Job Tool** dialog.
4. Input the following parameters:

Parameter	Definition
Name	The name for the new job tool
Description	A description of the job tool
Categories	Click **add category** to select a category from the available taxonomies (administrator perspective only)
Job Implementation Class ID	The class ID in the server configuration

5 Click **Save** to create the job tool.

This new job tool is now available for selection when creating a task, as described in Creating a Task on page 200.

Report Cleaner Job Tool

SOA Systinet is installed with the report cleaner tool. This tool is a utility for purging the repository of deleted and orphaned reports. HP Systinet recommend that a task be created to run this tool on a periodic basis to ensure that the repository does not fill up with obsolete reports. See Tasks and Scheduling on page 200 for details.

Reporting Tools

Reporting tools enable you to access customized reports stored on the reporting server for the purpose of periodic or timed execution using tasks.

SOA Systinet comes provided with preinstalled reporting tools which are available in the **Report Launcher** portlet (see Report Launcher Portlet on page 163).

This section describes:

Running a Reporting Tool

The context action for reporting tools is available in the **Report Launcher** portlet for the default reporting tools provided with SOA Systinet and any user created tools with valid URIs.

To execute a reporting tool:

1 In the **Report Launcher** portlet click **Generate** for the required reporting tool.

2 The view switches to the resulting report as described in Reporting Tool Reports on page 194.

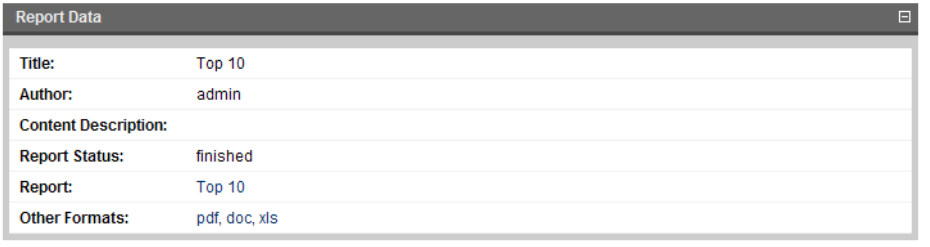
Reporting Tool Reports

Reporting tool reports are generated by running one of the default reporting tools as described in Running a Reporting Tool on page 193 or the result of automated tasks as described in Tasks and Scheduling on page 200.

To access reporting tool reports, browse the reports as described in Reports on page 203 and filter for report category **Reporting**.

The most important part of the impact report is the **Report Data** section:

Figure 45. Reporting Tool Report Data



This section provides progress and success details of the report and links to rendered versions of the report on the reporting server.

Creating a Reporting Tool

Reporting tools enable you to utilize custom reports deployed to the reporting server.

The SOA Systinet Report Editor can be used to create and modify report definitions. After these definitions are deployed to the reporting service, they are then available to be associated with a reporting tool. See the SOA Systinet Report Editor documentation for more information.

To create a reporting tool artifact:

1. In the **Catalog Browser**, click **[+]** next to **Tools** to expand it and show the list of tool types.
2. Click **Reporting Tools** to open the **Browse Reporting Tools** page.

3 Click **New** to open the **Publish Reporting Tool** dialog

4 Input the following parameters:

Parameter	Definition
Name	The name for the new reporting tool
Description	A description of the reporting tool
Categories	Click **add category** to select a category from the available taxonomies (administrator perspective only)
Report Definition	Select from the list of available report definitions from the reporting service
Additional Parameters	Depending on the report definition additional parameters may be input

5 Click **Save** to create the new reporting tool.

This new reporting tool is now available for selection when creating a task, as described in Creating a Task on page 200, or for immediate execution as described in Running a Reporting Tool on page 193.

Sync Tools

SOA Systinet stores all resources in its repository. They can be divided into two types: representational artifacts and local copies of imported resources. Sync tools focus on these imported resources. Such resources have a cached flag set and the origin URL associated with them. Sync tools are a powerful feature that make it possible to keep track of original resources, notifying the user about changes to them and maintaining up-to-date copies.

You can create new sync tools or use the **Change Management** tool provided with SOA Systinet.

This section describes:

Synchronization Policy

Externally sourced resources may have an associated synchronization policy. Automatic change management uses this policy to determine the action that should be performed during synchronization.

The following options are available:

- **None**. The cached resources will not be updated, except by a manual update of a single resource from a context action.
- **Automatic**. The cached resource is updated automatically if the original resource is changed.

Note: In order for automatic synchronization to function you must create a scheduled change management task. See Tasks and Scheduling on page 200 for details.

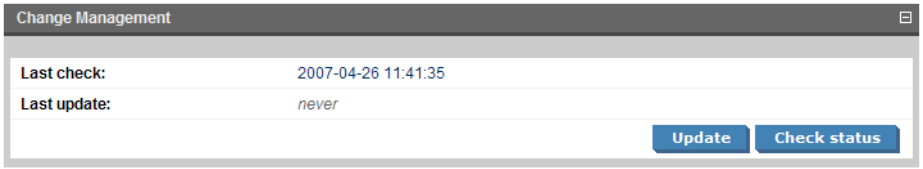
- **Approval Required**. The resource is marked with an out-of-sync flag and only updated after user approval. If you want to approve the change and update the document, run the change management tool as described in Running the Change Management Tool on page 196.

Note: Resources stored in a database may (and usually do) consist of imports of other resources. For example a WSDL file may contain imports of other WSDLs and XSDs. XSDs may contain imports of other XSDs or DTDs, etc. The result is a dependency tree with the WSDL that the user wants to publish or update at its root. The synchronization policy is usually associated with the root resource, but it is also applied to the other dependent resources in the tree.

Running the Change Management Tool

All artifacts that can be checked or updated have an associated change management section in their **browse artifact** and **detail view** pages. These include WSDLs, XSDs, DTDs and documentation. Change management context actions are available for single artifacts or for whole collections.

Figure 46. Change Management Section



Two actions can be performed on artifacts associated with external documents. Their behavior is as follows:

For a single artifact:

- **Update**. Updates a cached resource if the original has changed.
- **Check Status**. Only checks the resource status and sets the out-of-sync flag if the resource has been changed or is currently unreachable.

For a collection:

- **Update**. Shows all `out-of-sync` resources in a collection. You may approve synchronization for some resources and click **Finish** to complete the update.
- **Check Status**. Checks all resources with an associated synchronization policy. All resources that are found to be changed or unreachable are marked with the `out-of-sync` flag.

Important: When performing change management on a collection, only resources with an associated synchronization policy are checked or updated. If change management is performed on a single resource, the synchronization policy is not taken into account. Only resources for which you have write permission are checked or updated.

The dates of the last status check and last update access the latest reports as described in Change Management Reports on page 198.

Change Management Reports

Change management reports are generated by running the change management tool as described in Running the Change Management Tool on page 196 or the result of automated tasks as described in Tasks and Scheduling on page 200.

To access change management reports, browse the reports as described in Reports on page 203 and filter for report category **Change Management** or from the **Change Management** section of **browse view** or **detail view** pages as described in Running the Change Management Tool on page 196.

Select one of these by clicking the name to view the index report for that change management execution.

To view the result for a particular artifact, in the **Sub reports** section click the **Change Management Report** link for the artifact you are interested in.

The most important part of the change management report for an artifact is the **Report Data** section:

Figure 47. Change Management Report Data

This section displays the name of the artifact, its location in the repository and the location of the external document it represents and the status of the update or status check.

The possible statuses are:

Status	Definition
NEW	The resource is new
IDENTICAL	The cached resource was identical to the original
IDENTICAL (NO-PERMISSION)	The cached resource was identical to the original and the current user does not have permission to change it
UNREACHABLE	The original resource is unreachable, possibly due to a network error, or because the server is not running

Status	Definition
OUT-OF-SYNC	The cached resource differed from the original and was not updated. Root resources with imports (complex resources) are also set to out-of-sync if any of the imported resources is new, out-of-sync or unreachable
UPDATED	The cached resource differed from the original and was updated
CHANGED-IGNORED	The cached resource differed from the original but was not updated
CHANGED-IGNORED (NO-PERMISSION)	The cached resource differed from the original but was not updated because the current user does not have permission
CHANGED-IGNORED (UNEXPECTED-CONTENT)	The resource was not updated, because unexpected content was retrieved from the original location (for example badly formed xml)
NO-PERMISSION	The current user does not have permission to change this resource
UNKNOWN	The state was unknown

Creating a Sync Tool

Sync tools enable you to track changes to external documents associated with artifacts in the repository.

To create a sync tool artifact:

1 In the **Catalog Browser**, click **[+]** next to **Tools** to expand it and show the list of tool types.

2 Click **Sync Tools** to open the **Browse Sync Tools** page.

3 Click **New** to open the **Publish Sync Tool** dialog.

4 Input the following parameters:

Parameter	Definition
Name	The name for the new sync tool
Description	A description of the sync tool
Categories	Click **add category** to select a category from the available taxonomies (administrator perspective only)

5 Click **Save** to create the new sync tool.

This new impact tool is now available for selection when creating a task, as described in Creating a Task on page 200.

Policy Compliance Tools

Policy compliance tools validate whether artifacts conform with the requirements of one or more business policies.

Perform a compliance check using the provided **Validate Compliance** tool and the reports generated are described in detail in Validating Documents on page 137.

Tasks and Scheduling

A *task* is an artifact which associates other artifacts or resources with a tool. You can imagine it as a tool prepared for execution. A task is powerful way of performing an action on the same set of resources repeatedly. The specified resources are used as input when the tool is run. A task can be run manually but it is more usual to schedule automatic execution.

This section describes:

Creating a Task

Tasks are the way SOA Systinet associates a particular tool with a set of artifacts to produce reports.

To create a new task:

1 Do one of the following:

- In the tools menu, in the **New** section, click **Task**.
- Alternatively, in the **Tools** tab, in the **Tasks and Reports** portlet (see Tasks and Reports Portlet on page 162), click **New Task**.

- Alternatively, in the browse view of tasks click **New**.

The **Publish Task** page appears.

2 Use **Find** to search for the tool to associate with the task. Select the tool, and then click **Next** to select the artifacts to examine.

3 The selector page includes the following options:

- For collections select an artifact type collection from the drop-down list.
- For documents use **Find** to locate the documentation artifacts to associate with the task and check the radio button to select them, or click **Add Documents** and follow the wizard to select documents from a selected collection.
- For stored searches use **Find** to locate the stored search containing the artifacts to associate with the task and check the radio button to select it.

Note: Some tools do not require the selection of artifacts. For example, the report cleaner tool.

Click **Next** to set scheduling.

4 If you want this task to be executed at a set time or repeated on a periodic basis select **Scheduled**, complete the details as described in Setting a Schedule on page 201, and then click **Next** to set the task artifact name.

5 Optionally, edit the suggested name and description, and then click **Finish** to create the new task.

Setting a Schedule

SOA Systinet enables you to execute tasks on a timed or periodic basis.

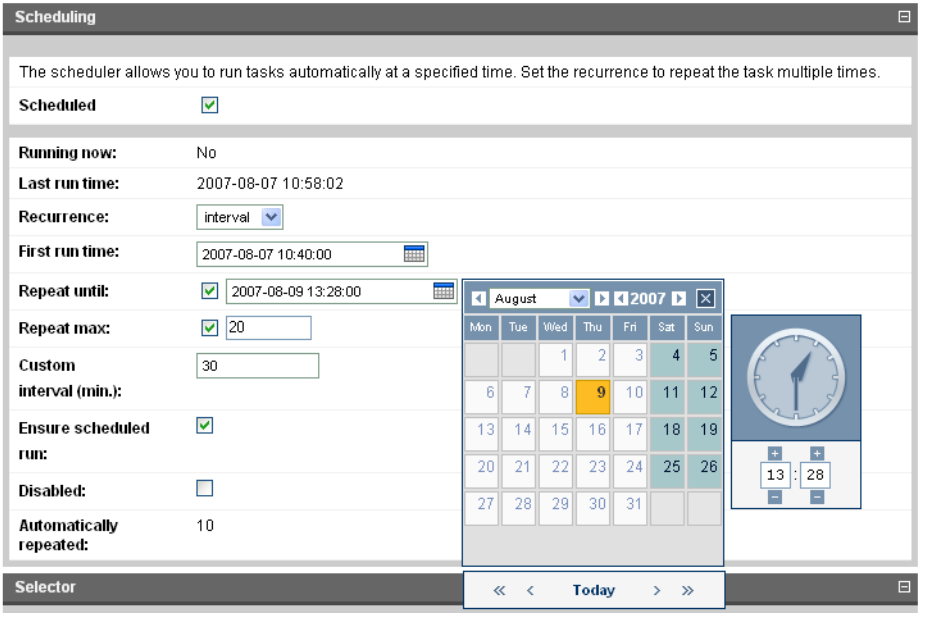
To schedule a task:

1 Do one of the following:

- In the detail view of the task click **Edit**, and then select **Scheduled**.

- Alternatively, select **Scheduled** during task creation as described in Creating a Task on page 200.

The schedule parameters appear:



2 Input the following parameters:

Parameter	Definition
Running now	A non-input field indicating whether the task is currently being executed
Last run time	The last execution time of the task
Recurrence	Select the frequency of execution if the task is to run periodically or **none** if the task is to be executed once
First run time	Use the calendar to set the date and time for the initial execution of the task
Repeat Until	If the task has a recurrence, optionally select **Repeat Until**, and use the calendar to select the date and time to stop executing the task.

Parameter	Definition
Repeat max	If the task has a recurrence, optionally select **Repeat Max**, and input the number of times to execute the task. This figure is compared to the **Automatically Repeated** figure to determine whether to execute the task again.
Custom Interval (min.)	If the task has the **Interval** recurrence, input the interval.
Ensure scheduled run	Select to prioritize scheduled execution. If for any reason the task cannot execute at the scheduled time (for example, if the server is not running), then the task executes at the at the earliest opportunity. HP Systinet recommend selecting this option for tasks with long recurrence intervals.
Disabled	Select to prevent the automatic execution of the task
Automatically repeated	Displays the number of scheduled executions (not including manual executions).  To reset this figure, remove the schedule and then create a new schedule.

3 Do one of the following:

- If you are editing a task, click **Save**.
- If you are creating a task, click **Next** and continue as described in Creating a Task on page 200.

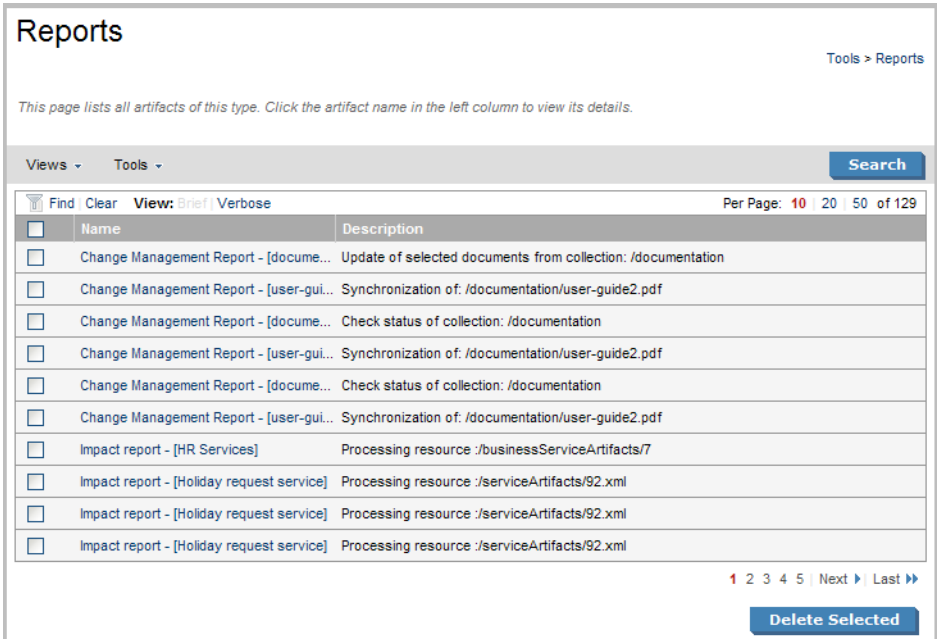
Reports

The result of a tool execution is a report. Reports are accessible from:

- The **Reports** link in the **Catalog Browser**.
- The **Tasks and Reports** portlet in the **Dashboard** and **Tools** tabs
- The **Tools** context menu in the **detail view** and **service view** of an artifact.

Clicking any of these links opens a report list view:

Figure 48. Reports List View



Find allows reports to be filtered according to various categories. Simply select the category and the browser only shows the reports which fulfill the given criteria.

The **Report Data** section contains output specific to each type of tool and is described in the report section of each tool in Tools on page 189.

23 Stored Searches

You can use SOA Systinet to create customized queries that search the repository. These searches can be stored and then reused. Stored searches can also be used to define a set of artifacts associated with a task or used to create an RSS feed for the dashboard.

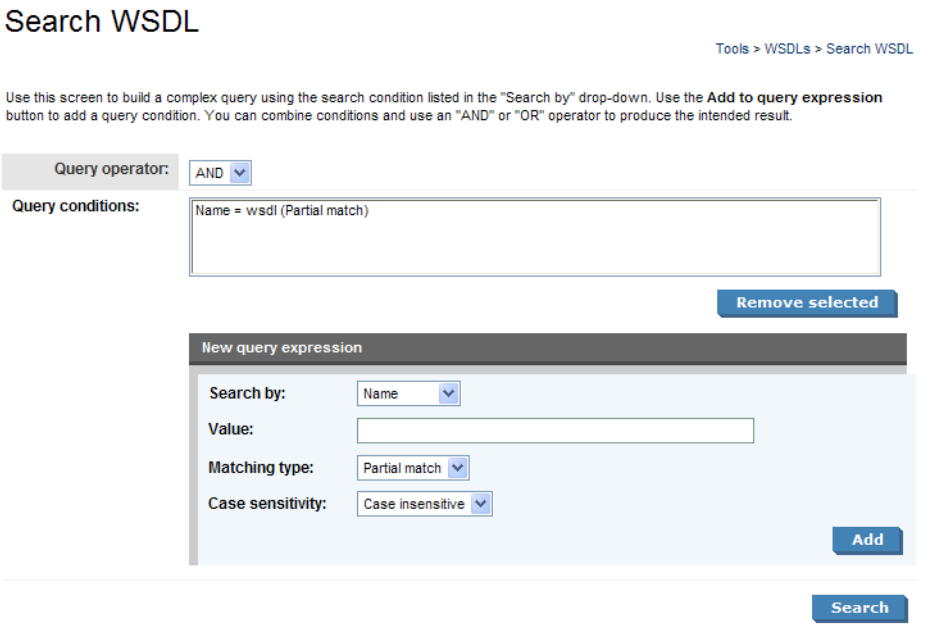
This chapter describes:

Creating a Stored Search

Each stored search is associated with one type of artifact.

To create a stored search:

1 In the browse view of an artifact type click **Search** to open the search page for that artifact type:



2 Input the search parameters in the **New query expression** section:

Parameter	Definition
Search by	Select the artifact property to search from the drop-down list **Note:** The options available depend on the artifact type.
Value	Input the value to search for
Matching type	Select the search type from the drop-down list with options: • **Partial Match.** Search for items containing the search string • **Equals.** Search for items identical to the search string

Parameter	Definition
Case sensitivity	Select whether the search is case sensitive or insensitive

3 Click **Add** to add the expression to **Query conditions**.

4 Optionally, select a **Query operator** and add more query expressions.

5 Click **Search** to run your query and view the results.

6 Optionally, use **Find** to filter the results.

7 Optionally, to store the search for later use, click **Store search** to open the **Publish Stored Search** page.

8 If you are storing the search for later use, amend the search name, description, and details, and then click **Save** to create the new stored search artifact.

Stored search artifacts are displayed in the **Custom Views** section of the **Services** menu.

Editing a Stored Search

Although the stored search is persisted it can be modified again. There are two kinds of modification:

- Changing the name and description properties of the stored search.
- Changing the parameters of the search.

To edit the basic search properties:

1 In the detail view of the stored search, click **Edit**.

2 Change the properties as required, and then click **Save**.

To modify the search parameters:

1 In the detail view of the stored search, click **Redefine**.

2 Select a condition, and then click **Remove selected** to remove conditions from the query and add new conditions as described in Creating a Stored Search on page 205.

3 Click **Save** to confirm your changes.

Running a Stored Search

To execute a stored search do one of the following:

- In the detail view (see Artifact Detail Pages on page 170) of the stored search, click **Run**.
- In the **Services** menu, **Custom Views** section, click the name of the stored search.

24 Registry Integration

SOA Systinet provides customizable mapping between UDDI entities and SDM artifacts. Mapping of the basic structures (types) is predefined, but several aspects can be significantly changed by mapping additional artifact properties to UDDI keyed references and vice versa.

Important: Before any data transfer takes place between SOA Systinet and a UDDI registry, a registry artifact must be created, registry certificates must be imported to SOA Systinet, and the taxonomies must be synchronized. These procedures are described in the Registry Setup and Configuration section of the HP SOA Systinet Administration Guide.

SOA Systinet artifacts correspond to registry entities as follows:

SOA Systinet Artifact	Registry Entity
Organization unit	Business entity
Business service	tModel
Implementation	Business service
Endpoint	Binding template
Custom (WS-Policy)	tModel

This chapter describes:

Importing Data From a Registry

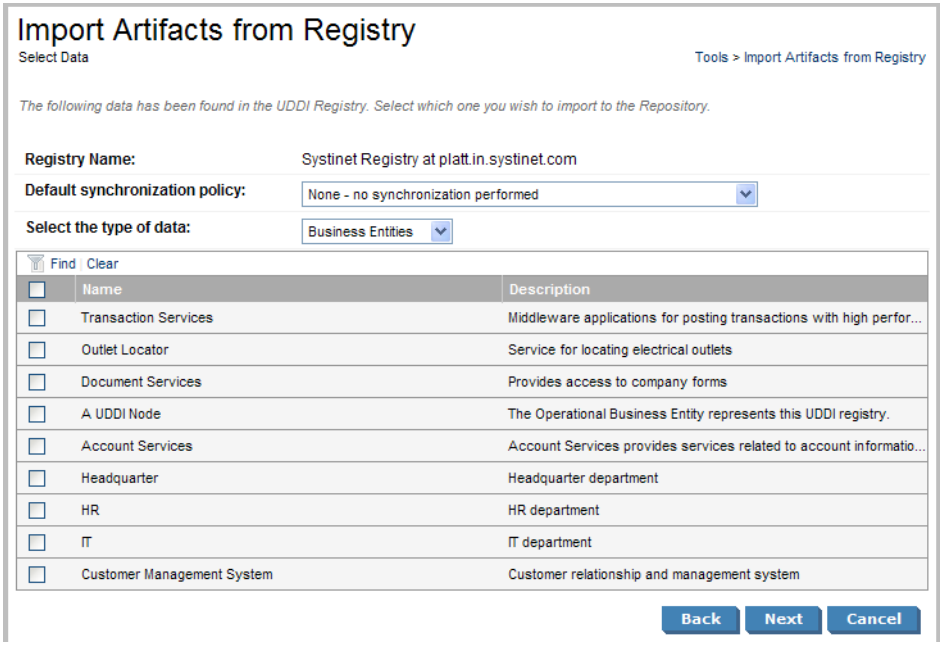
You can import services and associated entities from a registry.

To import data from a UDDI registry:

1 In the **Registry Content** section of the tools menu, click **Import Registry Content** to open the **Import Artifacts from Registry** page.

2 Select a registry from the drop-down list, or click **New** to create a new registry artifact as described in the Creating a Registry Artifact in the HP SOA Systinet Administration Guide.

Click **Next** to set the import details:



3 Input the following parameters:

Parameter	Definition
Registry Name	The target registry to import data from
Default synchronization policy	Select a policy from the drop-down list. For more details see Synchronization Policy on page 196
Select the type of data	Select entity type to populate the table

4 Use **Find** to filter that data set.

5 Select data from the registry to import and click **Next**.

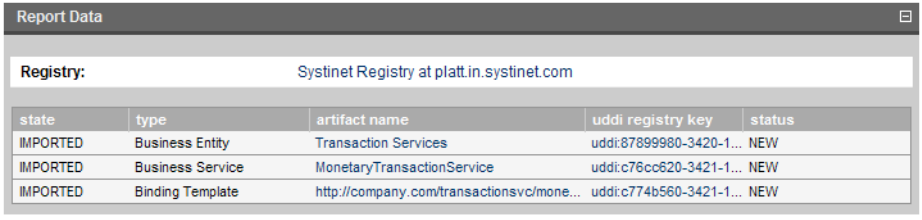
6 Verify the data to be imported on the summary page, and then click **Finish**.

Note: If you are importing a business entity, all its business services are imported as well, and if you are importing a business service, all its binding templates are also be imported. If a single business entity is imported then input a service name and description for the new business service artifact to associate with the imported items.

When the import process begins, an import report is created. This process takes some time so click **Refresh** every so often - you may have do this several times until the report is complete (and **Refresh** disappears).

When the import is complete, click one of the **Registry Import Reports** in the **Sub report** section to view the import report details for that entity.

The most important part of the report is the **Report Data** section:



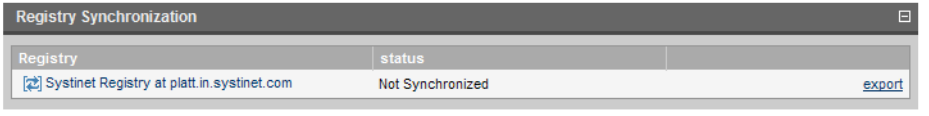
This report shows exactly what was imported, and the import status of all the imported items.

<table>
<tr><th>Parameter</th><th>Definition</th></tr>
<tr><td>state</td><td>
<table>
<tr><th>State</th><th>Description</th></tr>
<tr><td>IMPORTED</td><td>The item was successfully imported.</td></tr>
<tr><td>EXPORTED</td><td>The item was successfully exported.</td></tr>
<tr><td>DELETED</td><td>The item (Business Service or Binding Template) was deleted from the UDDI registry during export because the corresponding artifact had been deleted in HP SOA Systinet.</td></tr>
<tr><td>FAILED</td><td>An error occurred during the export/import of the item.</td></tr>
</table>
</td></tr>
<tr><td>type</td><td>The UDDI entity type: Business Entity, Business Service or Binding Template</td></tr>
<tr><td>artifact name</td><td>The SOA Systinet artifact name</td></tr>
<tr><td>uddi registry key</td><td>The unique id of the corresponding UDDI entity</td></tr>
<tr><td>status</td><td>The synchronization status before the import/export was performed</td></tr>
</table>

Registry Synchronization

Each artifact that corresponds to a UDDI entity contains a **Registry Synchronization** section in its detail view (see Artifact Detail Pages on page 170):

Figure 49. Registry Synchronization Details



Its synchronization status is shown and synchronization actions (export/import/delete) are offered for each known UDDI Registry.

Table 6. Synchronization Status

Synchronization Status	Description
Not Synchronized	HP SOA Systinet artifact does not correspond to any UDDI entity. It is not exported to UDDI or imported from UDDI. This synchronization status corresponds to the NEW resource status.
Synchronized	HP SOA Systinet artifact and corresponding UDDI entity are semantically the same, both are the same since the last synchronization. This synchronization status corresponds to the IDENTICAL resource status.
Local change	HP SOA Systinet artifact has changed (while the corresponding UDDI entity has not) since the last synchronization. This synchronization status corresponds to the LOCAL CHANGE resource status.
Remote change	The corresponding UDDI entity has changed since the last synchronization. This synchronization status corresponds to the REMOTE CHANGE resource status.
Local+Remote change	Both the HP SOA Systinet artifact and the corresponding UDDI entity have changed since the last synchronization. This synchronization status corresponds to the NEEDS MERGE resource status.
Unreachable	The UDDI registry is unreachable to check the synchronization status. This synchronization status corresponds to the UNREACHABLE resource status.

Exporting Data To Registry

You can export individual artifacts to an integrated registry.

To export an artifact to a UDDI registry:

1 In the **Registry Synchronization** section of the detail view of the artifact, click **export** for the registry that you want to export the artifact to.

Note: Only organizational unit, business service, implementation and WS-policy artifacts can be exported directly.

2 Provide the login name and password of the UDDI registry account where the data will be exported, and then click **Next**.

Note: For a successful export, the credentials used for registry sign-on must have the appropriate write permissions for the registry entities being created or amended.

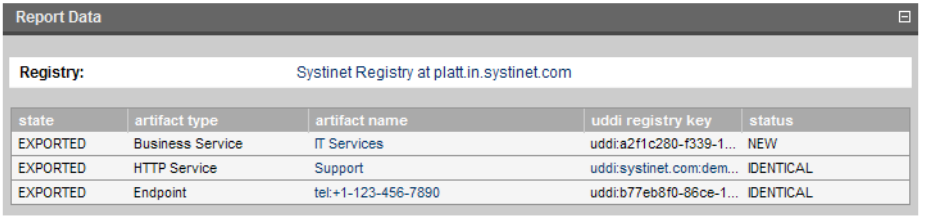
Tip: If the UDDI registry shares user identities via SSO (Single Sign On), this step is not necessary. Data will be exported to the UDDI registry under the account of the current user.

3 Select the associated artifacts to export on the summary page. If you are exporting a business service, all its implementations can be exported as well and if you are exporting an organizational unit, all its business services can also be exported.

4 Click **Finish** to export the selected artifacts.

When the export process begins, an export report is created. This process may take some time, so click **Refresh**. You may have do this several times until the report is complete (and **Refresh** disappears).

The most important part of the report is the **Report Data** section:


Report Data

Registry: Systinet Registry at platt.in.systinet.com

state	artifact type	artifact name	uddi registry key	status
EXPORTED	Business Service	IT Services	uddi:a2f1c280-f339-1...	NEW
EXPORTED	HTTP Service	Support	uddi:systinet.com:dem...	IDENTICAL
EXPORTED	Endpoint	tel:+1-123-456-7890	uddi:b77eb8f0-86ce-1...	IDENTICAL

It shows exactly what was exported, and the export status of all the exported items.

<table>
<tr><th>Parameter</th><th>Definition</th></tr>
<tr><td>state</td><td>
<table>
<tr><th>State</th><th>Description</th></tr>
<tr><td>IMPORTED</td><td>The item was successfully imported.</td></tr>
<tr><td>EXPORTED</td><td>The item was successfully exported.</td></tr>
<tr><td>DELETED</td><td>The item (Business Service or Binding Template) was deleted from the UDDI registry during export because the corresponding artifact had been deleted in HP SOA Systinet.</td></tr>
<tr><td>FAILED</td><td>An error occurred during the export/import of the item.</td></tr>
</table>
</td></tr>
<tr><td>artifact type</td><td>the UDDI entity type: Business Entity, Business Service, SOAP Service, etc.</td></tr>
<tr><td>artifact name</td><td>the SOA Systinet artifact name</td></tr>
<tr><td>uddi registry key</td><td>the unique id of the corresponding UDDI entity</td></tr>
<tr><td>status</td><td>the synchronization status before the import/export was performed</td></tr>
</table>

Deleting Data From a Registry

Entities in a synchronized registry can be deleted from the registry directly from SOA Systinet.

To delete an entity from a UDDI registry:

1 In the **Registry Synchronization** section of the detail view of an artifact, click **delete** for the registry that you want to delete the artifact from.

The delete functionality is also available from the detail view of artifacts already deleted from the repository, and in the dialog for deleting an artifact from the repository.

2 Provide the login name and password of the UDDI registry to delete the data from, and then click **Next**.

Note: For a successful delete, the credentials used for registry sign-on must have the appropriate write permissions for the registry entities being deleted.

Tip: If the UDDI registry shares user identities via SSO (Single Sign On), this step is not necessary. The data is deleted from the UDDI registry under the account of the current user.

3 Review the entities to be deleted. If you are deleting a business service, all its implementations are also deleted, and if you are deleting an organizational unit, all its business services are also deleted. Click **Finish** to delete displayed list of artifacts.

25 Business Availability Center Integration

HP Business Availability Center can access and generate statistics about the services in SOA Systinet. In turn SOA Systinet can access this information.

Important: Only one BAC server artifact can be stored in the SOA Systinet repository.

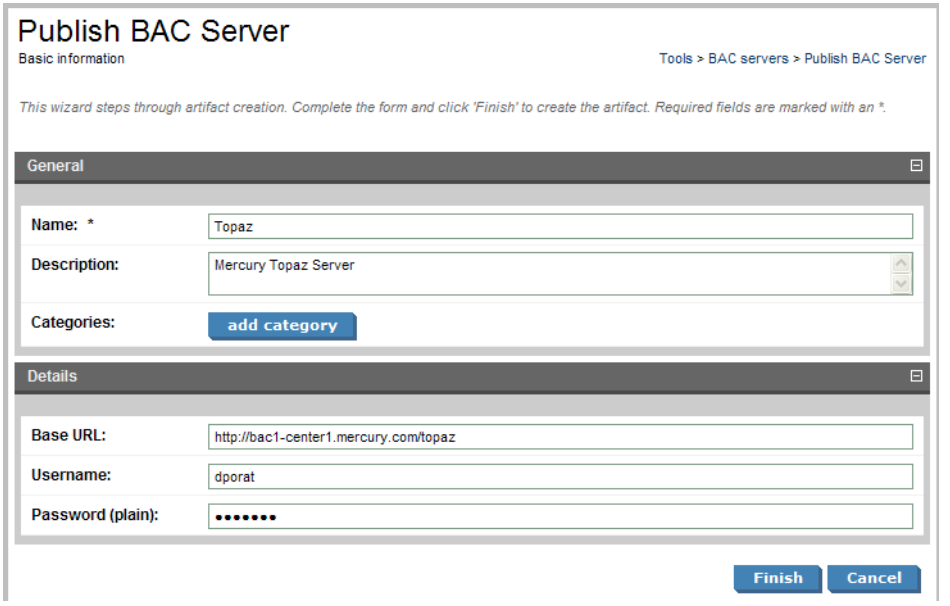
This chapter describes:

Creating a BAC Server Artifact

To receive service availability information from BAC, you must first identify the BAC server to use.

To create a BAC server artifact:

1. In the **Catalog Browser**, expand the **Integration** section, and then click **BAC Servers** to open the browse view of BAC server artifacts.
2. Click **New** to open the **Publish BAC Server** page:



3 Input the following parameters:

Parameter	Definition
Name	The name for the BAC server
Description	A description of the new BAC server
Categories	Click **add category** to select a category from the available taxonomies (administrator perspective only)
Base URL	The address of the BAC server
Username	A login for the BAC server
Password	A password for the BAC server

4 Click **Save** to create the new BAC server artifact.

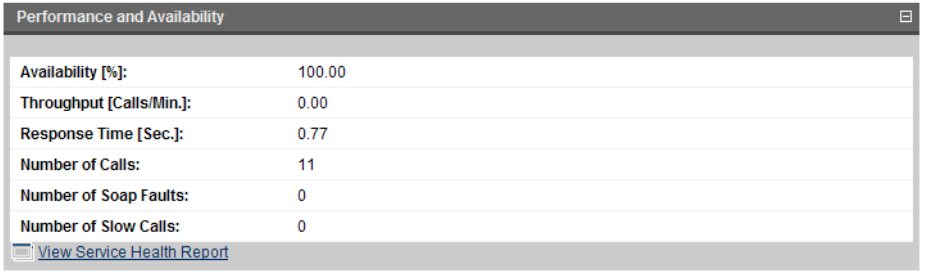
BAC Integration Features

After a BAC server has been integrated with SOA Systinet the service implementations shared by SOA Systinet and BAC are monitored and the analysis and statistics are returned to SOA Systinet.

Use the procedure described in Implementing a Service on page 65 or Publishing a SOAP Service from WSDL on page 186 to import a service monitored by BAC.

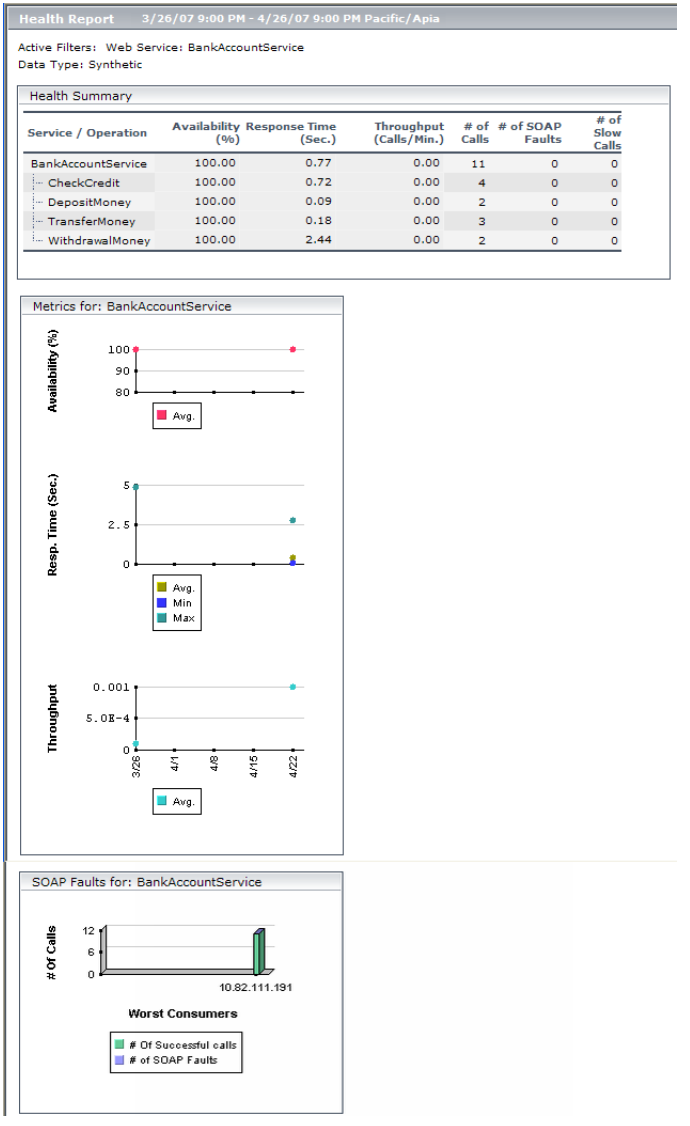
Any implementation that is monitored by BAC has an extra section in its detail view:

Figure 50. Performance and Availability Section



This sections contains statistics generated by BAC and clicking **View Service Health Report** displays the full report from BAC.

Figure 51. BAC Health Report



26 SOA Manager Integration

SOA Systinet provides links to HP SOA Manager for business services and SOAP service implementations stored by both sets of software.

Important: Only one SOAM server artifact can be stored in the SOA Systinet repository.

This chapter describes:

Creating an SOA Manager Server Artifact

To access service information in SOA Manager, you must first identify the SOA Manager server to use.

To create an SOA Manager server artifact:

1. In the **Catalog Browser**, expand the **Integration** section, and then click **SOAM Servers** to open the browse view of SOAM server artifacts.
2. Click **New** to open the **Publish SOAM Server** page:
3. Input the following parameters:

Parameter	Definition
Name	The name for the SOA Manager server
Description	A description of the new SOA Manager server
Base URL	The address of the SOA Manager server

Parameter	Definition
Username and Password	The credentials to login in to SOA Manager
HTTP Basic Authentication	Select to use the credentials to log in instead of anonymous access

4 Click **Save** to create the SOA Manager server artifact.

SOA Manager Integration Features

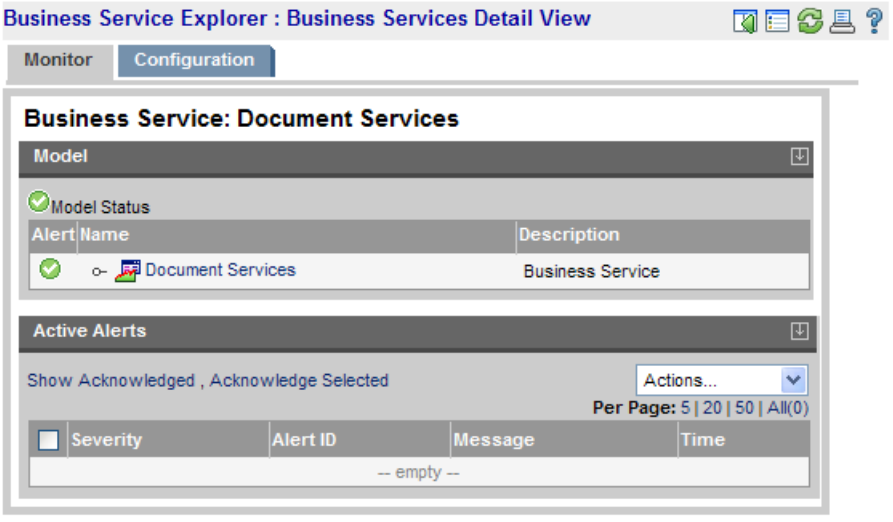
After an SOA Manager server has been integrated with SOA Systinet, the service information in SOA Manager is accessible from the SOA Systinet service view.

Services and SOAP Services have an extra section in their service view:

Figure 52. SOA Manager Section

Click **SOAM Service View** and login to SOA Manager to view the SOA Manager view of the service:

Figure 53. SOA Manager Service View



Note: Only a service or SOAP service with exactly the same name can be accessed in SOA Manager.

Index

V

W

X