HP SOA Systinet

Software Version: 3.00

User Guide

Document Release Date: June 2008
Software Release Date: June 2008

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

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP 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

About 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.

HP Software controls access to components of SOA Systinet with a license. This document describes the full functionality of SOA Systinet including licensed components. If your license does not include these licensed components, their features are not available.

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 user interface – a part for the common UI features and then a part for the features and functionality of each tab.

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.

For details, see the *HP SOA Systinet Administrator Guide* .

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

This document uses the following typographical conventions:

run.bat make	Script name or other executable command plus mandatory arguments.
[--help]	Command-line option.
either | or	Choice of arguments.
replace_value	Command-line argument that should be replaced with an actual value.
{arg1 | arg2}	Choice between two command-line arguments where one or the other is mandatory.
`rmdir /S /Q System32`	User input.
`C:\System.ini`	Filenames, directory names, paths and package names.
`a.append(b);`	Program source code.
`server.Version`	Inline Java class name.
`getVersion()`	Inline Java method name.
Shift+N	Combination of keystrokes.
Service View	Label, word, or phrase in a GUI window, often clickable.
OK	Button in a user interface.
New→Service	Menu option.

Documentation Updates

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

- Software version number, which indicates the software version.
- 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://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support Web site at:

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

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web 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, make sure that it is running on the server you want to access.

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

Enter the URL into your browser in the form:

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

where:

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

The default port is 8080 for HTTP and 8843 to use HTTPS.

For example:

- `http://mypc:8080/soa/web`
- `https://ourserver:8843/soa/web`

This should display the sign-in screen.

Use the credentials provided by your administrator to sign in.

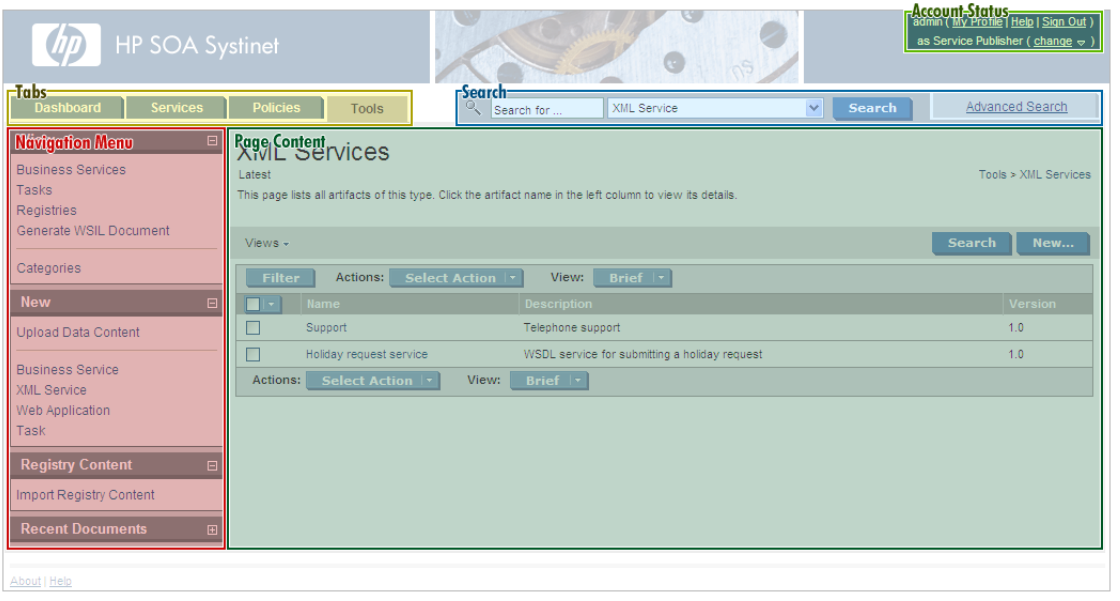
The first time you sign in, SOA Systinet displays a welcome panel.

Review the information on the panel, and click **OK** to display the **Dashboard**.

2 Features of the User Interface

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

Figure 1. A Typical SOA Systinet Page



Every page contains the following common elements:

- **Tabs**

  Access the main components of SOA Systinet, as described in Tabs on page 18.

- **Search**

Search the repository content, as described in Full Text Search on page 24.

- **Menu**

  Each tab contains a set of component specific links, as described in Menus on page 19.

- **Account Status**

  Sign out, edit your user profile and your view of SOA Systinet, as described in Profile Status on page 20.

- **Product Information**

  Access product information and the documentation.

Tabs

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

Figure 2. 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 Chapter 5, Dashboard UI.

The **Services** tab is the central location which shows all information about services, contracts, and lifecycles in one place to provide easy access and simple management. The Services tab is described in Chapter 8, Services UI.

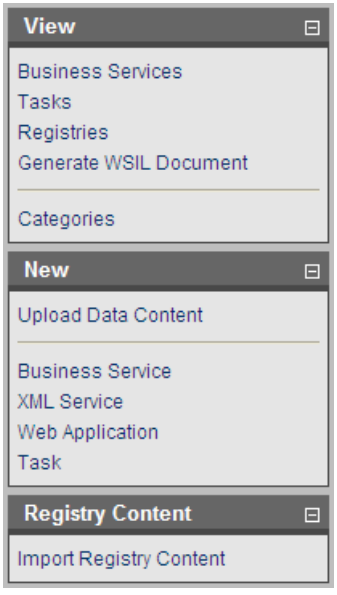
The **Policies** tab enables you to validate your business services against company policy, and to manage those policies. The Policies tab is described in Chapter 13, Policies UI.

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 Chapter 17, Tools UI.

Menus

On the left of each page is a section containing a menu of links specific to each SOA Systinet tab.

Figure 3. Menu



The context specific menus for each SOA Systinet tab are described in the following sections:

- Dashboard Menu on page 34
- Services Menu on page 48
- Policies Menu on page 142
- Tools Menu on page 210

Profile Status

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

Figure 4. Profile Status

- **My Profile**

  Manage your profile, as described in Chapter 3, Managing Your Profile.

- **Help**

  Access the product documentation.

- **Sign Out**

  Sign out of SOA Systinet.

- **Change**

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

3 Managing Your Profile

When you first sign in, SOA Systinet creates a user profile for you based on your account in the external user store.

Your profile details are available to amend.

To change profile details:

1 Click **My Profile** to display your profile information.

2 Click **Edit**.

3 The parameters are split into the following sections:

- **Basic Information**

Parameter	Definition
Name	Your profile name.
Description	Your profile description.
Email	The email used for notifications. Use **Add** and **Remove** for multiple entries. Email can only be amended if SOA Systinet is not integrated with an LDAP/AD user store.

- **Personal Information**

Parameter	Definition
Contact Role	Select a role from the list.
Instant Messenger	Your IM details. Use **Add** and **Remove** for multiple entries.
Phone	Your phone details. Use **Add** and **Remove** for multiple entries.
Language Code	Select a primary language from the list.
Categories	Set taxonomic categories for the search purposes.

- **Group Membership**

  Set a Primary Group from the list, if you want artifacts you create to be owned by the group you are a member of, instead of you.

- **Address Details**

  Your postal contact details, including Geographical Location category setting.

- **Related Repository Artifacts**

  Add any required relationships to existing repository artifacts.

  For details, see Adding a Relationship on page 237.

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

4 Exploring the Repository

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

- Full text search is available on every page.

  For details, see Full Text Search on page 24.

- Advanced search is available on every page.

  For details, see Chapter 20, Advanced Searches.

- Browsing by taxonomic category is accessible from the view menu on every page.

  For details, see Category Browsing on page 27.

- The Services tab provides list views that enable you to browse and filter service artifacts by column heading.

  For details, see List Views on page 54.

- 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.

  For details, see Browse Artifact Pages on page 219.

- Custom RSS views can be added to the Dashboard to provide periodically updated views of specific artifact types.

  For details, see RSS Content Feed Portlets on page 38 and Chapter 6, Adding a Content Feed.

- The REST interface enables you to browse the repository.

  For details, see "REST Interface" in the *HP SOA Systinet Developer Guide* .

- SOA Systinet integrates with IDEs, giving developers direct access to the SOA Systinet repository.

  For details, see "IDE Integration" in the *HP SOA Systinet Developer Guide* .

- Additional service discovery options are available to import service infrastructure into SOA Systinet.

  For details, see Chapter 10, Service Discovery.

Full Text Search

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

To use this functionality you must enable full text search on the database and in the configuration.

For details, see "Configuring the Database for Full Text Search" in the *HP SOA Systinet Installation and Deployment Guide* and "SOA Systinet Configuration Options" in the *HP SOA Systinet Administration Guide* .

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

Advanced Search is not part of full text search. It enables you to create a custom search within a particular artifact type set.

For details, see Creating an Advanced Search on page 273.

To perform a full text search in the SOA Systinet repository:

1 Type your full text search query in the input field.

  The full text query string should conform to the following rules:

  - A query is a list of words, phrases, and subqueries (collectively called terms) separated by spaces or logical operators AND, OR, and NOT.
  - A word is a string of characters, numbers, and some special characters.

- A phrase is a list of words enclosed by quotation marks.
- Enclose search terms including special characters in quotes.

  For example, `"Adam's"`.
- Wildcards `%` and `*` can be used to represent one or more arbitrary characters.

  MSSQL only treats `%` and `*` as wildcards at the end of words.
- Wildcard _ represents one arbitrary character.

  MSSQL does not support _ as a wildcard.
- `%`, `*`, and _ are not treated as wildcards in phrases.
- Logical operators AND and OR, which must be in uppercase, can be placed between terms. A space between terms is a default AND.
- Logical operator NOT, which must be in uppercase, can only be placed before a term if there is at least one preceding term.

  For example, `a AND b NOT c`.
- A subquery is a query enclosed in brackets.

  For example `a AND (b OR c)`.
- For MSSQL, avoid searches using ` (backward apostrophe).
- For MSSQL, to search for words containing < or > in XML/HTML documents, use `<` or `>` instead.

2 Optionally, select an artifact type from the drop down list to restrict your search.

3 Click **Search**.

The results of your search appear as a listing that can be further reduced using filters, as described in Full Text Search Results on page 26.

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

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 in the configuration file.

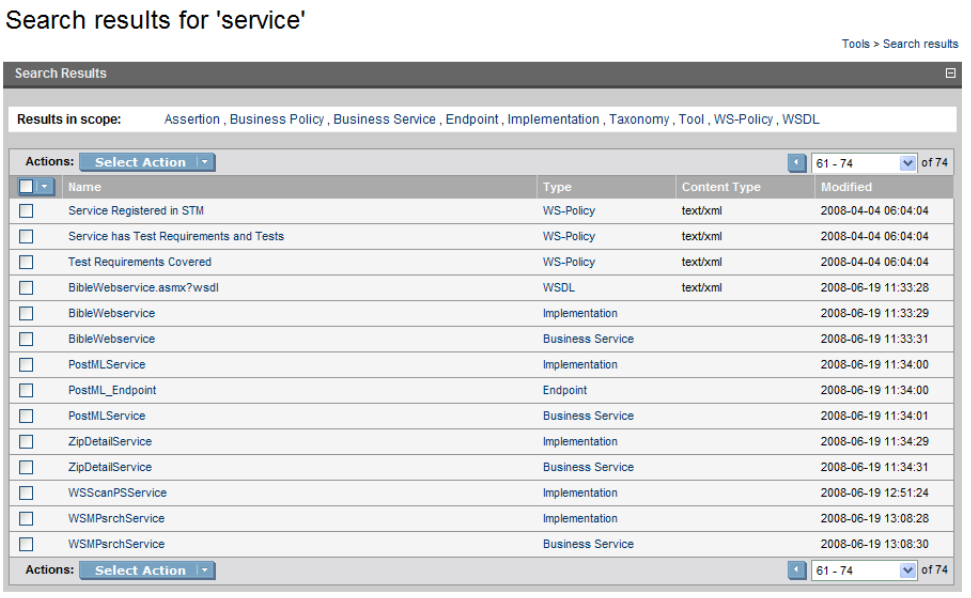
An exception can occur in the event of a wildcard resulting in excessive search terms. If this occurs, resolve the problem with one of the following methods:

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

Full Text Search Results

If you did not select an artifact type, you can reduce the scope of the search.

Figure 5. Search Results Page



Use the artifact type selection in the search bar to reduce the scope, and click **Search**. 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.

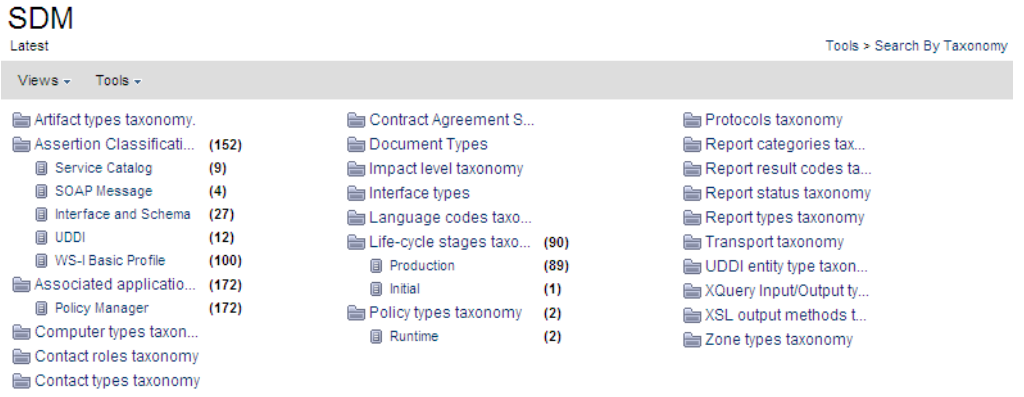
Category Browsing

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

To browse by categories:

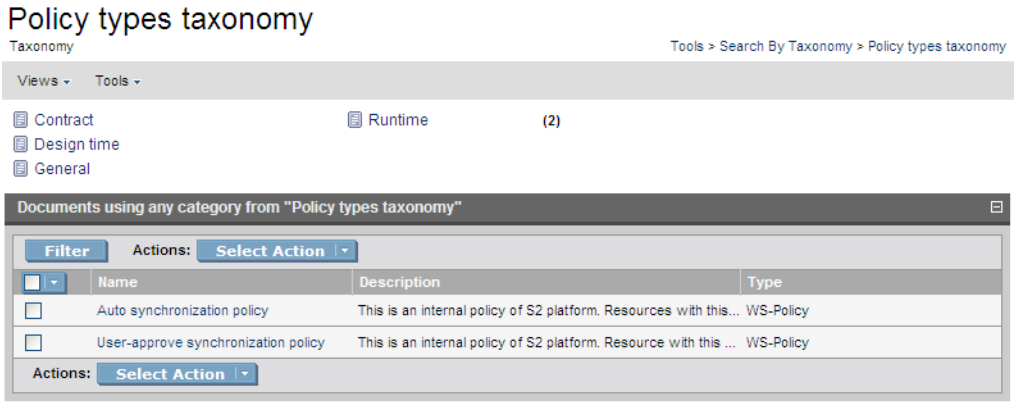
1 In the View section of the menu on any page in the Dashboard, Services, or Tools tabs, click **Categories**.

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 the following 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 the administrator 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 page.

The Filter and Actions functionality in the list of artifacts is the same as for Tools browse pages.

For details, see Browse Artifact Pages on page 219.

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:

- Chapter 5, Dashboard UI

  Describes the user interface elements on the Dashboard.

- Chapter 6, Adding a Content Feed

  Explains how to add a new RSS feed to the Dashboard.

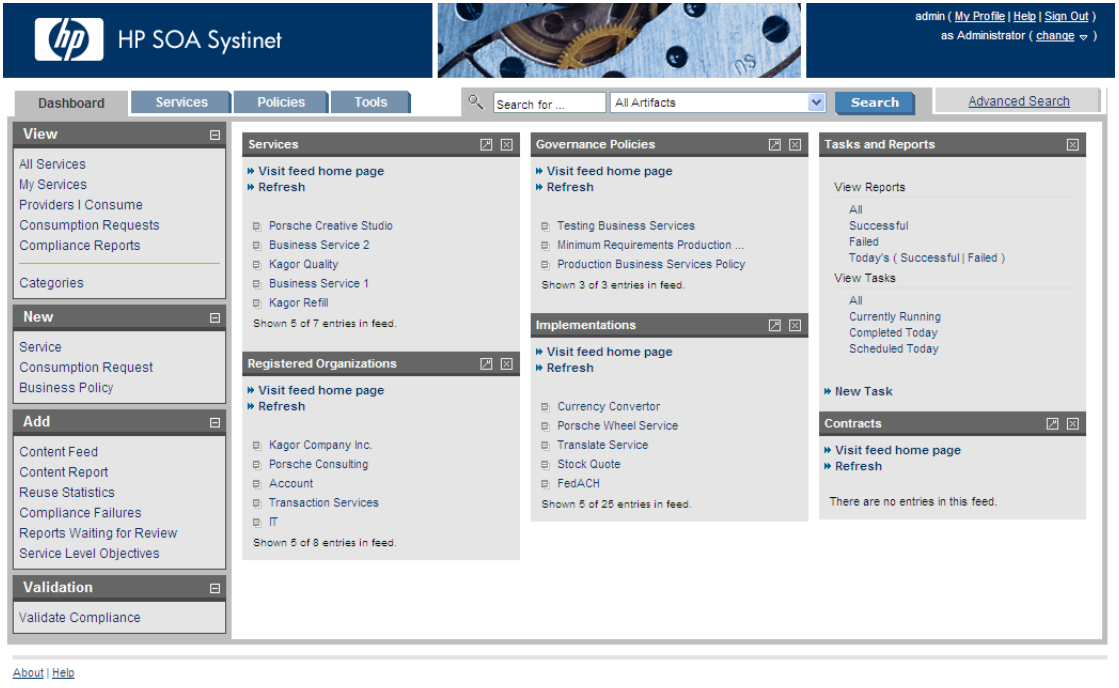
- Chapter 7, Adding a Content Report

  Explains how to add new report content to the Dashboard.

5 Dashboard UI

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

Figure 6. 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.

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** or **5** to select the portlet.
4. Use the **arrow keys** to move the portlet into position.
5. Press **Enter** or **5** to fix the portlet in place.
6. Press **F9** to exit portlet navigation mode.

This chapter describes:

- Dashboard Menu on page 34

  The items in the dashboard menu.

- RSS Content Feed Portlets on page 38

  The RSS content feed portlets on the dashboard.

- Reuse Statistics Portlet on page 38

  Displays statistics of service use.

Dashboard Menu

The Dashboard menu is split into collapsible segments.

Each segment is described in the following sections:

- Dashboard View Menu on page 35

  A set of links to various aspects of service and contract management.

- Dashboard New Menu on page 36

  Create new artifacts.

- Dashboard Add Menu on page 37

  Create new content feeds or add reports to the dashboard.

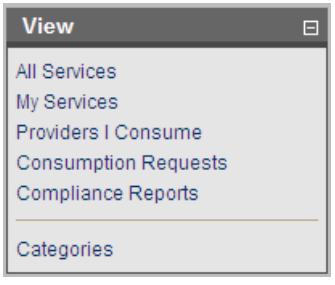
- Validation Menu on page 144

  Validate the policy compliance of an artifact.

Dashboard View Menu

The View menu in the Dashboard provides links to list views for service, contract and policy management.

Figure 7. Dashboard View Menu



The View menu contains the following links:

- Service List Views

  Views of various aspects of service and contract management.

  For details, see List Views on page 54.

- **Compliance Reports**

  A link to the list view of policy compliance reports.

  For details, see Policy and Report List Views on page 148.

- **Categories**

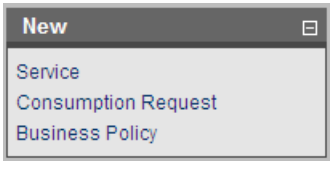
  Browse the repository by taxonomic category.

  For details, see Category Browsing on page 27.

Dashboard New Menu

The New menu in the Dashboard provides quick links to create new artifacts.

Figure 8. Dashboard New Menu



The New menu links to the following artifact creation pages:

- **Service**

  Create a new business service.

  For details. see Creating Business Services on page 73.

- **Consumption Request**

  Request the consumption of a provided artifact.

  For details, see Requesting Consumption on page 134.

- **Business Policy**

Create a new policy.

For details, see Creating Business Policies on page 169.

Dashboard Add Menu

The Add menu in the Dashboard enables you to add and restore content to the Dashboard.

Figure 9. Dashboard Add Menu

The Add menu contains the following functionality:

- **Content Feed**

  Add a new RSS feed to the Dashboard.

  For details, see Chapter 6, Adding a Content Feed.

- **Content Report**

  Add a new Content Feed to the Dashboard.

  For details, see Chapter 7, Adding a Content Report.

- Portlet Names

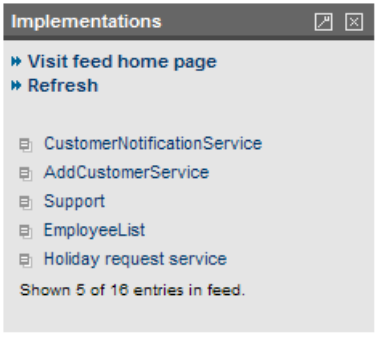
  Any Dashboard portlets that you close appear in this menu.

  Click the name to restore the portlet to the Dashboard.

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.

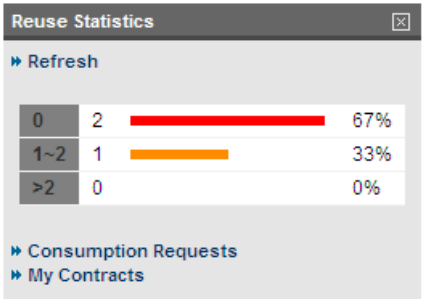
The portlet can be removed from the dashboard by clicking **[X],** and new portlets can be added as described in Chapter 6, Adding a Content Feed.

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

Reuse Statistics Portlet

Contract Manager 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.

Click **Refresh** to reload the service statistics.

Click **Consumption Requests** or **My Contracts** to open the relevant List View for that item.

For details, see List Views on page 54.

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

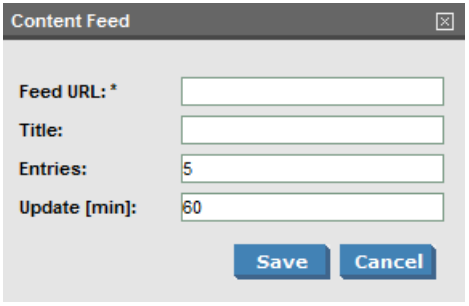
Click one of the graph bars to view the services that fit the selected criteria. For each service the table lists all consumers.

6 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 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 219 and Tools View on page 223) or the **RSS of Result** view accessed from the **View** context menu for a saved search.
Title	The heading for the new feed portlet

Parameter	Definition
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.

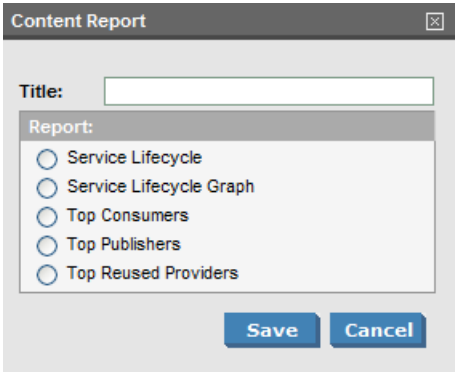
7 Adding a Content Report

The Dashboard can display content from specially designed reports.

SOA Systinet contains a standard set of dashboard reports which can be added to using SOA Systinet Report Editor. See the *SOA Systinet Report Editor Guide* 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 Select a report from the list and then, if required, change the title.

3 Click **Save** to access the most recent report from the reporting server.

4 Click **Reload** to execute 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 the following chapters:

- Chapter 8, Services UI

  The user interface elements of the services tab.

- Chapter 9, Creating Services

  Create services, their implementation, and make them available for use.

- Chapter 10, Service Discovery

  Populate SOA Systinet with service infrastructure from external sources.

- Chapter 11, Lifecycle Governance

  Create governance processes to manage your SOA.

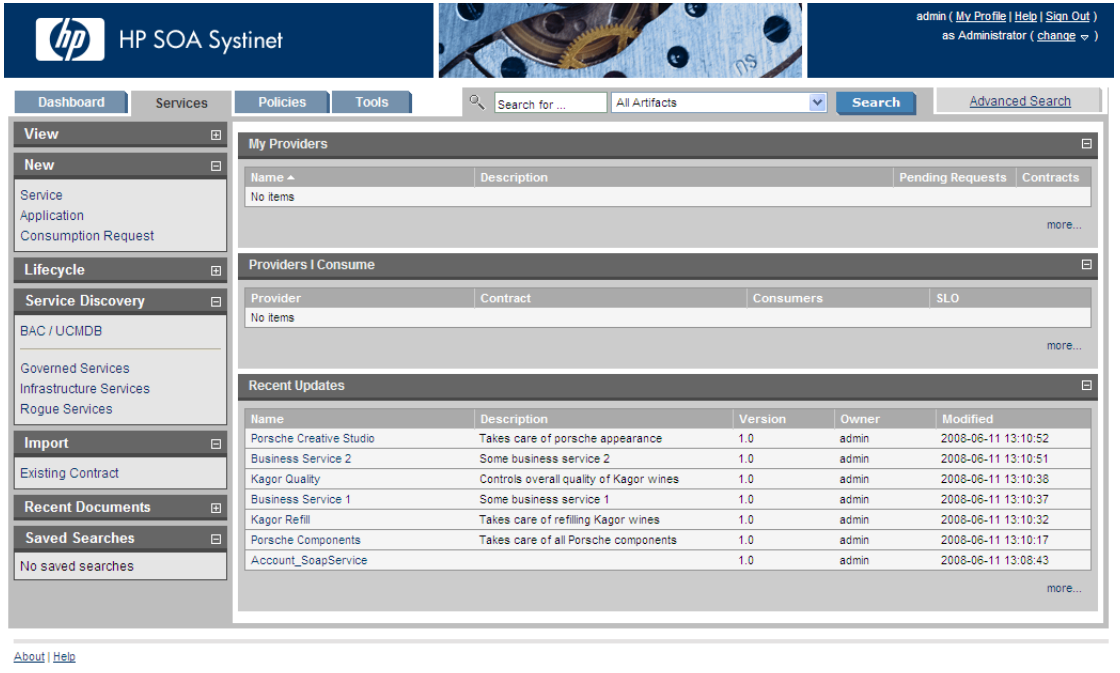
- Chapter 12, Managing Contracts

  Establish and manage contracts between providers and consumers.

8 Services UI

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 48

  A description of the items in the **Services Menu**.

- **My Services**. Shows the services that you provide that are ready for consumption.
- **Providers I 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 a List View for that type of artifact.

For details, see Service View on page 56 or List Views on page 54.

Services Menu

The Services menu is split into collapsible segments.

Each segment is described in the following sections:

- Services View Menu on page 49

  A set of links to various aspects of service and contract management.

- Services New Menu on page 50

  Create new service artifacts.

- Lifecycle Menu on page 51

  Access the lifecycle functionality in SOA Systinet.

- Service Discovery Menu on page 52

  Discover and manage artifacts from an integrated BAC/UCMDB server.

- Import Menu on page 52

  Import existing contracts into SOA Systinet.

- **Recent Documents**

  Quick links to the last few artifacts viewed.

- Saved Searches Menu on page 53

  Quick links to user specified searches.

Services View Menu

The View menu in the Services tab provides links to list views for service, contract and lifecycle management.

Figure 13. Services View Menu

The View menu contains the following links:

- Service List Views

  Views of various aspects of service, lifecycle, and contract management.

  For details, see List Views on page 54.

- Artifact Names

  View the Tools browse pages for these artifact types.

  For details, see Browse Artifact Pages on page 219.

- **Categories**

  Browse the repository by taxonomic category.

  For details, see Category Browsing on page 27.

Services New Menu

The New menu in the Dashboard provides quick links to create new artifacts.

Figure 14. Services New Menu

The New menu links to the following artifact creation pages:

- **Service**

  Create a new business service.

  For details. see Creating Business Services on page 73.

- **Application**

  Create a application artifact.

  For details, see Using Applications on page 93.

- **Consumption Request**

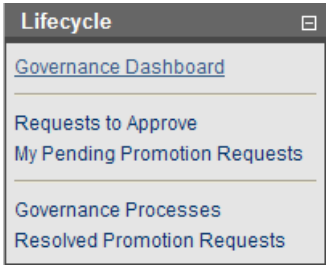
Request the consumption of a provided artifact.

For details, see Requesting Consumption on page 134.

Lifecycle Menu

The Lifecycle menu in the Service tab enables you to access the lifecycle functionality in SOA Systinet.

Figure 15. Services Lifecycle Menu



The Lifecycle menu contains the following links:

- **Governance Dashboard**

  Opens an overview page of governance records in which you have an interest.

- **Requests to Approve**

  Opens an overview page of promotion requests that require your approval. An overview of the last five requests is available in the Governance Dashboard.

- **My Pending Promotion Requests**

  Opens an overview page of all your promotion requests that require approval from other parties. An overview of the last five requests is available in the Governance Dashboard.

- **Governance Processes**

  Opens an overview page of all governance processes.

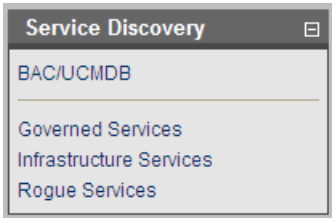
- **Resolved Promotion Requests**

  Opens an overview page of all resolved (historical) promotion requests.

Service Discovery Menu

The Service Discovery menu provides access to services stored in products using a *Universal Configuration Management Database* (UCMDB), specifically *HP Business Availability Center* (BAC), and their representations in the SOA Systinet repository.

Figure 16. Service Discovery Menu



The Service Discovery menu contains the following links:

- **BAC/UCMDB**

  Discover services stored in a Universal Configuration Management Database (UCMDB) used by *HP Business Availability Center* (BAC).

  For details, see BAC/UCMDB Service Discovery on page 106.

- Discovered Service List Views

  List views of services accessed from BAC/UCMDB and processed in SOA Systinet.

  For details, see BAC/UCMDB Service Discovery on page 106.

Import Menu

The Import menu in the Services tab enables you to represent existing contracts in the SOA Systinet repository.

Figure 17. Services Import Menu

The Import menu contains the following link:

- **Existing Contract**

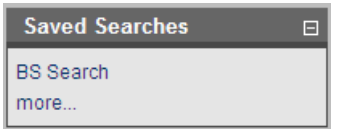
  Import a contract that exists outside SOA Systinet into the repository.

  For details, see Importing Existing Contracts on page 136.

Saved Searches Menu

The Saved Searches menu in the Services tab contains quick links to user created saved searches.

Figure 18. Saved Searches Menu



The Saved Searches menu contains the following links:

- Saved Search names

  Click a search name to open the search.

  For details, see Chapter 20, Advanced Searches.

- **more...**

  View the list of saved searches.

Service Pages

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

- List Views on page 54

  Describes the index views of service artifacts.

- Service View on page 56

  Describes the detailed view of service related artifacts in the Service Catalog.

- Governance Dashboard on page 63

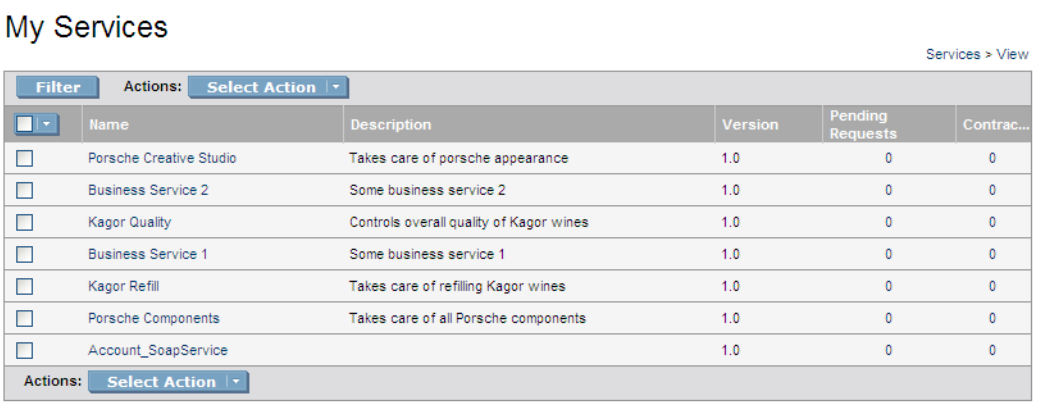
  Describes the lifecycle management page displaying an overview of your approval requests.

List Views

Click one of the links in the Services tab **View** menu to open a list view of that type of artifact.

For example, **My Services**:

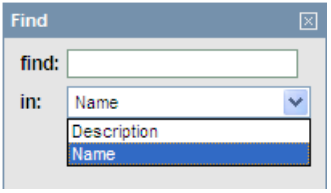
Figure 19. My Services List View



You can reduce the list of artifacts using **Filter**.

Click **Filter** to open a query window:

Figure 20. List View Filter



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

Click **Clear Filter** to remove the filter and restore the list of artifacts, or open the Filter menu and select **Edit Filter** to change the filter terms.

List views also enable you to carry out bulk operations on selected artifacts using the **Actions** menu.

The available bulk operations vary depending on the artifact type.

To perform a bulk operation:

- Select the service artifacts you require, and open the **Select Actions** menu.

  The menu offers the following bulk operations:

  - **Edit Access Rights**

    The owner of an artifact or administrator can edit the permissions of selected artifacts.

    For details, see "Access Rights" in the *HP SOA Systinet Administration Guide*.

  - **Edit Category Bag**

    Change the categorization for the selected artifacts.

    For details, see Categorizing Artifacts on page 240.

- **Change Owner**

  Change the person or group responsible for the artifact.

  For details, see Changing Artifact Ownership on page 239.

- **Synchronize**

  Perform change management on the selected artifacts.

  For details, see Running the Synchronization Tool on page 263.

- **Change Version**

  Create new versions of the selected artifacts.

  For details, see Managing Versions on page 245.

- **Delete**

  Mark the selected artifacts as deleted.

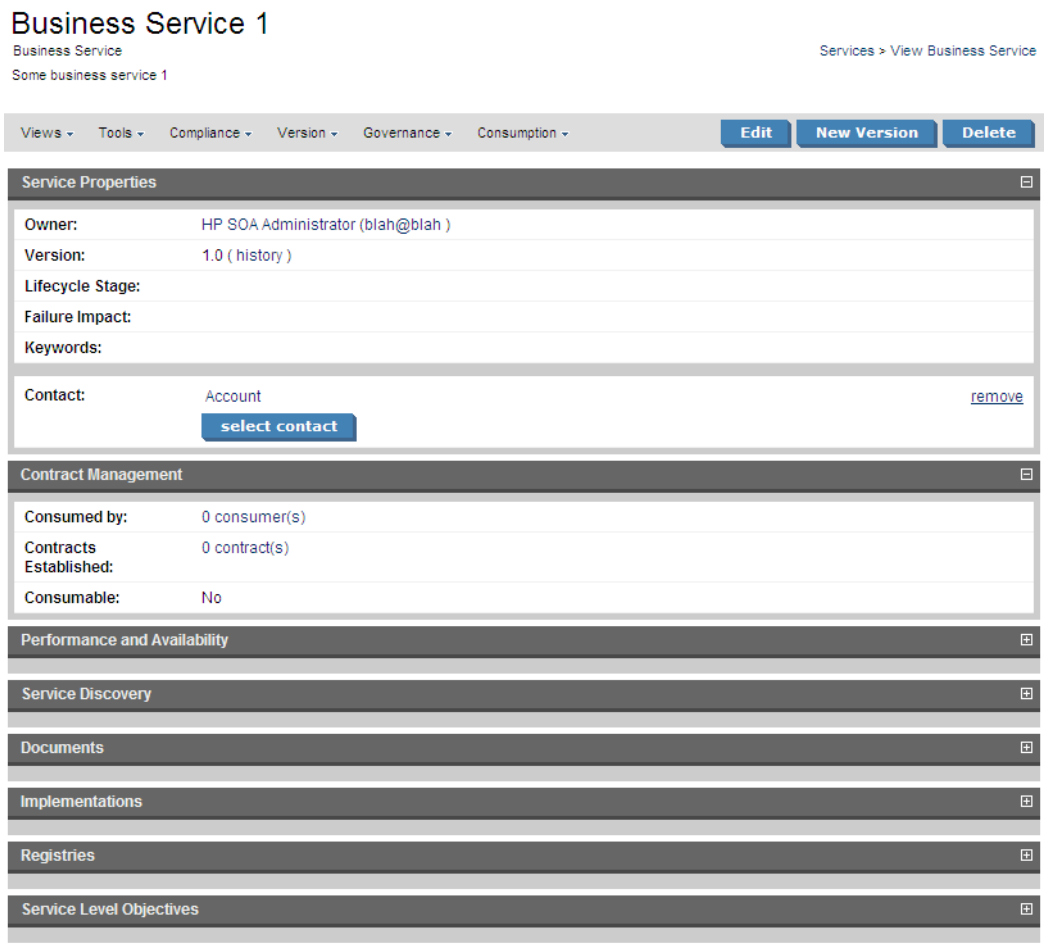
  For details, see Deleting an Artifact on page 237.

Service View

Clicking the name of a service artifact in the Services tab opens the service view for that artifact:

For the purposes of documentation, service artifact refers to any artifact type that is available to view in the Services tab. These include applications, business services, implementations, endpoints, and operations.

Figure 21. View Service Page



The service view is the central location for information about service artifacts.

This following sections describe the content and functionality of these pages:

- Service View Context Actions on page 58

- Service View Page Content on page 61

Service View Context Actions

The grey bar contains a set of context action menus and functions.

The actions vary depending on the artifact but they include:

- **Views**:
  - **Consumer View** and **Services View**

    Switch between the default view of the current revision and the last approved revision of the artifact for artifacts subject to lifecycle management.

    For more details, see Chapter 11, Lifecycle Governance.

    This view selection is preserved if you navigate away from the page.

  - **Advanced View**

    Switches to the detailed view of the artifact in the Tools tab.

    For details, see Tools View on page 223

  - **Navigator View**

    Opens a graphical representation of the artifact and its relationships.

    For details, see Navigator View on page 231.

  - **Revisions**

    View the revision history of the artifact.

    For details, see Revision and Version History on page 233.

  - **Access Rights**

Opens a view of the access permissions for the artifact.

For details, see "Edit Access Rights" in the *HP SOA Systinet Administration Guide* .

- **Tools**:
  - **Related Reports**

    A list of the reports related to this artifact.

    For details, see Reports on page 271.
  - **Dependency Analysis** and **Impact Analysis**

    Execute the impact management tool on the artifact.

    For details, see Impact Tools on page 256.
  - **Change Owner**

    The administrator or owner of the artifact to can transfer ownership to a different user.

    For details, see Changing Artifact Ownership on page 239.
- **Compliance**:
  - **Validate Compliance**

    Validate the policy compliance of an artifact.

    For details, see Chapter 16, Validating Resources.
  - **Compliance Status**

    View the compliance status of the artifact.

    For details, see Report Views on page 158.
  - **Effective Policies**

View the business policies associated with the service artifact.

- **Reset Compliance Statistics**

  Delete all compliance reports associated with the artifact.

- **Version**:
  - **Versions**

    View the version history for the artifact.

    For details, see Revision and Version History on page 233.

  - Version Navigation

    Open specific next, previous, or last versions of the artifact.

- **Governance**
  - **Start Governance**

    Enter the artifact into a lifecycle process.

    For details, see Starting Artifact Governance on page 125.

  - **Start Promotion**

    Request artifact promotion to the next lifecycle stage.

    For details, see Submitting a Promotion Request on page 127.

  - **View Stage Details**

    View the page showing the details for the current lifecycle stage.

  - **Promotion History**

    View the promotion request and voting details for each previous lifecycle stage.

- **Consumption**:
  - **New Request**

    Request consumption of the artifact.

    For details, see Submitting a Promotion Request on page 127.
  - **Pending Requests**

    View the list of outstanding consumption requests for the artifact.
  - **Accepted Requests**

    View the list of accepted consumption requests for the artifact.
  - **Rejected Requests**

    View the list of rejected requests for the artifact.

- **Edit**

  Change the attributes of the artifact.
- **New Version**

  Create a new version of the artifact.

  For details, see Managing Versions on page 245.
- **Delete**

  Mark the artifact as deleted with a further option to purge it from the repository.

Service View Page Content

The service view page contains a set of collapsible segments specific to each artifact type:

- **Properties**

Information about the service artifact specific to the artifact type.

- **Contract Management**

  Service artifacts that are *providers* display contract information.

  For details, see Chapter 12, Managing Contracts.

- **Governance**

  Service artifacts subject to lifecycle management display the last approved stage and the current stage with options to view the stage details, view changes since the last approved version, and to start promotion to the next lifecycle stage.

  For details, see Chapter 11, Lifecycle Governance.

- Related Artifacts Sections

  SOA defines a set of relationships between service artifacts. These sections, including **Documents**, **Implementations**, **Service Level Objectives**, **Endpoints**, and **Operations** enable you to manage these relationships.

  For more details, see Chapter 9, Creating Services.

- **Registries**

  If you integrate SOA Systinet with UDDI Registries, this section displays each registry and the status of the service artifact compared to that registry. There are synchronization options depending on the relative status of the artifact with each registry.

  For details, see Registry Integration on page 248.

- **Service Quality**

  If you integrate SOA Systinet with *HP Service Test Manager* (STM), SOAP Services display a section for service quality statistics from STM.

  This section enables you to register a service with STM and then displays information about requirements, tests, and defects from STM.

For details, see Service Test Manager Integration Features on page 70.

- **Service Discovery**

  If you import a service artifact from an external source, such as *HP Business Availability Center* (BAC), this section displays the source of the original service and its change management status. There are options to display the discovery details, or import changes.

  For details, see Synchronizing Discovered Services on page 111.

- **Performance and Availability**

  The content of this section depends on which product you integrate SOA Systinet with.

  - If you integrate SOA Systinet with *HP Business Availability Center* (BAC), this section displays statistics generated by BAC and enables you to open the BAC view of the service artifact.

    For integration details, see "Setting Up BAC/UCMDB Integration" in the *HP SOA Systinet Administration Guide* .

    For feature details, see BAC/UCMDB Integration Features on page 64.

  - If you integrate SOA Systinet with *HP SOA Policy Enforcer* (SPE), this section enables you to open the SPE view of the service artifact if it is shared with SPE.

    For integration details, see "Setting Up SOA Policy Enforcer Integration" in the *HP SOA Systinet Administration Guide* .

    For feature details, see SOA Policy Enforcer Integration Features on page 68.

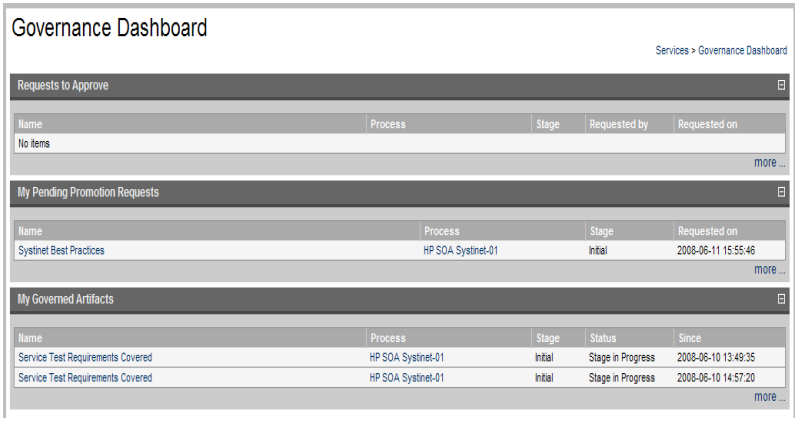
Governance Dashboard

The Governance Dashboard page is part of lifecycle management displaying an overview of promotion requests and governed artifacts relevant to you.

Access the page from the Services tab Lifecycle menu with the **Governance Dashboard** link.

The page is split into the following sections displaying different stages of service and lifecycle approvals, as shown in Figure 22.

Figure 22. Governance Dashboard



- **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.

  For details, see Handling Promotion Requests on page 129.

- **My Pending Promotion Requests**.

  Displays your outstanding change requests that require review by the relevant approvers.

- **My Governed Artifacts**.

  Displays a list of all artifacts currently under governance.

BAC/UCMDB Integration Features

HP Business Availability Center (BAC) monitors run-time services and collects statistics their perfromance. These statistics enable you to verify that a service meets its service level objectives. BAC uses a Universal Configuration Management Database (UCMDB).

SOA Systinet enables you to discover services stored in BAC/UCMDB.

For details about BAC/UCMDB service discovery, see BAC/UCMDB Service Discovery on page 106

Before any data transfer takes place between SOA Systinet and BAC/UCMDB, a BAC/UCMDB server artifact must be created.

For details, see "Setting Up BAC/UCMDB Integration" in the *HP SOA Systinet Administration Guide* .

SOA Systinet artifacts correspond to UCMDB entities as follows:

SOA Systinet Artifact	**UCMDB Entity**
Organizational unit	Business Unit
Business Service	Business Service for Catalog
SOAP Service	Web Service
Operation	Operation

BAC/UCMDB cannot access services directly from SOA Systinet. You must integrate a UDDI Registry with SOA Systinet and UCMDB enables you to access the service entities in the UDDI Registry.

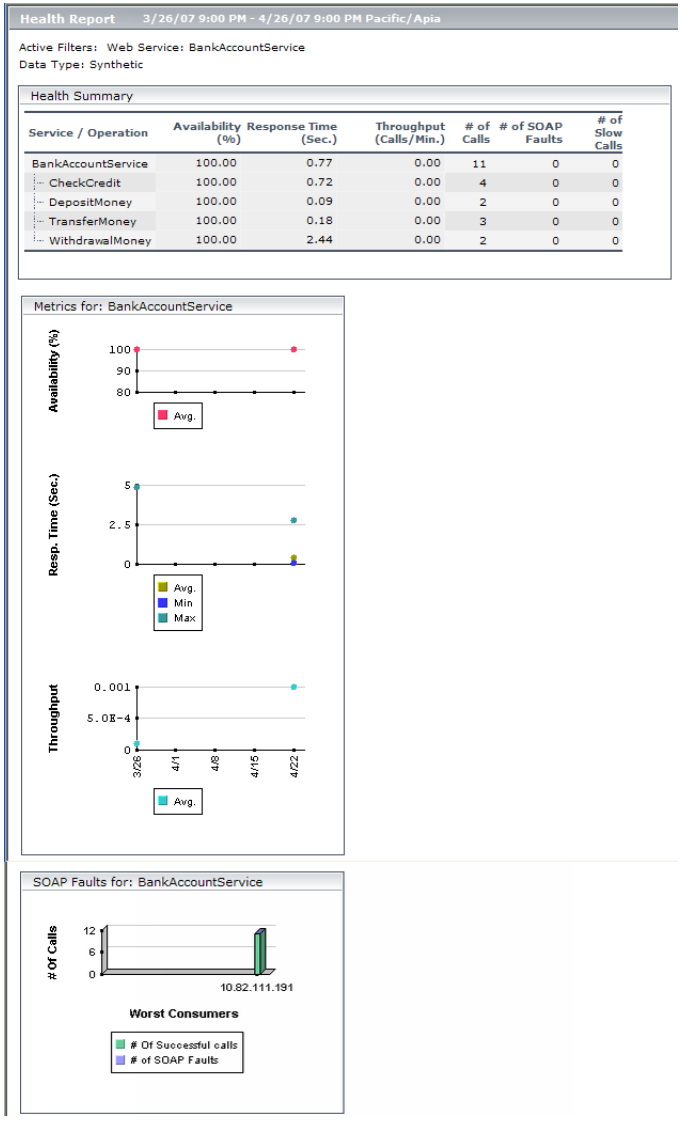
For details, see "Setting Up Registry Integration" in the *HP SOA Systinet Administration Guide* and the *HP Business Availability Center* documentation.

Any service artifact monitored by BAC has an extra section in Services and Tools detail pages:

Figure 23. Performance and Availability Section

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

Figure 24. BAC Health Report



SOA Policy Enforcer Integration Features

HP SOA Policy Enforcer (SOA PE) enables you to monitor the confomance of your run-time services against your business policy.

If you integrate SOA Systinet with (SOA PE), the service information in SOA PE is accessible from the SOA Systinet service view and SOA PE statistics are displayed for SOAP services..

Before you can access services in SPE from SOA Systinet, an SOA Policy Enforcer Server artifact must be created.

For details, see "Setting Up SOA Policy Enforcer Integration" in the *HP SOA Systinet Administration Guide* .

After SOA PE integration is complete, policies you create in SOA PE are published directly to the SOA Systinet repository.

For details, see the *HP SOA Policy Enforcer* documentation.

SOA Systinet artifacts correspond to SPE entities as follows:

SOA Systinet Artifact	**SOA PE Entity**
WS-Policy	Policy
Business Service	Business Service
SOAP Service	Web Service

Services shared by SOA Systinet and SOA PE must have the same *QName*, defined by the namespace of the WSDL describing the service and the local name stated in the `wsdl-service-name` element.

Apart from the SOA PE policy publishing, there is no direct import or export functionality between SOA PE and SOA Systinet. You must integrate a UDDI Registry with SOA Systinet and SOA PE enables you to access the service entities in the UDDI Registry.

For details, see "Setting Up Registry Integration" in the *HP SOA Systinet Administration Guide* and the *HP SOA Policy Enforcer* documentation.

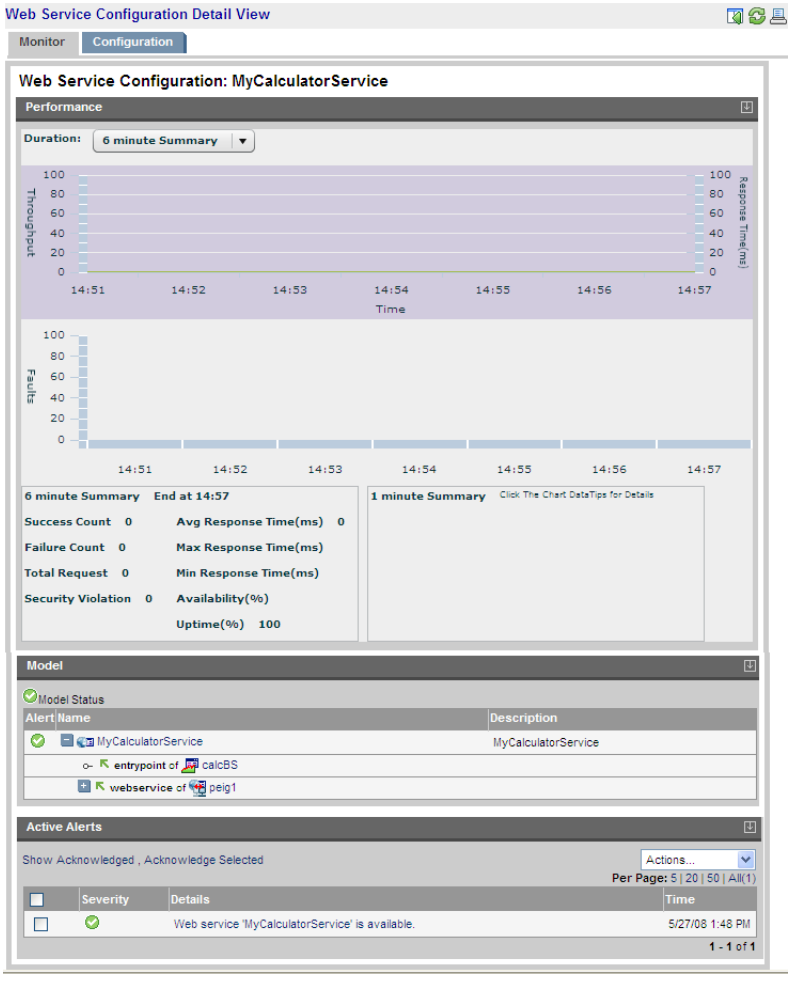
Services and SOAP Services have an extra section in their service view:

Figure 25. Performance and Availability Section

For shared SOAP services the section displays SOA PE statistics.

For both business services and SOAP services, click **SOA Policy Enforcer Service View** and login to SOA PE to view the Policy Enforcer view of the service:

Figure 26. SOA Policy Enforcer Service View



Service Test Manager Integration Features

HP Service Test Manager (STM) is an *HP Quality Center* component that enables you to test services in conjunction with Quality Center functionality.

SOA Systinet enables you to register SOAP services in STM for testing. Statistics for the test results are then available in the Services and Tools detail pages for SOAP services.

Before any data transfer takes place between SOA Systinet and STM, an STM server artifact must be created.

For details, see "Setting Up STM Integration" in the *HP SOA Systinet Administration Guide* .

SOA Systinet artifacts correspond to STM entities as follows:

SOA Systinet Artifact	**STM Entity**
SOAP Service	Web Service

After an STM server has been integrated with SOA Systinet, you can register SOAP services in STM.

SOAP Services have an extra Service Quality section in their Service and Tools detail view:

Figure 27. Service Quality Section

Expand **Register in STM** and click the STM server to export the SOAP service to.

The SOAP service you want to register must be created in SOA Systinet by uploading a WSDL that defines it.

For details, see Uploading Service Infrastructure from Definition Documents on page 99.

You must log in to Quality Center and the STM services page opens.

To be able to register services in STM you must install this *HP Quality Center* plugin:

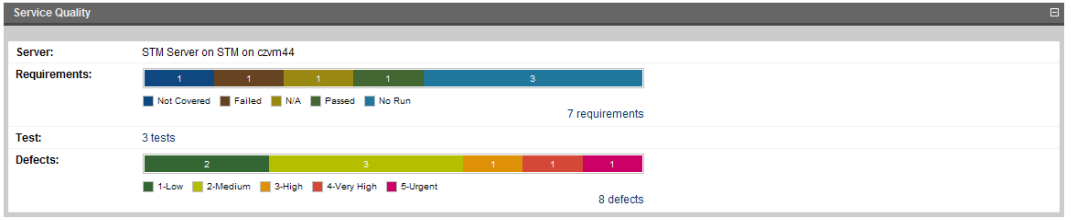
- `Service Test Add-in for Quality Center 9.14`

  Microsoft Internet Explorer must be the default browser when accessing STM.

  Access STM and allow the client code to install (ActiveX) to the browser.

A registered SOAP service displays testing statistics in the Service Quality section:

Figure 28. Service Quality Section



Use the requirement, test and defect links to open the relevant pages in STM.

9 Creating Services

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

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

This section assumes that Business Service is your primary service artifact for organizing your SOA. SOA Systinet also enables you to manage your SOA at a higher level using Applications or at a lower level using Operations.

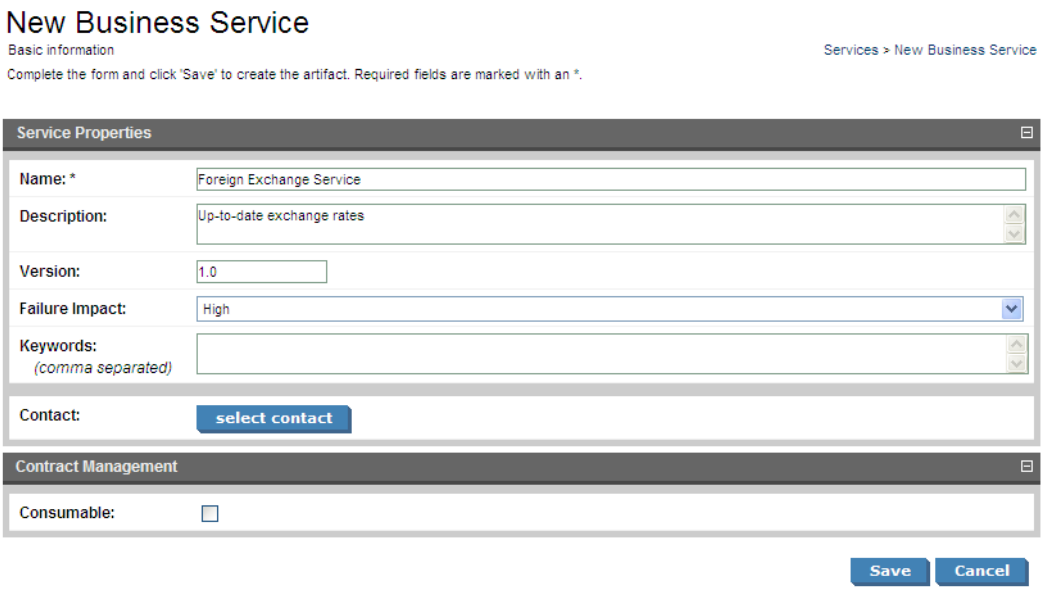
For details, see Using Applications on page 93 and Using Operations on page 95.

Creating Business Services

You can create new business services from the Dashboard or the Services tab.

To publish a new service:

1 In the Dashboard or Services tab New menu, click **Service** to open the New Business Service page:



2 Enter the following parameters:

Parameter	Definition
Name	The name of the new business service.
Description	A description of the new service.
Version	The initial version number of the service.
Failure Impact	Select an impact from the drop-down list.
Keywords	Optionally, add search terms for the service.
Contact	Optionally, click **Select Contact** to select a service contact from the list. For more details, see Setting Contacts on page 75.
Consumable	Select to make the service available to consumers (not visible in the **General** perspective).

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

Setting Contacts

A business service is usually associated with a particular person or group.

To set a contact for a service:

1. In the Services view of the service expand the Contact section by clicking **Select Contact**.
2. Use **Find** to search for the required contact and click **select** to set the contact from the list.

Adding Service Documentation

Services often have associated documentation.

To add documentation to a service:

- In the Services view of a service, in the Documentation section, place the cursor over **Add Document** to view the following options:
  - **From Local File**

    Upload a document from your local file system.

    For details, see To upload a document from your local file system:
  - **From Remote File**

    Upload a document from a remote location.

    For details, see To upload a document from a remote location:
  - **Link to a Remote File**

    Create a link to a document on a remote location.

    For details, see To link to a document on a remote location:
  - **From Catalog**

Select a document from the collection in the repository.

For details, see To select from the list of the documentation artifacts in the repository:.

To upload a document from your local file system:

1 In the Services view of a service place the cursor over **Add Document** for view the available options.

2 Click **From Local File** to open the Local File dialog box.

3 Input the following parameters:

Parameter	Definition
File	Input a path or use **Browse** to locate the file on your local file system.
Location	Input a directory name to store the uploaded document in the repository. **View Locations** enables you to browse the existing locations.
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.

4 Click **Save** to upload the document, create a new documentation artifact, and create the relationships between the service and the documentation artifact.

To upload a document from a remote location:

1 In the Services view of a service place the cursor over **Add Document** for view the available options.

2 Click **From Remote File** to open the **Remote File** dialog box.

3 Input the following parameters:

Parameter	Definition
URL	Input the URL of the remote document.

Parameter	Definition
Location	Input a directory name to store the uploaded document in the repository. **View Locations** enables you to browse the existing locations.
Base URL	The part of the URL location to ignore when creating the publishing location.
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.
Synchronization	Select a synchronization policy for change management. For more details, see Synchronization Policy on page 262.

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

To link to a document on a remote location:

1 In the Services view of a service place the cursor over **Add Document** for view the available options.

2 Click **Link to a Remote File** to open the Link to a Remote File dialog box.

3 Input the following 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.

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

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

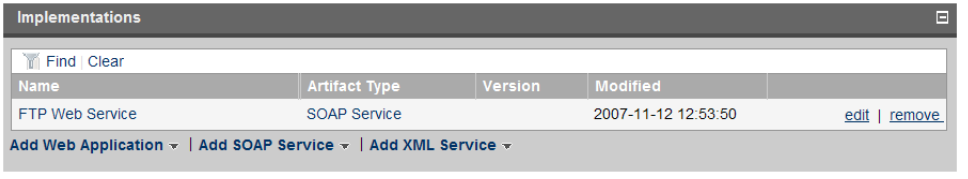
1. In the Services view of a service place the cursor over **Add Document** for view the available options.
2. Click **From Catalog** to open the Browse Catalog dialog box.
3. Use **Find** to search for the required documentation artifact and click **add** to select the document from the list.

Implementing Services

Business services are implemented in the Services tab.

The Services view of a business service contains an **Implementation** section:

Figure 29. Implementations Section



You can add the following implementations types:

- **Add SOAP Service**

  for details, see Adding SOAP Services on page 79.

- **Add XML Service**

  For details, see Adding XML Services on page 81.

- **Add Web Application**

  For details, see Adding Web Applications on page 83.

Implementations consist of a set of methods represented in SOA Systinet as operations.

For details, see Adding Operations on page 85.

XML services and web applications also require the creation of an endpoint to make them functioning implementations.

For details, see Adding an Endpoint on page 86.

XML services can also be defined with an XML schema document.

For details, see Adding an XML Service Definition on page 87.

Adding SOAP Services

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

To add a SOAP service to a business service:

- In the Services view of a service, in the Implementations section, place the cursor over **Add SOAP service** to view the following options:
  - **From Local File**

    Add a SOAP service defined by a WSDL in a local file system.

    For details, see To add a SOAP service from your local file system:

    This process uses the publisher functionality.

    For details, see Uploading Service Infrastructure from Definition Documents on page 99.

  - **From Remote File**

    Add a SOAP service defined by a WSDL in a remote location.

    For details, see To add a SOAP service from a remote location:

This process uses the publisher functionality.

For details, see Uploading Service Infrastructure from Definition Documents on page 99.

- **From Catalog**

  Select a SOAP service already in the repository.

  For details, see To select a SOAP service from the repository:

To add a SOAP service from your local file system:

1. In the Services view of a service, in the Implementations section, place the cursor over **Add SOAP service** to view the available options.
2. Click **From Local File** to open the Local File dialog box.
3. Input the path or use **Browse** to locate the WSDL file on your local file system.

You can reference a zip file containing several WSDLs, including referenced schemas.

4. Input a directory location to store the uploaded document in the repository. **View Locations** enables you to browse the existing locations.
5. Click **Save** to start the publication process for the implementations contained in the WSDL file.
6. Review the artifacts to be created, and then click **Finish**.
7. Review the publishing report, and then click **OK** to return to the Services view of the service.

To add a SOAP service from a remote location:

1. In the Services view of a service, in the Implementations section, place the cursor over **Add SOAP service** to view the available options.

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

3 Complete the dialog with parameters:

Parameter	Definition
WSDL File	Input the url of the remote WSDL file.  You can reference a zip file containing several WSDLs, including referenced schemas.
Location	Input a directory location to store the uploaded document in the repository. **View Locations** enables you to browse the existing locations.
Base URL	The part of the URL location to ignore when creating the publishing location.
Synchronization	Select a synchronization policy for change management. For more details, see Synchronization Policy on page 262.

4 Click **Upload** to start the publication process for the implementations contained in the WSDL file.

5 Review the artifacts to be created, and then click **Finish**.

6 Review the publishing report, and then click **OK** to return to the Services view of the service.

To select a SOAP service from the repository:

1 In the Services view of a service, in the Implementations section, place the cursor over **Add SOAP service** to view the available options.

2 Click **From Catalog** to view a list of SOAP services in the repository.

3 Click **add** next to the SOAP service you require to associate it with the business service.

Adding XML Services

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

To add an XML service to a business service:

- In the Service view of a service, in the Implementations section, place the cursor over **Add XML Service** to view the following options:
  - **New XML Service**

    Create a new XML service to associate with the business service.

    For details, see To create a new XML service:
  - **From Catalog**

    Select an XML service already in the repository.

    For details, see To select an XML service from the repository:.

To create a new XML service:

1. In the Service view of a service, in the Implementations section, place the cursor over **Add XML Service** to view the available options.
2. Click **New XML Service** to open the New XML Service page.
3. Input the following 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.
Consumable	Select to make the service available to consumers (not visible in the **General** perspective).

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

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.

For details, see Adding an Endpoint on page 86.

An XML schema document can also be added to an XML service.

For details, see Adding an XML Service Definition on page 87.

To select an XML service from the repository:

1. In the Service view of a service, in the Implementations section, place the cursor over **Add XML Service** to view the available options.
2. Click **From Catalog** to view a list of XML services in the repository.
3. Click **add** next to the XML service you require to associate it with the business service.

Adding Web Applications

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

To add a web application to a service:

- In the Services view of the service, in the Implementations section, place the cursor over the **Add Web Application** to view the following options:
  - **New Web Application**

    Create a new web application associated with the business service.

    For details, see To create a new web application:
  - **From Catalog**

    Select a web application already in the repository.

For details, see To select a web application from the repository:

To create a new web application:

1 In the Services view of the service, in the Implementations section, place the cursor over the **Add Web Application** to view the available options.

2 Click **New Web Application** to open the New Web Application page.

3 Input the following 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.
Consumable	Select to make the service available to consumers (not visible in the **General** perspective).

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

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.

For details, see Adding an Endpoint on page 86.

To select a web application from the repository:

1 In the Services view of the service, in the Implementations section, place the cursor over the **Add Web Application** to view the available options.

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

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

Adding Operations

Implementations consist of a set of *methods* with specific functionality. These are represented in SOA Systinet by operations.

To add an operation to an implementation:

- In the Service view of an implementation, in the Operations section, place the cursor over Add Operation to view the following options:
  - **New Operation**

    Create a new operation to associate with the implementation.

    For details, see To create a new operation:
  - **From Catalog**

    Select an operation already in the repository.

    For details, see To select an operation from the repository:.

To create a new operation:

1. In the Service view of an implementation, in the Operations section, place the cursor over Add Operation to view the available options.
2. Click **New Operation** to open the New Operation page.
3. Input the following parameters:

Parameter	Definition
Name	The name of the new operation
Description	A description of the operation
Consumable	Select to make the service available to consumers (not visible in the **General** perspective).

4 Click **Save** to create the new operation and the relationships with the implementation.

To select an operation from the repository:

1 In the Service view of an implementation, in the Operations section, place the cursor over Add Operation to view the available options.

2 Click **From Catalog** to view a list of operations in the repository.

3 Click **add** next to the operation you require to associate it with the implementation.

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 implementation:

- In the Services view of an implementation, in the Endpoints section, place the cursor over Add Endpoint to view the following options:
  - **New Endpoint**

    Create a new endpoint to associate with the implementation.

    For details, see To create a new endpoint:
  - **From Catalog**

    Select an endpoint already in the repository.

    For details, see To select an endpoint from the repository:.

To create a new endpoint:

1 In the Services view of an implementation, in the Endpoints section, place the cursor over Add Endpoint to view the available options.

2 Click **New Endpoint** to open the **Create New Endpoint** dialog.

3 Input the following parameters:

Parameter	Definition
Name	The name of the new endpoint
Description	A description of the endpoint
Version	A version number for the endpoint artifact.
Endpoint Address	The URL for the actual implementation of the service
Consumable	Select to make the service available to consumers (not visible in the **General** perspective).

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

To select an endpoint from the repository:

1 In the Services view of an implementation, in the Endpoints section, place the cursor over Add Endpoint to view the available options.

2 Click **From Catalog** to view a list of endpoints in the repository.

3 Click **add** next to the endpoint you require to associate it 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:

- In the Service view of an XML service, in the Definitions, place the cursor over **Add Definition** to view the following options:
  - **From Local File**

    Upload an XSD file from your local file system.

    For details, see To upload an XSD file from your local file system:

- **From Remote File**

  Upload an XSD file from a remote location.

  For details, see To upload an XSD file from a remote location:

- **From Catalog**

  Select an XML schema artifact from the collection in the repository.

  For details, see To select an XML schema from the repository:

To upload an XSD file from your local file system:

1. In the Service view of an XML service, in the Definitions, place the cursor over **Add Definition** to view the available options.
2. Click **From Local File** to open the Local File dialog box.
3. Input the path or use **Browse** to locate the XSD file.
4. Input a directory location name to store the uploaded document in the repository. **View Locations** enables you to browse the existing locations.
5. Click **Save** to upload the XSD, create a new XML schema artifact and the relationships between the XML service and the XML schema artifact.

To upload an XSD file from a remote location:

1. In the Service view of an XML service, in the Definitions, place the cursor over **Add Definition** to view the available options.
2. Click **From Remote File** to open the Remote File dialog box.
3. Input the following parameters:

Parameter	Definition
URL	Input the remote location of the file.

Parameter	Definition
Location	Input a directory name to store the uploaded document in the repository. **View Locations** enables you to browse the existing locations.
Base URL	The part of the URL location to ignore when creating the publishing location.
Synchronization	Select a synchronization policy for change management. For more details, see Synchronization Policy on page 262.

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

To select an XML schema from the repository:

1 In the Service view of an XML service, in the Definitions, place the cursor over **Add Definition** to view the available options.

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

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

Adding Service Level Objectives

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

This section describes adding an SLO to a business service. The functionality is the same for any artifact that is defined as a provider.

To add a service level objective to a service:

- In the Services view of a service, in the Service Level Objectives section, place the cursor over **Add SLO** to view the following options:
  - **New SLO**

    Create a new service level objective to associate with the service.

For details, see To create a new service level objective:

- **From Catalog**

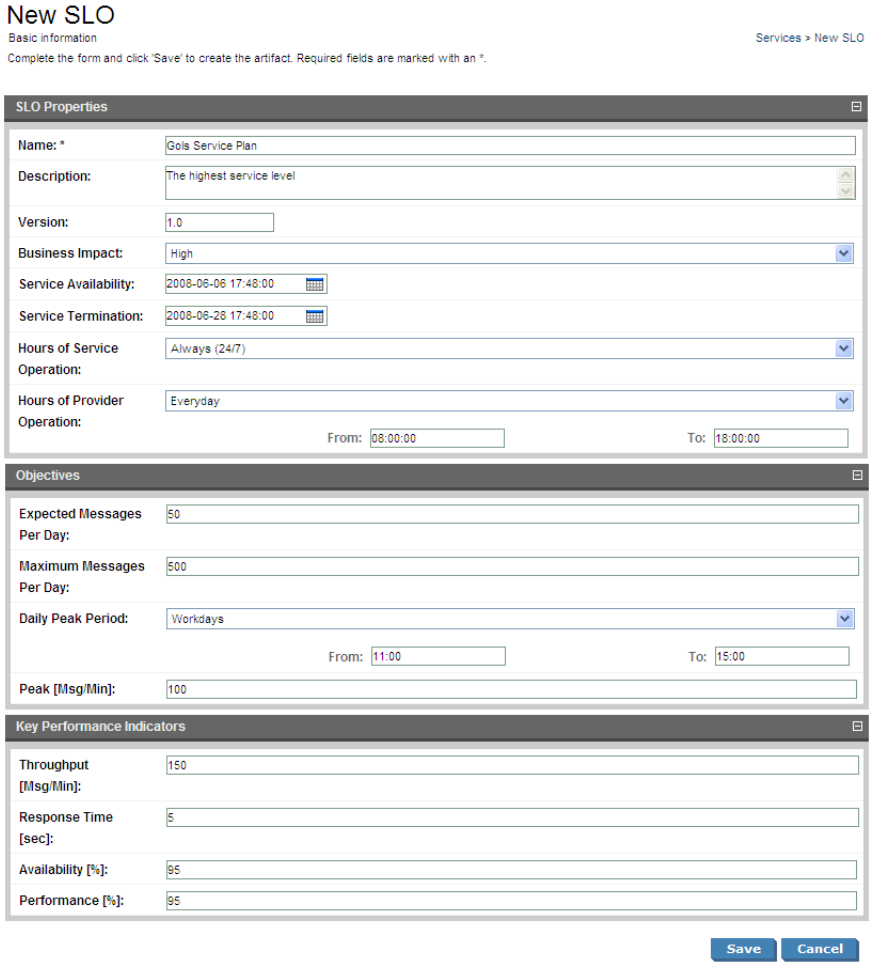
  Select a service level objective already in the repository.

  For details, see To select a service level objective from the repository:

To create a new service level objective:

1 In the Services view of a service, in the Service Level Objectives section, place the cursor over **Add SLO** to view the available options.

2 Click **New SLO** to open the New SLO page:



3 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.
Version	The initial version number for the SLO.
Business Impact	Select an impact from the list.
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.

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

To select a service level objective from the repository:

1. In the Services view of a service, in the Service Level Objectives section, place the cursor over **Add SLO** to view the available options.
2. Click **From Catalog** to view a list of service level objectives in the repository.
3. Click **add** next to the service level objective you require to associate it with the business service.

Making Services Available

When you consider a service to be ready you can make it available for consumption.

To make a service available to consumers:

1. In the Services view of a service, click **Edit**.

   The Edit page for the service opens.
2. Select **Consumable**.
3. Click **Save** to make the service available for consumption.

Using Applications

SOA Systinet enables you to organize your business services into a set of applications. You can use these applications as the primary service artifact for the purposes of contract and lifecycle management.

The following sections describe how to use applications:

- Creating an Application on page 94
- Adding a Service on page 94

The following functionality for applications is the same as for a business service:

- Attaching documentation.

  For details, see Adding Service Documentation on page 75.

- Applying service level objectives.

  For details, see Adding Service Level Objectives on page 89

- Making the application available to consumers.

  For details, see Making Services Available on page 93.

Creating an Application

SOA Systinet enables you to create artifacts to represent your applications.

To create a new application:

1 In the Services tab New menu, click **Application** to open the New Application page.

2 In the New Application page, input the following parameters:

Parameter	Definition
Name	A name for the application.
Description	A description of the application.
Alias	An alias for the application.
Categories	Select taxonomic categories for the operation.
Version	The initial version number for the application.
Consumable	Select to make the application available to consumers.

3 Click **Save** to create the new application artifact.

Adding a Service

An application represents a set of business services.

To add a business service to an application:

1 In the Business Services section of the application view place the cursor over **Add Business Service** to view the following options:

- **New Business Service**

  Create a new business service as part of the application.

- **From Catalog**

  Select a business service already in the repository.

2 Do one of the following:

- **To create a new business service:**

  1 Click **New Business Service** to open the New Business Service page.

  2 Input the business service parameters.

  For details, see Creating Business Services on page 73.

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

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

  1 Click **From Catalog** to view a list of business services in the repository.

  2 Click **add** next to the business service you want to associate with the application.

Using Operations

SOA Systinet enables you to use operations as the primary service artifact for contract and lifecycle management.

To create a new operation:

1 In the Tools tab Catalog Browser, click **Operations** to open the Operations browse page.

2 Click **New** to open the New Operation page.

3 In the New Operation page input the following parameters:

Parameter	Definition
Name	The WSDL operation name (pt:plaintext). For example `doGetCachedPage`.
Description	A description of the application.
Categories	Select taxonomic categories for the operation.
Operation name	The WSDL operation name (optional, pt:plaintext). For example `doGetCachedPage`.
Port Type	The WSDL port type (optional, pt:plaintext). For example `RegistrySearchPort`.
Target Namespace	The WSDL target namespace (optional, pt:plaintext). For example `ure:RegistrySearch`.
Input Types	The XSD input message types (multiple pt:plaintext). For example `{http://www.w3.org/2001/XMLSchema}string`.
Output Types	The XSD output message types (multiple pt:plaintext). For example `{http://www.w3.org/2001/XMLSchema}base64binary`.
Fault Types	The XSD fault message types (multiple pt:plaintext). For example `{urn:RegistrySearch}failure`.
Consumable	Select to make the operation available to consumers.

4 Click **Save** to create the new operation.

The Tools detail view for the operation opens. Switch to the service view to add implementations and service level objectives.

The following functionality for operations is the same as for a business service:

- Adding implementations.

Operations can be added to implmentations.

For details, see Implementing Services on page 78.

- Applying service level objectives.

  For details, see Adding Service Level Objectives on page 89

- Making the operation available to consumers.

  For details, see Making Services Available on page 93.

10 Service Discovery

SOA Systinet enables you to publish entire service infrastructures based on a number of different architectures.

These methods are described in the following sections:

- Uploading Service Infrastructure from Definition Documents on page 99

  Publish service infrastructures using definition documents that describe them.

- Importing Services from Registries on page 103

  Import service infrastructure from a UDDI Registry.

- BAC/UCMDB Service Discovery on page 106

  Import service infrastructure from a BAC/UCMDB server.

Uploading Service Infrastructure from Definition Documents

SOA Systinet enables you to upload definition documents that describe service infrastructures. SOA Systinet processes the content of the document and enables you to create the artifacts to represent this infrastructure in SOA Systinet.

SOA Systinet can process the following definition document types:

- Web Service Definition Language documents (**WSDL**)
- Service Component Architecture documents (**SCA 1.0**)
- Business Process Execution Language documents (**BPEL 1.1 and 2.0**)
- XML Schema Definition documents (**XSD**)

- Extensible Stylesheet Language Transformation documents (**XSLT**)
- Document Type Definition documents (**DTD**)
- Any other file type is treated as documentation.
- Zip archives containing the above types of files.

Large zip files may take some time to process. The publisher aborts if the process is running after an hour.

If this occurs, HP Software recommend splitting the zip file into smaller archives and submitting them separately.

To publish service infrastructure definitions:

1. In the Tools tab menu New section, click **Upload Data Content**.

   The Upload Data Content page opens.

2. Do one of the following:

   - **To upload from a local file system:**

     1. Select **Local File**.
     2. Use **Browse** or input a file path.
     3. Input the Location to store the data content files.

Click **View Locations** to browse the locations workspace.

- **To upload from a remote location:**

  1 Select **Remote File**.

  2 Input the URL for the remote file location.

  3 Input the Location to store the data content files.

  Click **View Locations** to browse the locations workspace.

  4 Input the Base URL which is the part of the URL location to ignore when creating the publishing location.

  5 Select a Synchronization policy for change management.

  For more details, see Synchronization Policy on page 262.

  The final publishing location for remote resources is determined by the Input URL, the Location and the Base URL, as follows:

  If you publish a file from `http://server/some/path/somefile.wsdl`, select a publishing location `/mywsdls`, and set the Base URL to `http://server/some`, the final publishing location is `/mywsdls/path/somefile.wsdl`.

3 Select **Create Business Services** if your external resource contains implementation definitions and you want to create a business service artifacts to associate them with.

4 Click **Next**.

The publisher processes the content of the file and the Publishing Overview page opens. This page displays a list of the content of the file and a decomposition of any definition documents. The page displays the artifacts to create and a publishing status compared to existing artifacts.

The content is listed with the following possible statuses:

- **New**

  A new artifact will be created.

- **Update**

  The artifact already exists and will be updated.

- **Duplicate**

  A similar artifact exists, usually in a different publishing location.

- **Identical**

  An identical artifact exists, usually in the same publishing location.

- **Error**

  The publisher encountered an problem processing this content.

- **Warning**

  Additional warnings reported.

It is possible for particular content to have multiple statuses.

If there are any publishing problems, a warning box displays and you can click **Details** to view the specific problems for particular content.

5 Select the file content to publish and then click **Finish**.

SOA Systinet processes the selected content and creates the associated artifacts. The Publishing Result page opens.

De-selecting any content also removes any referenced dependent content as well.

6 Review the Publishing Result page and click **OK** to return to the Tools tab.

If you accessed the publisher functionality from another page, that page re-opens.

SOA Systinet also uses the definition document processing functionality of the publisher if you publish a document using the following functionality:

- Adding documents to SOA Systinet with an associated external resource.

  For details, see Adding Documentation on page 241 and Managing Definition Data on page 244.

- Adding a SOAP Service implementation to a business service.

  For details, see Adding SOAP Services on page 79.

- Adding an XSD definition to an XML service.

  For details, see Adding an XML Service Definition on page 87.

Importing Services from Registries

SOA Systinet enables you to import services and associated entities from a UDDI Registry.

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.

For details, see "Registry Setup and Configuration" in the *HP SOA Systinet Administration Guide* .

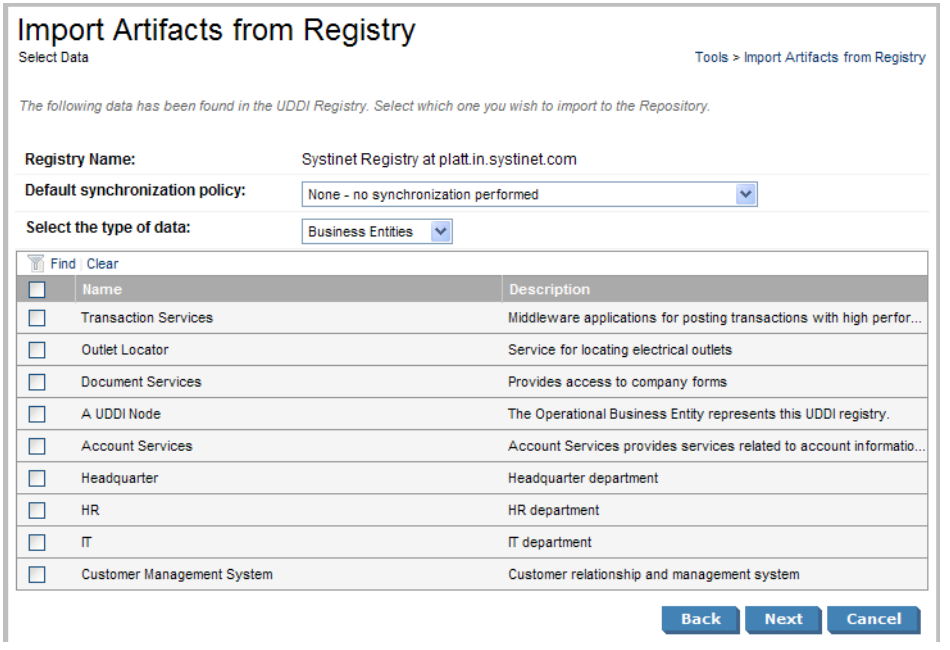
To import data from a UDDI registry:

1 In the Tools tab menu, under Registry Content, click **Import Registry Content** to open the Import Artifacts from Registry page.

2 In the Import Artifacts from Registry, select a registry from the drop-down list or click **New**, to create a new registry artifact.

For details about creating a registry artifact, see "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

Parameter	Definition
Default synchronization policy	Select a policy from the drop-down list. For more details see Synchronization Policy on page 262
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 then click **Next**.

6 In the summary page, verify the data to be imported, and then click **Finish**.

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 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>

BAC/UCMDB Service Discovery

SOA Systinet enables you to import services from the Universal Configuration Management Database (UCMDB) used by *HP Business Availability Center* (BAC).

BAC/UCMDB server must be integrated with SOA Systinet.

For details, see "Setting Up BAC/UCMDB Integration" in the *HP SOA Systinet Administration Guide* .

To import services from BAC/UCMDB:

1 In the Services tab menu Service Discovery section, click **BAC/UCMDB** .

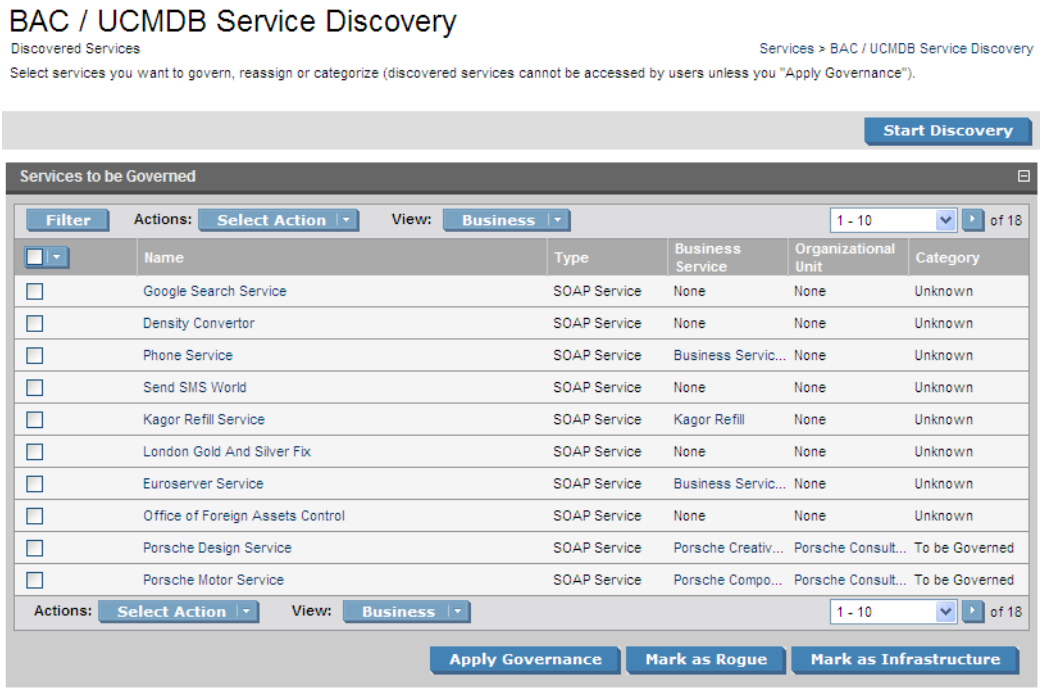
The BAC/UCMDB Service Discovery page opens.

2 Click **Start Discovery**.

The page is populated with a list of services from the BAC/UCMDB server that are not already in governance in SOA Systinet, or have not been marked as rogue or infrastructure. The equivalent artifacts are created in the SOA Systinet repository for newly discovered services.

This process takes some time. The process is executed asynchronously, so you can navigate away from this screen and come back to it later.

Figure 30. BAC/UCMDB Service Discovery



You can process services imported from BAC/UCMDB.

For details, see the following sections:

- Governing Discovered Services on page 108

  Put services into a governance lifecycle process.

- Marking Discovered Services as Rogue on page 110

  Mark discovered services as unnecessary and ignore them in subsequent discoveries.

- Marking Discovered Services as Infrastructure on page 110

  Mark discovered services as background services and ignore them in subsequent discoveries.

After discovery, services are monitored for changes and can be synchronized.

For details, see Synchronizing Discovered Services on page 111.

In addition, you can use bulk operations on these services using the functionality in the **Actions** menu.

These actions are the same as those described in List Views on page 54.

Governing Discovered Services

You can start lifecycle management for the services imported from BAC/UCMDB.

For details about Lifecycle Management, see Chapter 11, Lifecycle Governance.

The govern discovered service process checks the repository for matching artifacts and resolves potential conflicts. The default rules for a conflict are determined by a configuration file. The default behaviour is to check for artifacts with matching *name* properties. For SOAP Services, SOA Systinet checks for matching *serviceName* and *serviceNamespace* properties before checking the *name*.

A matching Business Service, SOAP Service, or Organizational Unit in the repository is assumed to be the same entity discovered in BAC/UCMDB. The artifact properties in the repository version are overwritten by the properties of the discovered entity. These properties are defined by a mapping file.

Any existing relationships with the existing repository artifact are preserved with the exception of previously discovered entities. For example, a Business Service created in SOA Systinet is implemented with a SOAP Service previously discovered in BAC/UCMDB. The same business service in BAC/UCMDB has the SOAP service removed and is then discovered. SOA Systinet removes the relationship to that SOAP Service.

In the event that there are two or more artifacts in SOA Systinet that conflict with a discovered entity, you must resolve the conflict manually as described in To govern discovered services:.

To govern discovered services:

1 In the Services tab menu Service Discovery section, click **BAC/UCMDB**.

The BAC/UCMDB Service Discovery page opens.

2 Select the services to enter into governance, and click **Apply Governance**.

The Govern Discovered Services page opens.

3 If the default governance process is not the correct process, use **Change** to select one.

4 Select the lifecycle stage at which to enter the governance process, and select **Stage Completed** if all the requirements of the lifecycle stage are complete.

5 Do one of the following:

- If there are no unresolved conflicts, click **Save** to enter the service into the selected governance process.

  The BAC/UCMDB Service Discovery page re-opens and the newly governed service is removed from the list of discovered services.

- If there are conflicts that require manual resolution, click **Next**.

  The Resolve Ambiguities page opens.

6 Do any of the following:

- To leave the discovered entities ungoverned, select the entities and click **Skip**.
- To create a new artifacts without merging with existing ones, select the entities and click **Mark as New**.
- To merge a discovered entity with an existing artifact, click **Map to** for the entity, select the artifact to merge and click OK.

Each action changes the **Resolve as** status.

7 Do one of the following:

- If there are conflicts for another artifact type, click **Next** and return to Step 6 for that artifact type.
- When all the conflicts are resolved, click **Finish** to perform your selected actions.

Marking Discovered Services as Rogue

Some of the discovered services may not be useful or necessary. Marking them as rogue makes them invisible in the SOA Systinet UI and ignores them in subsequent discovery processes.

To mark a discovered service as rogue:

1 In the Services tab menu Service Discovery section, click **BAC/UCMDB**.

The BAC/UCMDB Service Discovery page opens.

2 Select the services to mark as rogue, and click **Mark as Rogue**.

The Govern Discovered Services page opens.

3 Review the list of services, and then click **Mark as Rogue**.

The BAC/UCMDB Service Discovery page re-opens and the rogue service is removed from the list of discovered services.

Marking Discovered Services as Infrastructure

Some discovered services may be internal parts of third party products. Marking them as infrastructure makes them invisible in the SOA Systinet UI and ignores them in subsequent discovery processes.

To mark a discovered service as infrastructure:

1 In the Services tab menu Service Discovery section, click **BAC/UCMDB**.

The BAC/UCMDB Service Discovery page opens.

2 Select the services to mark as infrastructure, and click **Mark as Infrastructure**.

The Govern Discovered Services page opens.

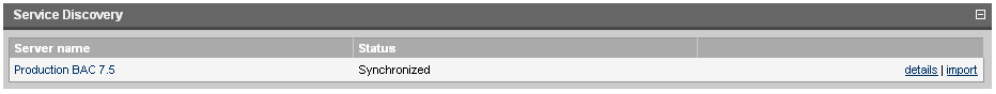
3 Review the list of services, and then click **Mark as Infrastructure**.

The BAC/UCMDB Service Discovery page re-opens and the infrastructure service is removed from the list of discovered services.

Synchronizing Discovered Services

Services discovered in BAC/UCMDB and entered into governance in SOA Systinet are monitored for changes.

The Service Discovery section of the Services view of a discovered services displays the source of the service, and it synchronization status:



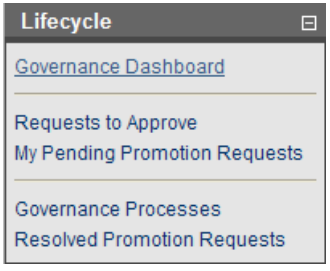
Click **details** to view more information about the status and source of the discovered service.

Click **import** to update the SOA Systinet artifact with the latest changes from BAC/UCMDB.

11 Lifecycle Governance

SOA Systinet provides functionality that enables you to manage the lifecycle of artifacts by creating approval definition processes. Each artifact can then be associated with a different governance process.

In the Services tab, the **Lifecycle** section gives access to these features:



- **Governance Dashboard**

  Opens an overview page of governance records in which you have an interest.

- **Requests to Approve**

  Opens an overview page of promotion requests that require your approval. An overview of the last five requests is available in the Governance Dashboard.

- **My Pending Promotion Requests**

  Opens an overview page of all your promotion requests that require approval from other parties. An overview of the last five requests is available in the Governance Dashboard.

- **Governance Processes**

  Opens an overview page of all governance processes.

- **Resolved Promotion Requests**

  Opens an overview page of all resolved (historical) promotion requests.

The lifecycle process described in this chapter is based on the standard lifecycle taxonomy provided with SOA Systinet. You can modify the lifecycle taxonomy with using HP SOA Systinet Taxonomy Editor.

For details, see the *HP SOA Systinet Taxonomy Editor Guide*.

The lifecycle management procedures are described in the following sections:

- Defining Governance Processes on page 114
- Managing Governance Processes on page 123
- Governing Artifacts on page 125
- Lifecycle Reports on page 130

Defining Governance Processes

Governance is a combination of processes, practices and tools which facilitate the lifecycle of artifacts. SOA Systinet lifecycle governance enables the successful management of processes, their associated stages, and the creation and management of approval processes, tasks, and policies.

Only the Administrator can create a governance process.

The creation of a governance process is described in the following sections:

- Creating a Governance Process on page 115

  Explains how to create an initial governance process.

- Cloning a Governance Process on page 118

Describes how to clone an existing governance process.

- Defining Lifecycle Stages on page 119

  Explains how to define lifecycle stages of primary and secondary artifacts.

- Copying Lifecycle Stages on page 122

  Shows how to copy previously defined lifecycle stages.

- Deleting Lifecycle Stages on page 123

  Shows how to delete previously defined lifecycle stages.

Creating a Governance Process

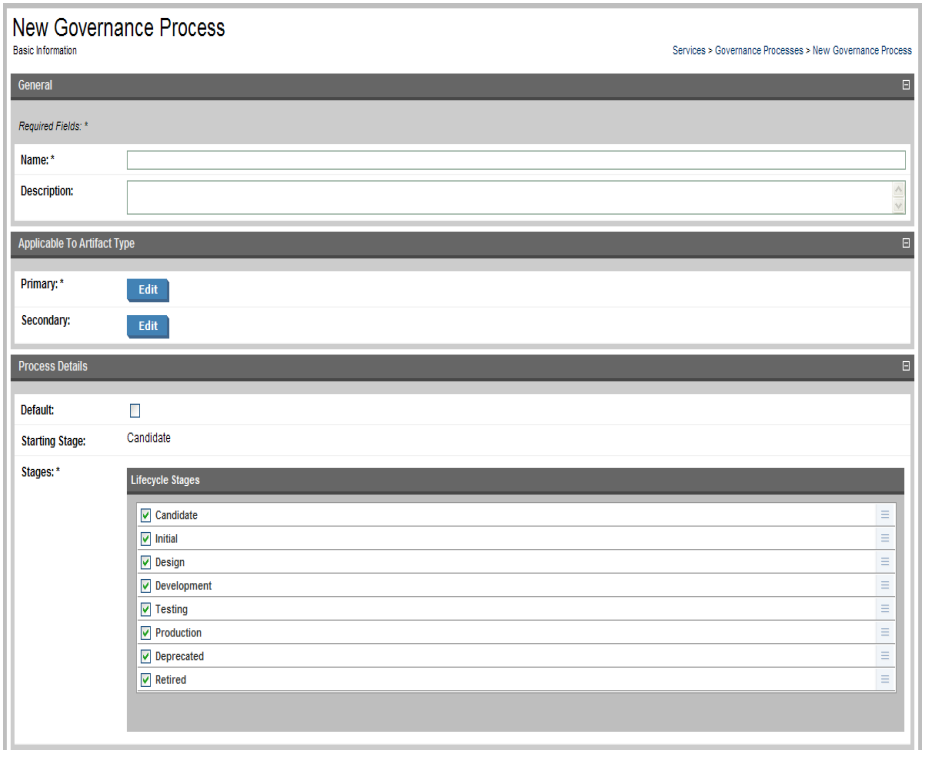
The first stage in artifact lifecycle management is the creation of a governance process.

To create a new governance process:

1. In the Lifecycle menu of the Services tab, click **Governance Processes** to open the Governance Processes page, and then click **New**.

   The **New Governance Process** page opens, as shown in Figure 31.

Figure 31. New Governance Process



2 In the **General** pane, enter a **Name** and **Description** for the governance process.

3 In the **Applicable to Artifact Type** pane, select the **Primary** (required) and **Secondary** (optional) artifacts to be governed.

To select artifact types, do the following:

- Click **Edit** to open a list of available artifact types.
- Browse or use the Quick Find box to select the artifacts you need and click **OK**.

4 In the **Process Details** pane, define the lifecycle stages for the governance process, as follows:

- If you want this process to be used automatically when defining further governance processes, select the **Default** check-box.
- The Starting Stage is automatically set to Initial and all lifecycle stages are selected.
- De-select the check-box of the lifecycle stages you do not need.

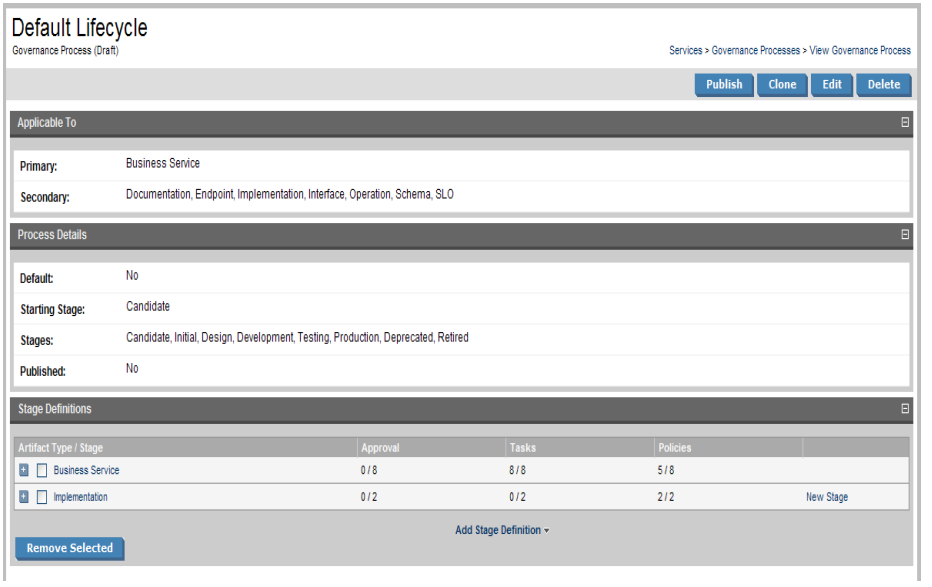
  To reorder lifecycle stages to suit your preferences, you can use the click and drag function.

5 Click **Save**.

The new governance process is now visible in the Governance Processes page, as shown in Figure 32.

As this is a new governance process, the default Published status is **No**.

Figure 32. View Governance Process



Cloning a Governance Process

Creating governance processes can take some time. SOA Systinet includes a feature which enables you to create a new governance process with parameters based on an existing governance process, enabling one process to be used as a template in the creation of others.

To clone a governance process:

1. In the Lifecycle menu of the Services tab, select **Governance Processes** to open the Governance Processes page.
2. Click the required process to open the **Governance Process** page, and click **Clone**.
3. To edit the cloned governance process, click **Edit** and follow the procedure from Step 2 of Creating a Governance Process on page 115.

Defining Lifecycle Stages

Lifecycle stages represent important milestones in the governance process.

The lifecycle stages and their order are defined in the governance process definition. Preconditions of stage promotion can be set in the lifecycle stages of primary and secondary artifacts.

To define lifecycle stages:

1 In the Lifecycle menu of the Services tab, click **Governance Processes** to open the Governance Processes page, and then click the name of the required process.

The Governance Process page opens.

2 For primary artifacts, do the following:

- In the Stage Definitions pane, expand the primary artifact node to open the list of defined stages and click **Edit** next to the stage you want to modify.

  The Edit Stage Definition page opens.

- In the Next Stage field, click **Edit** to open a list of available stages and select the ones you want to follow the current stage.

  Proceed to Step 4.

3 For secondary artifact, do the following:

- In the Stage Definitions pane, navigate to and click **Add Stage Definition** to open the drop-down list, and then select the name of the secondary artifact you want.

  The Edit Stage Definition page opens.

- In the Stage field, open the drop down list of available stages and select the one you want to define.

  Proceed to Step 4.

4 In the **Approval** field, enter the total number of votes, from individual users and group members, required to approve the promotion request, and then do the following:

- To add an individual voter:

  1 Click **Add Users** to open the search view.

  2 In the **Search for** field, enter the name to search - using an asterisk (*) as a wildcard, and then select whether you want to search by **Full Name** or **Login Name** from the drop down menu.

  3 Click **Go** to show matching search results.

  4 Click **Add** next to the name that you want.

  The selected voters are now visible in the Approval field.

  Select the **Required** check-box to make voters mandatory.

- To remove an individual voter, click **Remove** next to the name you want.

  The removed voters are no longer visible in the Approval field.

- To add a group voter, do the following:

  1 Click **Add Groups** to open the search view.

  2 In the **Search for** field, enter the name to search - using an asterisk (*) as a wildcard.

  3 Click **Go** to show matching search results.

  4 Click **Add** next to the name that you want.

  The selected group voters are now visible in the Approval field.

  5 In **Total Required Votes**, enter the number of votes required from group members.

- To remove a group voter, click **Remove** next to the name you want.

  The removed group voters are no longer visible in the Approval field.

5 In the **Tasks** field, you can add, remove, or edit associated tasks.

To create a task, do the following:

- Click **Add** to open the **Add Task** view.
- Enter a name and description of the task.
- Select the check-box **Completion Tracking** if completion of this task is required prior to stage promotion.
- Click **Add**.

  The new task is visible in the Task view.

To edit an associated task, click the **Edit** link to the right of the task, edit the parameters as required, and then, click **Save**.

To remove tasks, select the check-box to the left of the task name, and click **Remove**.

The tasks are no longer visible in the Task view.

6 In the **Policies** field, you can add and remove predefined technical policies.

To associate technical policies, do the following:

- Click **Add** to open the **Add Policy** pane, then do one of the following:

  1 Browse for and select the policies you need, and click **Add**.

  2 In the **Search for** field enter the text to search - using an asterisk (*) as a wildcard, and select whether to search by name or description.

  3 Click **Go** to show matching search results.

  The selected policies are now visible in the Policies view.

  Click the **Required** check-box for policies that must pass validation prior to stage promotion.

- To remove an associated policy, select the check-box to the left of the policy name, and click **Remove**.

  The removed polices are no longer visible in the Policies view.

7 Click **Save**.

The stage definition is updated in the Stage Definitions pane.

To view definitions of all stages of a specific artifact, click the artifact name in the Stage Definitions pane to open the Stage Definitions page.

All stage details are listed. You can edit and copy each stage definition, using **Edit** and **Copy**.

Copying Lifecycle Stages

As with cloning a governance process, SOA Systinet makes it easier for you to define lifecycle stages by enabling you to copy details from one lifecycle stage to another.

To copy a lifecycle stage definition:

1 In the Stage Definitions pane, expand the required artifact type to view available stages, and then click **Copy** next to the stage that you want.

The **Copy Stage** page opens.

2 In the Destination pane, do the following:

- In the Stage field, click **Edit** to open a list of available stages, select the destination stages you need, and then click **OK**.
- In the Artifact Type field, click **Edit** to open a list of available artifacts, select the destination artifacts, and then click **OK**.

3 In the What To Copy pane, select whether to copy the associated approvals, tasks, or policies from the source stage, and then click **Save**.

The destination stages are updated in the Stage Definition pane.

Deleting Lifecycle Stages

You can delete lifecycle stages after they have been defined.

To delete a lifecycle stage definition:

- In the Stage Definitions pane, do one of the following:
  - Select the check-box next to the artifact you need and click **Remove Selected**.

    All stage definitions for the artifact are deleted.
  - Expand the node of the artifact you need to view its stages.

    Select the check-box next to the stage you want to delete and click **Remove Selected**.

    The selected stage definitions are deleted.

Managing Governance Processes

Before a governance process can be successfully used, you must publish it.

The publication and management of a governance process is described in the following sections:

Publishing a Governance Process

After creating a governance process, the next step is to make it available for the governance of artifacts.

To publish a governance process:

- From the Lifecycle menu of the Services tab, click **Governance Processes** to open the Governance Process page, and then do one of the following:
  - Select the check-box next to the name of the governance process you need and click **Publish**.
  - Click the name of the governance process you need to open the Governance Process page, and click **Publish**.

This governance process is now available to be used in the governance of primary and secondary artifacts.

Deprecating a Governance Process

If you need to make a governance process **unavailable** for the governance of artifacts, you can deprecate it.

To deprecate a governance process:

- From the Lifecycle menu of the Services tab, click **Governance Processes** to open the Governance Process page, and then do one of the following:
  - Select the check-box next to the name of the governance process you need and click **Deprecate**.
  - Click the name of the governance process you need to open the Governance Process page, and click **Deprecate**.

  The governance process is deprecated and its status is changed to **Draft** and is not available for the governance of artifacts until it is published.

Deleting a Governance Process

If a governance process is no longer being used in the governance of artifacts, you can delete it.

To delete a governance process:

- From the Lifecycle menu of the Services tab, click **Governance Processes** to open the Governance Process page, and then do one of the following:

- Select the check-box next to the name of the governance process you need and click **Delete**.
- Click the name of the governance process you need to open the Governance Process page, and click **Delete**.

The governance process is deleted and is no longer available to be used in the governance of artifacts.

Governing Artifacts

During the process of artifact governance, each lifecycle stage represents an important milestone. Depending on the configuration of the lifecycle stage, requests for promotion to the next lifecycle stage require approval.

The Administrator has the ability to change governance processes, lifecycle stages, and to force promotion without approval.

You can do this from the Manage Governance page of the artifact Stage Details.

The promotion of a lifecycle stage is described in the following sections:

- Starting Artifact Governance on page 125
- Managing Associated Policies and Tasks on page 126
- Submitting a Promotion Request on page 127
- Handling Promotion Requests on page 129
- Ending Artifact Governance on page 130

Starting Artifact Governance

This function enables the governance of an artifact that is not currently governed, and where the artifact will act as the primary artifact in an existing governance process.

To start governing an artifact:

1. From the browse page of any ungoverned artifact, open the Governance menu and select **Start Governance**.

The Start Governance page opens.

2 In the Process field, select the process you want to use and click **OK**.

Managing Associated Policies and Tasks

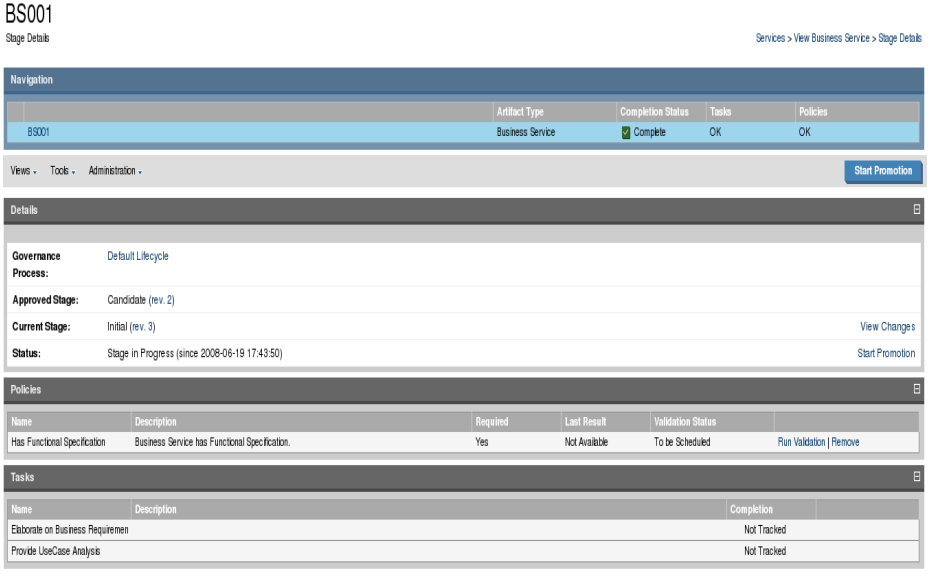
To ensure promotion of stages, it is important that you successfully manage policies and tasks associated with an artifact under governance.

To manage policies associated with a governed artifact:

1 From the browse page of any governed artifact, navigate to the Governance pane and click **Details**.

The Stage Details page opens, as shown in Figure 33.

Figure 33. Stage Details



2 In the Policies pane, do one of the following:

- Click **Run Validation** next to the policy you need to validate.

  If the result of validation is available, it is shown in the **Last Result** column of the Policies pane.

- Click **Remove** next to a policy name to delete it.

This option is only available if you are the Administrator.

To manage tasks associated with a governed artifact:

1 From the browse page of any governed artifact, navigate to the Governance pane and click **Details**.

The Stage Details page opens.

2 In the Tasks pane, depending whether the Completion column shows the task as incomplete or complete, you can click **Mark as Complete** or **Mark as Incomplete** to change the status.

To manage policies and tasks in related artifact, click the artifact name in the Navigation pane and follow the procedures To manage policies associated with a governed artifact: and To manage tasks associated with a governed artifact:.

Submitting a Promotion Request

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

Promotion can only be requested on a **primary** artifact and only when all mandatory tasks are complete on all related artifacts.

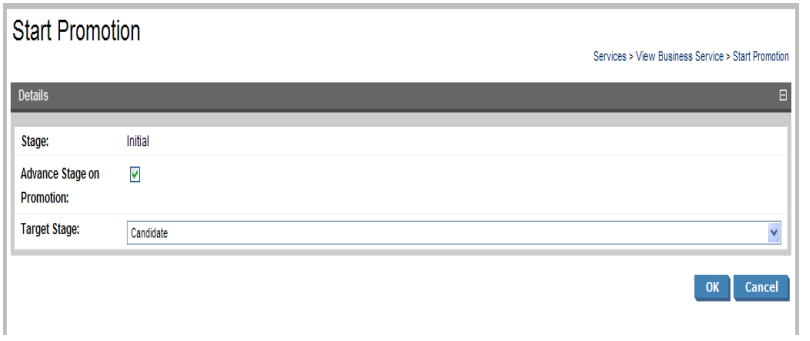
To submit a promotion request:

1 From the browse page of any governed primary artifact, navigate to the Governance pane and click **Details**.

The Stage Details page opens.

2 Click **Start Promotion** to open the Start Promotion page, as shown in Figure 34.

Figure 34. Start Promotion



3 To promote stages automatically after an approved promotion request, select the **Advance Stage on Promotion** check-box, and in **Target Stage**, select the next stage from the drop down list.

If you do not select the check-box, you must make this change manually from the Stage Details page by expanding **Tools→Change Stage to *'stage name'*** .

This can only be done after stage approval.

4 Click **OK** to send the approval request to the users and groups listed in the Approvers section for the current lifecycle stage.

To check the approval status of a promotion request, open the Stage Details page of the artifact, and then do the following:

- Expand **Views** and select **Approvers** to open the Approvers pane.

Handling Promotion Requests

A request requiring your approval appears in the Requests to Approve page.

To approve or reject a change request:

1 In the Lifecycle menu of the Services tab, click **Requests to Approve** to open the Requests to Approve page.

2 Click the name of the request to open the Promotion Approval page, as shown in Figure 35.

Figure 35. Promotion Approval

3 Review the request and any responses made by other approvers, and then do any of the following:

- **Approve**

  To approve the promotion request. Enter comments if required, and click **Save**.

  This option is only available if you are the Administrator or an Approver.

- **Reject**

  To reject the promotion request. Enter comments if required, and click **Save**.

This option is only available if you are the Administrator or an Approver.

- **Notify Approvers**

  To make comments on the promotion request without approving or rejecting the request.

  This option is only available if you are the Administrator or a Maintainer.

- **Cancel Request**

  To cancel the promotion request.

  This option is only available if you are the Administrator or a Maintainer.

An e-mail is sent to the requester when the required number of votes for that stage are received.

Ending Artifact Governance

This function enables you to end the governance of an artifact.

If the artifact is the secondary artifact in the lifecycle, you can exclude the secondary artifact from the governance process.

To end artifact governance:

1. From the browse page of any governed artifact, navigate to the Governance pane and click **Details** to open the Stage Details page.
2. Expand **Administration→End Governance** to open the End Governance page.
3. In the **Exclude from Governance** field, select the check-box to exclude the artifact from governance.
4. Click **OK**.

   The artifact is no longer governed.

Lifecycle Reports

SOA Systinet enables the production of lifecycle statistics reports.

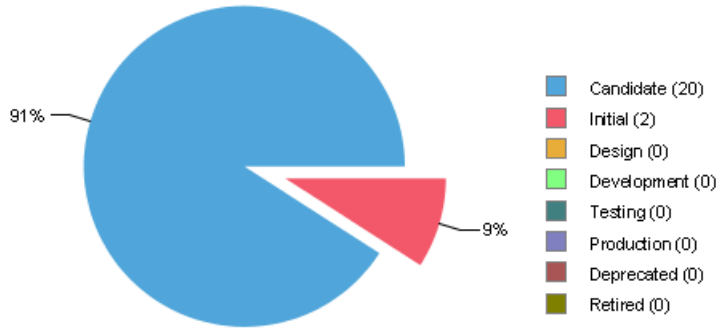
Two reporting tasks can be scheduled, one running a report hourly and the other running a report daily.

The resulting report is dependant on the details specified. However, an example report is shown below.

HP SOA Systinet

Service Lifecycle Statistics

Lifecycle Stage	Number of SERVICES
Candidate	20
Initial	2
Design	0
Development	0
Testing	0
Production	0
Deprecated	0
Retired	0
Total:	22



The available report is always the last scheduled report completed successfully.

To save a copy of a report, you can export it to PDF format.

For details on creating and running reports, see Reporting Tools on page 260.

For details on scheduling tasks, see Tasks and Scheduling on page 267.

For details on searching for reports available to produce, see Reports on page 271.

12 Managing Contracts

SOA Systinet enables contracts to be set up between providers and consumers with associated service level objectives (SLO).

Contract Manager is an additional component of SOA Systinet. If your license does not include Contract Manager these features are not available.

By default the following artifact types are defined as providers and consumers:

Provider Artifact Types	Consumer Artifact Types

• Application
• Business Service
• Implementation
  • SOAP Service
  • XML Service
  • Web Application
• Endpoint
• Operation
	• Application
	• Business Service
	• Implementation
	  • SOAP Service
	  • XML Service
	  • Web Application
	• Contact
	  • User Profile
	  • Organizational Unit

The set of provider and consumer artifacts is configurable.

For details, see "Configuring Consumer and Provider Artifacts" in the *HP SOA Systinet Administrator Guide* .

Contract management is enabled by the following set of procedures:

- Requesting Consumption on page 134
- Processing Consumption Requests on page 136
- Importing Existing Contracts on page 136
- Revoking an Active Contract on page 137

At each stage in the request process SOA Systinet sends mail notifications to the following users:

- Users with write permission for the provider artifact.
- Users with write permission for the consumer artifact.
- Any additional e-mails listed in the provider artifact `stakeHolderEmails` property.
- The administrator is not notified unless they are specifically granted write permission from another source.

Requesting Consumption

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

You can make a request if you have write permission for the consumer artifact (the owner, a member of the owning group, a user with ACL write permission, or the administrator).

To request consumption of a provider artifact:

1. Do one of the following:
   - In the Services tab menu New section, click **Consumption Request**.

- In the service or detail view of a provider artifact that is available for consumption, open the **Consumption** context menu and select **New Request**.

  Skip to Step 4

The New Consumption Request page opens.

2 Select the provider artifact type from the list and then click **Next**.

If there are no available provider artifacts for the selected type SOA Systinet warns you.

3 Use **Filter** to find the provider artifact.

Select the provider from the list and then click **Next**.

4 Select the consumer artifact type from the list and then click **Next**.

If there are no available consumer artifacts for the selected type SOA Systinet warns you.

5 Use **Filter** to find the consumer artifact.

Select the consumer from the list and then click **Next**.

6 If required, select **Select Specific SLO**, select an SLO from the list, and then click **Next**.

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

8 Review the request details and click **Finish** to place your request.

You can view your consumption requests from the Services tab View menu with the **My Consumption Requests** link.

Processing Consumption Requests

When consumers request a provider artifact you must either approve or reject their request.

You can approve or reject a request if you have write permission for the provider artifact (the owner, a member of the owning group, a user with ACL write permission, or the administrator).

To process consumption requests:

1. In the Services menu View section, click **Requests to Approve** to open 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.

If a request is accepted it becomes a contract between the consumer and provider artifacts.

A contract becomes invalid under the following conditions:

- The provider artifact is deleted.
- The consumer artifact is deleted.
- The associated SLO, if there is one, is deleted.

Importing Existing Contracts

There may be existing contracts between providers and consumers that are not stored in the repository.

SOA Systinet enables you to import these contracts without requiring the request approval process.

You can import a contract if you have write permission for the provider artifact (the owner, a member of the owning group, a user with ACL write permission, or the administrator).

To import an existing contract:

1. In the Services menu Import section, click **Existing Contract**.

The Enter Existing Contract page opens.

2 Select the provider artifact type from the list and then click **Next**.

3 Use **Filter** to find the provider artifact.

Select the provider artifact from the list and then click **Next**.

4 Select the consumer artifact type from the list and then click **Next**.

5 Use **Filter** to find the consumer artifact.

Select the consumer artifact from the list and then click **Next**.

6 If required, select **Select Specific SLO**, select one from the list, and then click **Next**.

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

8 Review the details and click **Finish** to create the contract.

Revoking an Active Contract

You may need to cancel an active contract.

You can revoke a contract if you have write permission for the provider artifact (the owner, a member of the owning group, a user with ACL write permission, or the administrator).

To revoke a contract:

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

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

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

Part IV. Policies

Policy Manager enables you to implement your company policy in SOA Systinet and verify the compliance of your service infrastructure. Access the main features of Policy Manager in the **Policies** tab.

Policy Manager is an additional component of SOA Systinet. If your license does not include Policy Manager these features are not available.

The following chapters describe Policy Manager features:

- Chapter 13, Policies UI

  Navigate the Policies UI.

- Chapter 14, Managing Business Policies

  Create and manage business policies.

- Chapter 15, Managing Technical Policies

  Create and manage technical policies.

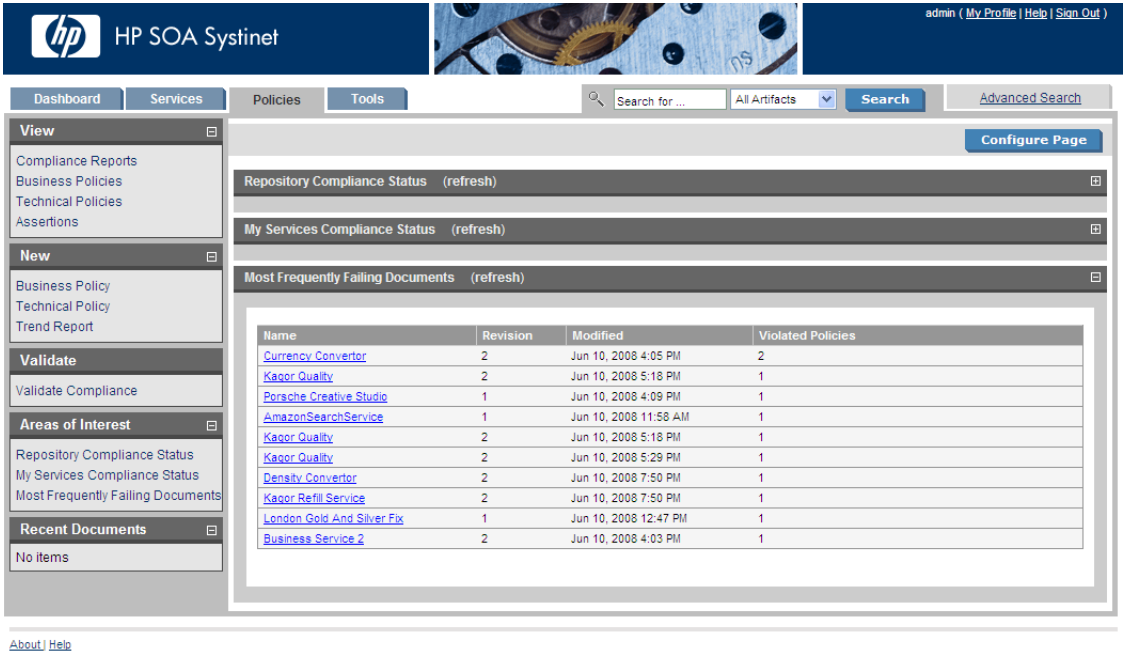
- Chapter 16, Validating Resources

  Validate documents using your policies.

13 Policies UI

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.

Figure 36. 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 142
- Areas of Interest on page 145

- Policy Pages on page 147

Policies Menu

The Policies tab menu is split into collapsible segments.

Each segment is described in the following sections:

- Policies View Menu on page 142

  Access list views of policy artifacts.

- Policies New Menu on page 143

  Create new policy artifacts.

- Validation Menu on page 144

  Validate the policy compliance of an artifact.

- Areas of Interest Menu on page 144

  Click an Area of Interest to return to the main Polices tab.

- **Recent Documents**

  Quick links to the last few artifacts viewed.

Policies View Menu

The View menu in the Policies tab provides links to list views for policy management.

Figure 37. Policies View Menu

The View menu contains the following links:

- Policy List Views

  Links to list views for policy artifacts.

  For details, see Policy and Report List Views on page 148.

Policies New Menu

The New menu in the Policies tab provides quick links to create new policy artifacts.

Figure 38. Policies View Menu

The New menu links to the following policy artifact creation pages:

- **Business Policy**

  Create a new business policy.

  For details. see Creating Business Policies on page 169.

- **Technical Policy**

Create a a new technical policy.

For details, see Creating Technical Policies on page 177.

- **Trend Report**

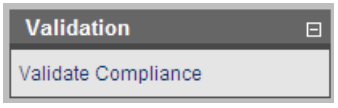
  Create a new trend report.

  For details, see Compliance Trends on page 194.

Validation Menu

The Validation menu in the Dashboard and Policies tab links to policy compliance functionality.

Figure 39. Validation Menu



The Validation menu contains the following functionality:

- **Validate Compliance**

  Start policy compliance validation for a resource.

  For details, see Resource Compliance on page 187.

Areas of Interest Menu

Each Area of Interest selected for display in the Polices tab is shown in the Area of Interest menu.

Figure 40. Areas of Interest Menu

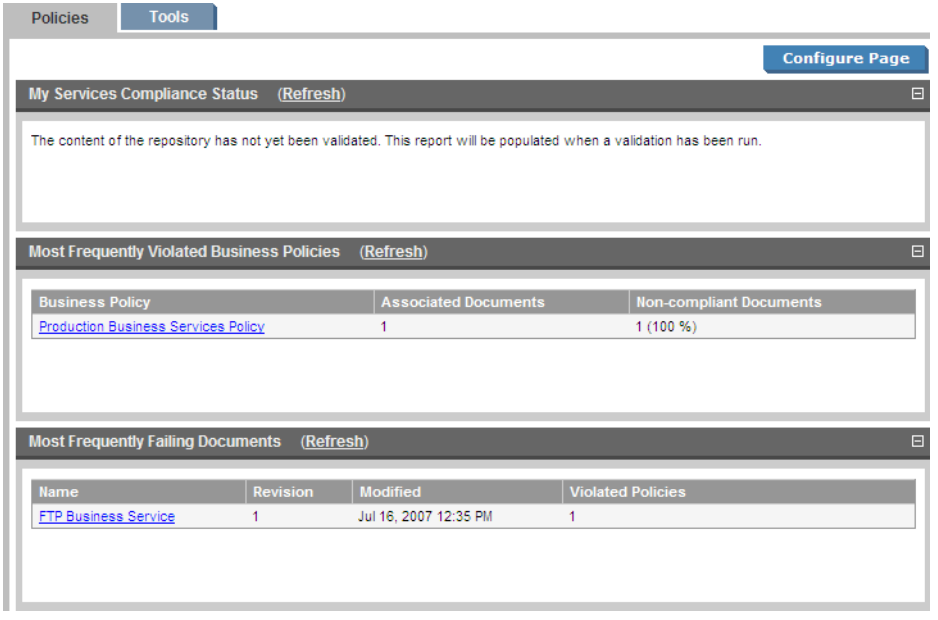
Click an Area of Interest to return to the main Polices tab and expand that Area of Interest if it is closed.

For details about Areas of Interest, see Areas of Interest on page 145.

Areas of Interest

When you open the Policies tab, the page displays Areas of Interest in the main view.

Figure 41. Policies Tab Showing Areas of Interest



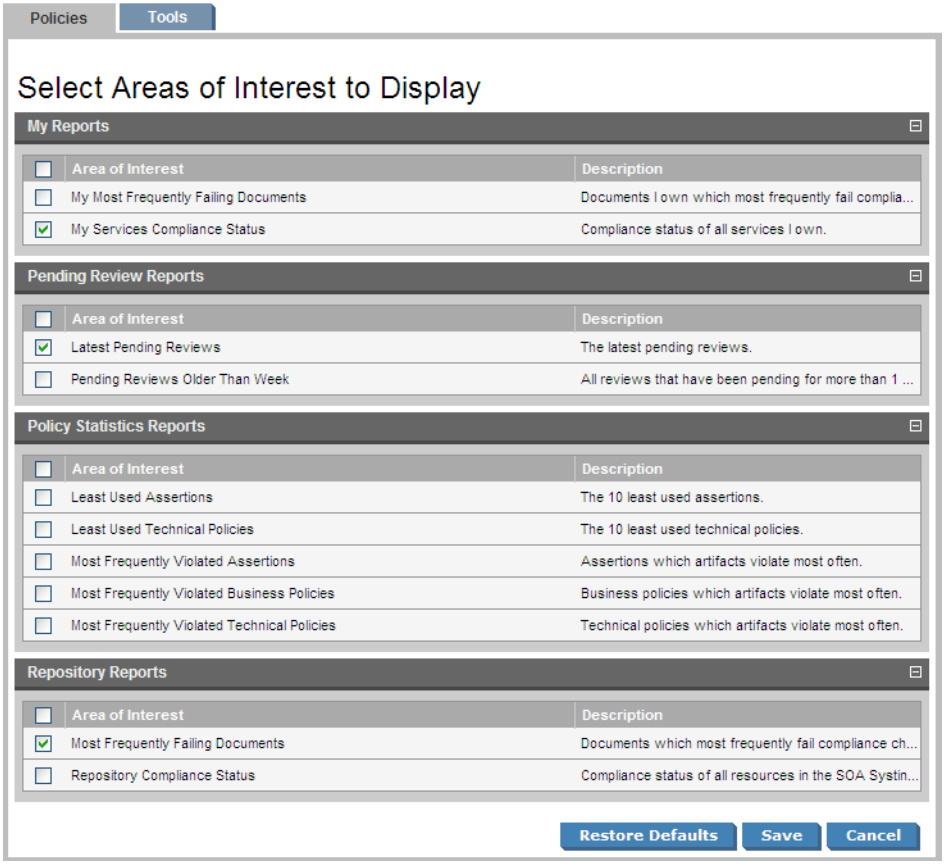
You can return to this view and display a specific Area of Interest at any time by clicking it in the Policies tab Areas of Interest menu.

Areas of Interest do not update when you open them. To see an up-to-date Area of Interest, click **Refresh** after you open it. You may need to refresh the Area of Interest more than once to show the results of a recent action.

HP Software recommend scheduling a task using the AOI Preparation Tool to perform a daily update of all areas of interest. As this task is CPU intensive, it should be scheduled for a non-peak period. See Creating a Task on page 268.

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 42. Select those you want displayed and click **Save**.

Figure 42. Select Areas of Interest to Display



Areas of Interest include the following types:

- **My Reports**

  A report, policy, service, etc. is 'yours' if you own it.

  For details, see Changing Artifact Ownership on page 239.

- **Pending Reviews**

  Some assertions cannot be resolved automatically and require you to decide whether a validated document conforms to the requirements of an assertions (for example, quality requirements). These Areas of Interest list all reports where the final status is pending until manual validation is performed.

  For details, see Reviewing Documents Manually on page 190.

- **Policy Statistics** and **Compliance Status**

  After you resolve policy violating problems, you can reset the statistics for Areas of Interest. All artifact detail pages in Services, Policies, and Tools contain a Compliance context menu with the option to **Reset Compliance Statistics**. This tool deletes all reports for that artifact, policy, or assertion.

  You can also delete all compliance reports in the SOA Systinet repository with the command-line `reset` tool.

  For details, see "Reset Tool" in the *HP SOA Systinet Administration Guide* .

Policy Pages

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

- Policy and Report List Views on page 148

  Index views of policies, reports and assertions.

- Business Policy View on page 149

  The business policy detail page.

- Technical Policy View on page 153

The technical policy detail page.

- Assertion View on page 155

  The assertion detail page.

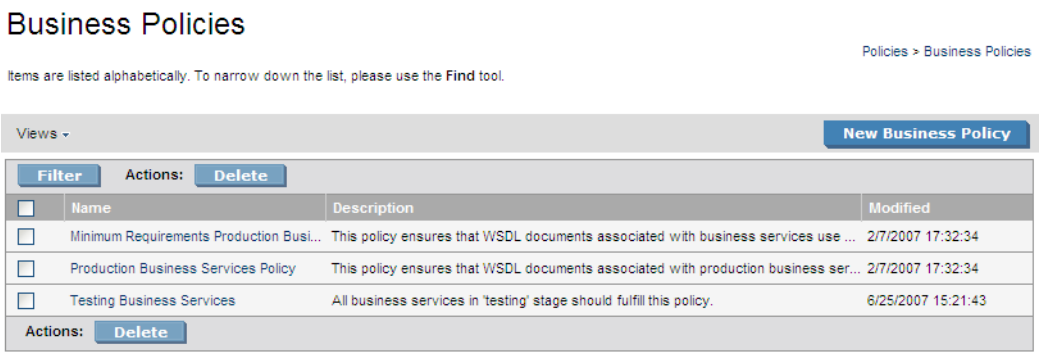
- Report Views on page 158

  The various reports Policy Manager generates.

Policy and Report List Views

Click one of the links in the Polices tab View menu to open a list view of that type of document:

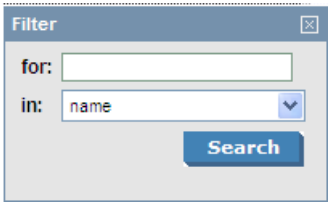
Figure 43. List of Business Policies



You can reduce the list of policy artifacts using **Filter**.

Click **Filter** to open a query window:

Figure 44. Policies List View Filter



To filter the list, enter your search parameter, select a column, and then click **Search**.

Click **Clear Filter** to remove the filter and restore the list of artifacts, or open the Filter menu and select **Edit Filter** to change the filter terms.

All policy list views contain a bulk delete function.

Select the policy artifacts from the list, click **Delete**, and then confirm.

The following functionality is specific to each policy artifact type:

- **Compliance Reports**

  Validate Compliance enables you to execute a new compliance check.

  For details, see Chapter 16, Validating Resources.

- **Business** and **Technical Policies**

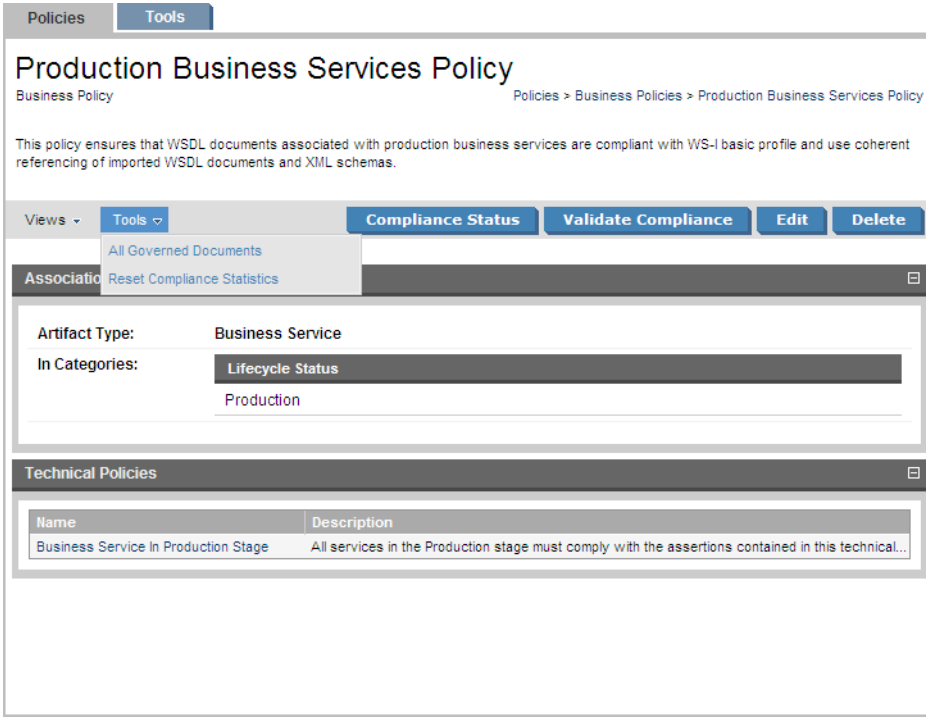
  New Business Policy or **New Technical Policy** enable you to create new policy artifacts.

  For details, see Creating Business Policies on page 169 and Creating Technical Policies on page 177.

Business Policy View

Click the name of a business policy to open the business policy detail view:

Figure 45. Business Policy Details



The business policy detail view lists the technical policies and association rules of the business policy.

This following sections describe the content and functionality of these pages:

- Business Policy Page Context Actions on page 150
- Business Policy Page Content on page 152

Business Policy Page Context Actions

The grey bar contains the following context action menus and functions:

- **Views**:

- **Revisions**

  View the revision history of the artifact.

  For details, see Revision and Version History on page 233.

- **Advanced View**

  Switches to the detailed view of the artifact in the Tools tab.

  For details, see Tools View on page 223

- **Tools**:

  - **All Governed Documents**

    Lists all documents associated with the business policy. You can run a business policy validation from this view.

    For details, see Business Policy Validation on page 186.

  - **Reset Compliance Statistics**

    Deletes compliance reports for this policy, which resets the relevant Area of Interest statistics.

- **Compliance Status**

  View the current compliance status of all artifacts associated with the business policy.

  For details, see Business Policy Summary Reports on page 159.

- **Validate Compliance**

  Validate the documents associated with the business policy against all its technical policies.

  For details, see Business Policy Validation on page 186.

If a specified Additional Artifact associated with the business policy is missing from the repository, you are warned in the detail view. Validations performed on such a policy will automatically fail.

- **Edit**

  Open the Edit view of the business policy.

  For details, see Editing Business Policies on page 174.

- **Delete**

  Delete the business policy.

  Policy deletion is permanent. Deleted polices cannot be recovered.

Business Policy Page Content

The **Association Rules** section includes the following information:

Table 1. Association Rules

Artifact Type	The type of artifact to which the policy applies.
In Categories	The business policy applies to only those artifacts with the selected values in the selected categories.
Not In Category	As **In Categories**, except the business policy *does not* apply to those artifacts with the selected values in the selected category.
Exclude	The business policy does not apply to these specific artifacts.
Additional Artifacts	The business policy applies to these specific artifacts even if the category rules would exclude them.

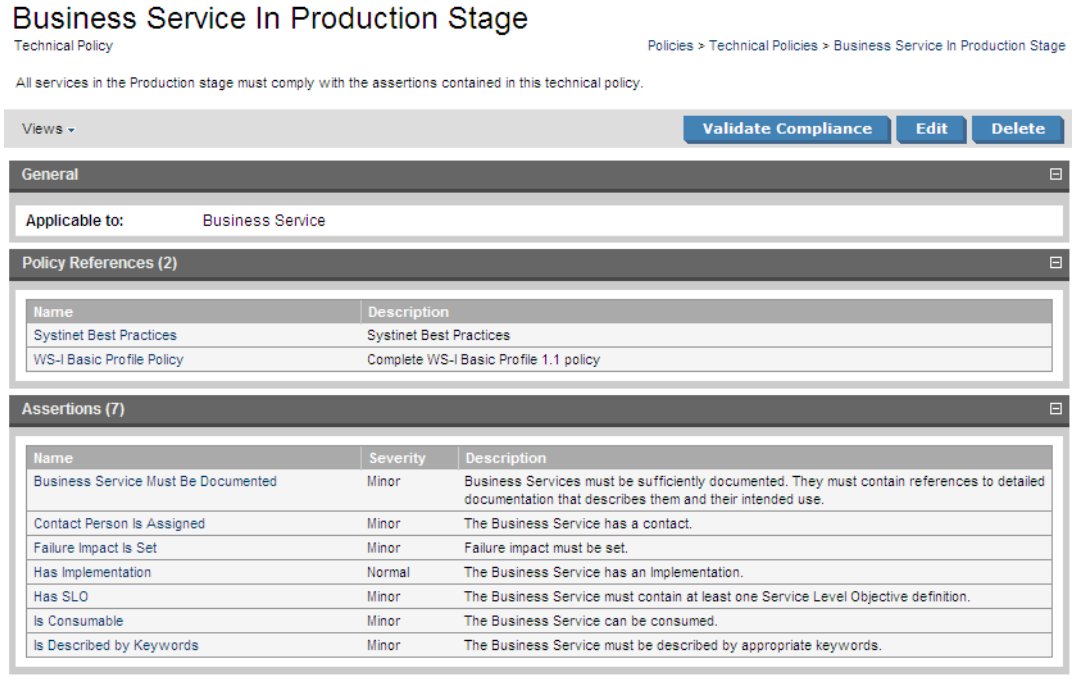
The **Technical Policies** section lists all technical policies associated with an artifact. Click the name of a technical policy to open its detail view.

For details, see Technical Policy View on page 153.

Technical Policy View

Click the name of a technical policy to open the technical policy detail view, shown in Figure 46. The detail view lists the policy's assertions and policy references.

Figure 46. Technical Policy Details



This following sections describe the content and functionality of these pages:

- Technical Policy Page Context Actions on page 154

- Technical Policy Page Content on page 155

Technical Policy Page Context Actions

The grey bar contains the following context action menus and functions:

- **Views**
  - **Revisions**

    View the revision history of the artifact.

    For details, see Revision and Version History on page 233.
  - **Advanced View**

    Switches to the detailed view of the artifact in the Tools tab.

    For details, see Tools View on page 223

- **Validate Compliance**

  Run a compliance check of the technical policy against artifacts. The artifact types to which the policy may apply are listed in the General section as **Applicable to**.

  For details, see Resource Compliance on page 187.
- **Edit**

  Opens a view in to edit the technical policy.

  For details, see Editing Technical Policies on page 181.
- **Delete**

  Delete the technical policy.

  Policy deletion is permanent. Deleted polices cannot be recovered.

Technical Policy Page Content

The content of the technical policy detail page is divided into the following sections:

- **General**

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

- **Policy References**

  A table of other referenced technical policies.

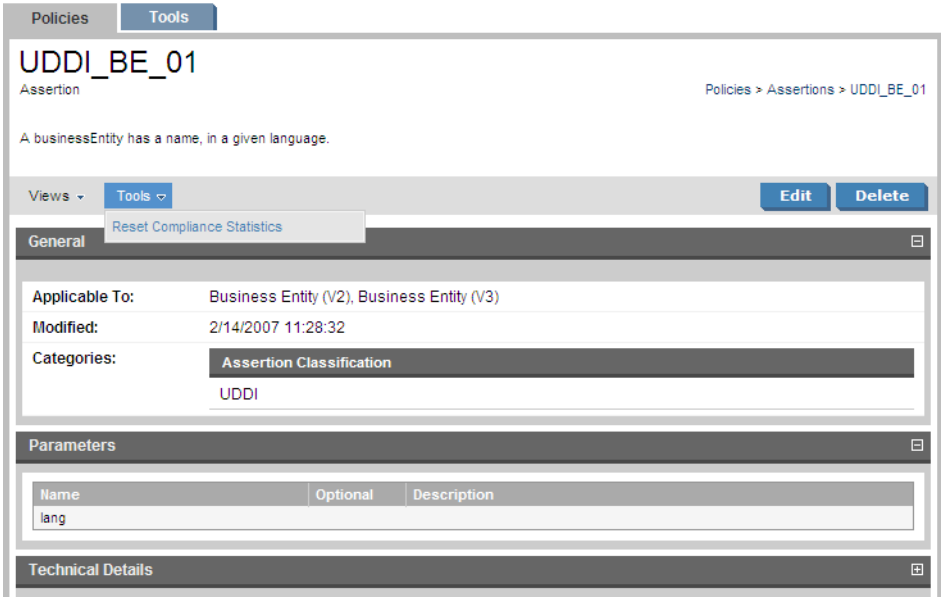
- Assertions

  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.

Assertion View

Click the name of an assertion in the **Assertions** list to open that assertion's detail view, shown in Figure 47.

Figure 47. UDDI BE 01 Assertion

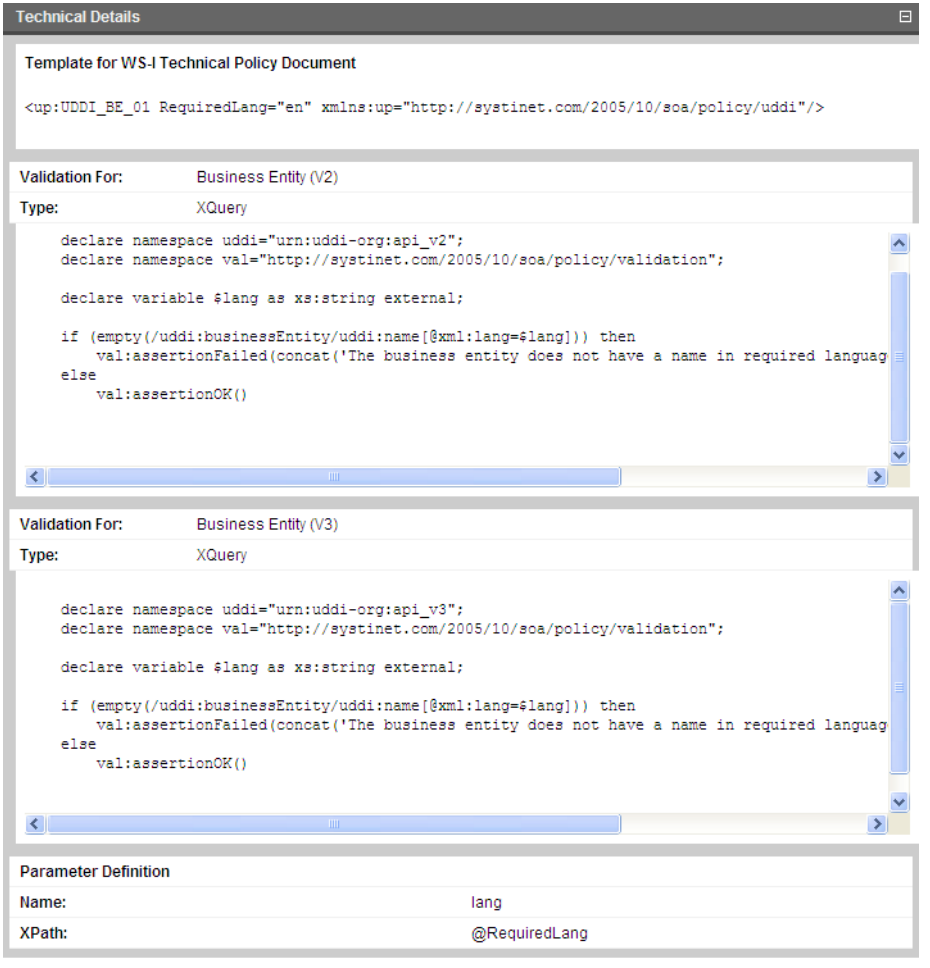


An assertion detail view shows what types of document the assertion applies to, when it was last modified, and the categories to which it belongs. Assertion detail views include a toolbar with the following buttons and context action menus:

- **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 Tools View on page 223. 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 48 are the technical details of the UDDI BE 01 assertion. These details are explained in the Assertion Schema chapter of the Reference Guide.

Figure 48. UDDI BE 01 Technical Details



Report Views

Compliance checks generate the following reports:

- **Business Policy Summary Report**

  Running a business policy validation generates a business policy summary report. This report lists a business policy's associated artifacts, says whether they complied with all of the associated technical policies, and gives a breakdown of how many assertions the artifact complied with, how many it violated and how many require manual review. It includes links to reports for each document.

  For details, see Business Policy Validation on page 186 and Business Policy Summary Reports on page 159.

- **Document Summary Report**

  Validating an artifact against its associated business policies generates a document summary report. This lists an artifact's governing business policies, says whether the artifact complied with them, and gives a breakdown of how many assertions the artifact complied with, how many it violated and how many require manual review. It includes links to reports for each business policy.

  For details, see Document Summary Reports on page 160

- **Document Report**

  A document report describes the compliance of an artifact and its related artifacts with the assertions contained in the policies used to validate the artifact.

  For details, see Document Reports on page 162.

- **Business Policy Report**

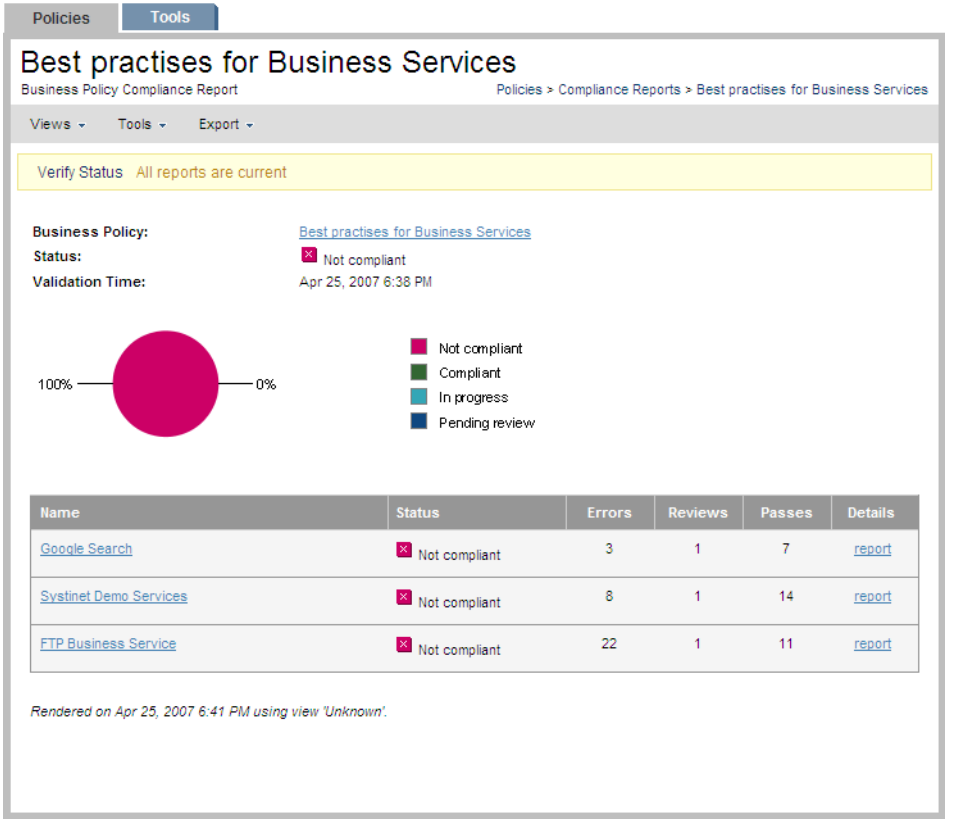
  A business policy report describes the compliance of all artifacts associated with a business policy with the policy's constituent assertions.

  For details, see Business Policy Reports on page 168.

Business Policy Summary Reports

A business policy validation, where all associated documents are validated against the business policy (see Business Policy Validation on page 186), 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 49 shows the summary report for a business policy with three associated documents.

Figure 49. 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.

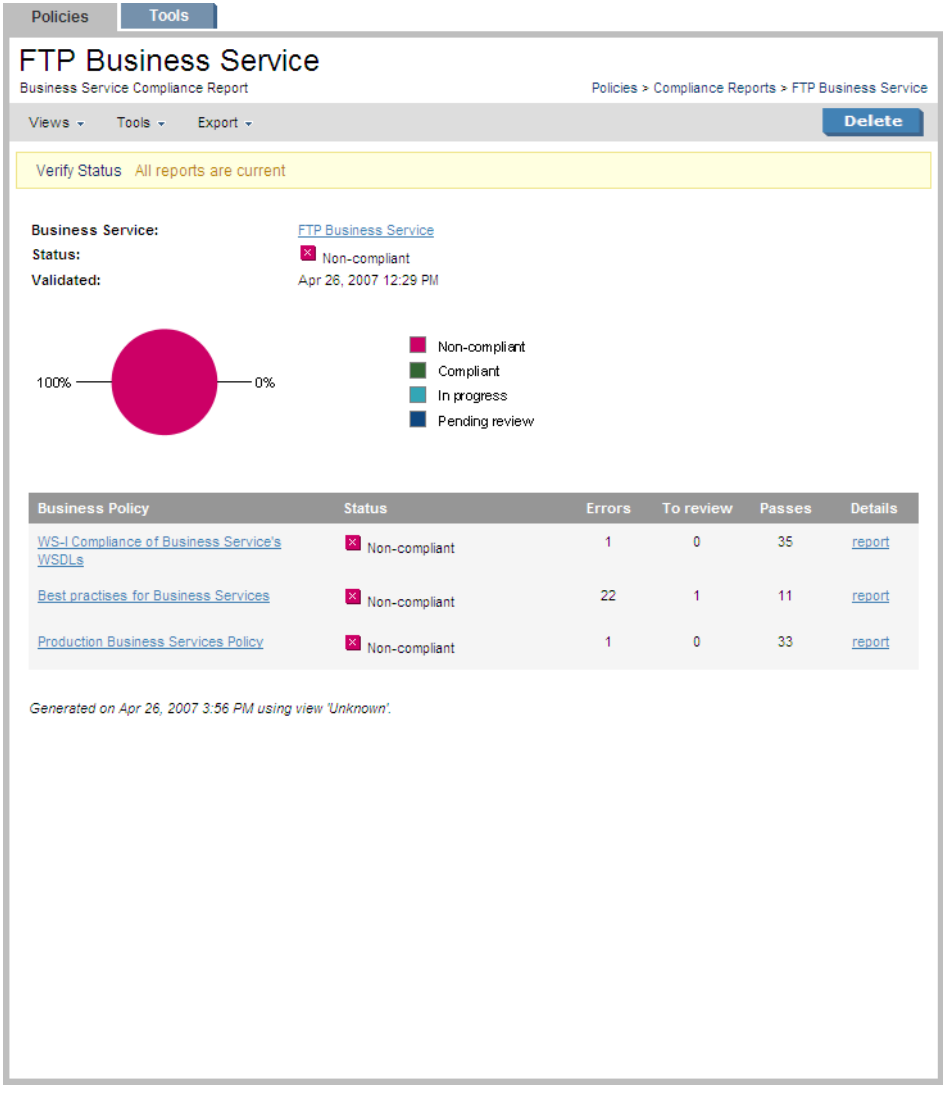
A table of tested documents occupies the bottom of business policy reports. The name of each document is a link to its detail page (see Tools View on page 223). You can see whether a document passed the latest validation, how many assertions it violated (**Failed**), how many it complied with (**Passed**) 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 50 shows the summary report for a document validated against three business policies.

Figure 50. 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 Tools View on page 223). 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 149). 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

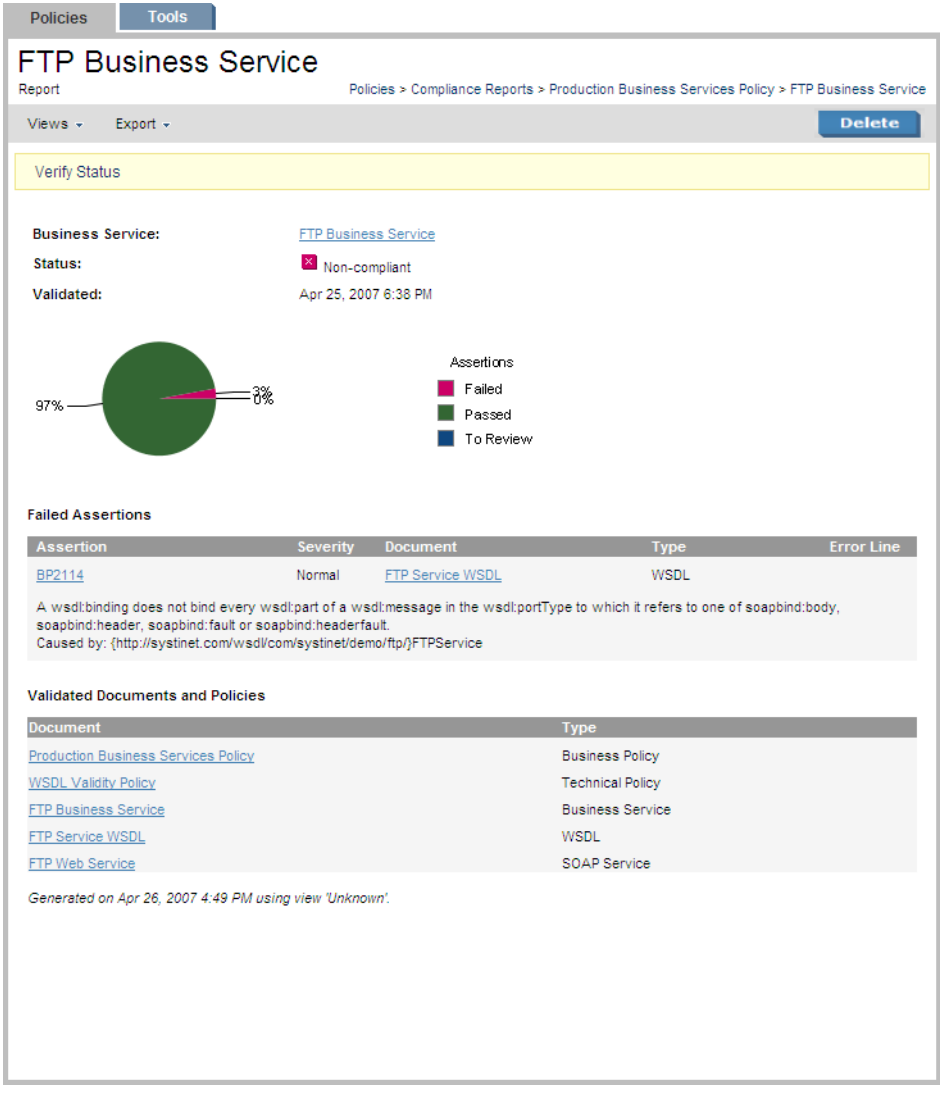
A document report describes the compliance of a document with business and/or technical policies. Document reports are generated in the following cases:

- During business policy validation. They are listed in the business policy summary report.

  For details, see Business Policy Summary Reports on page 159.
- When a single resource is validated.

The report in Figure 51 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 51. 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 50, which gives the percentage of business policies with which it complies.) The name of the document is a link to its detail page (see Tools View on page 223). 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.

- **Export**

  You can export the report as a PDF or .csv file.

- **Delete**

  Deletes the report.

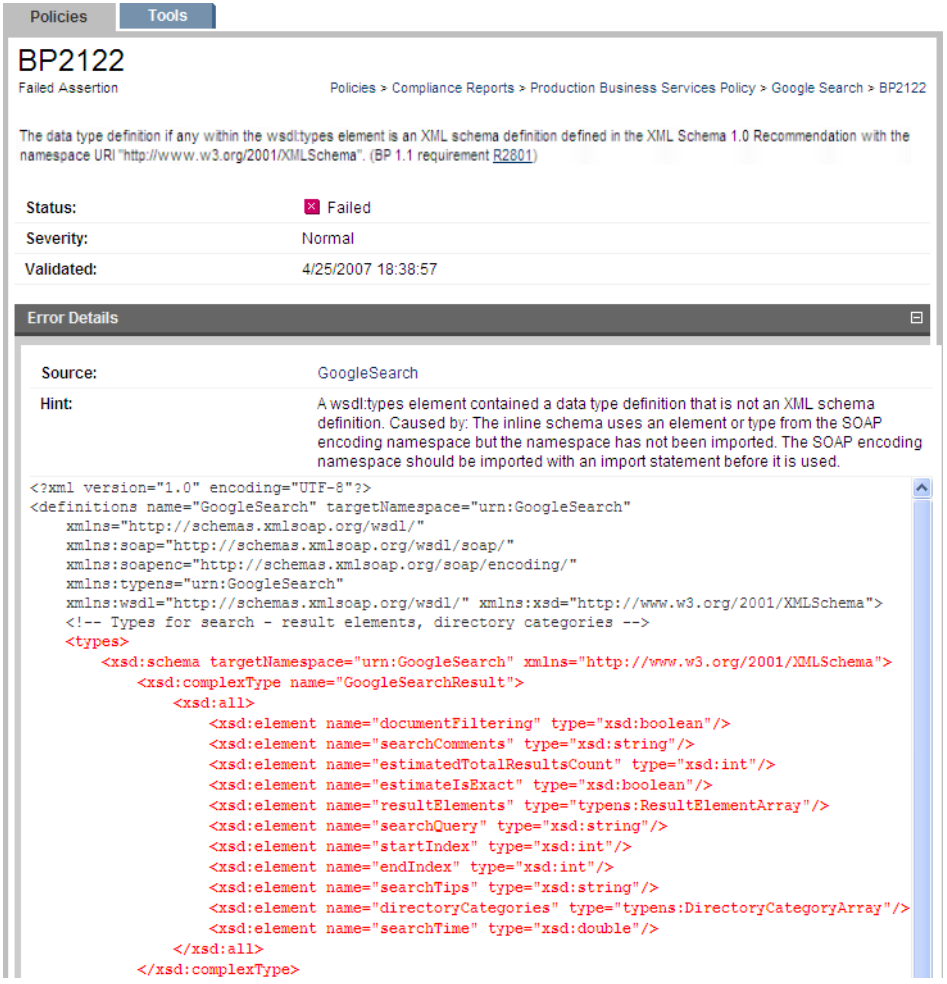
All violated and pending assertions are listed in a table beneath the pie chart. (In the **Full View**, passed assertions are listed as well.) For each assertion, the table shows:

- The name of the assertion. Clicking this opens the compliance status view of the assertion. Figure 52 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 52. 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 162 for details.

14 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

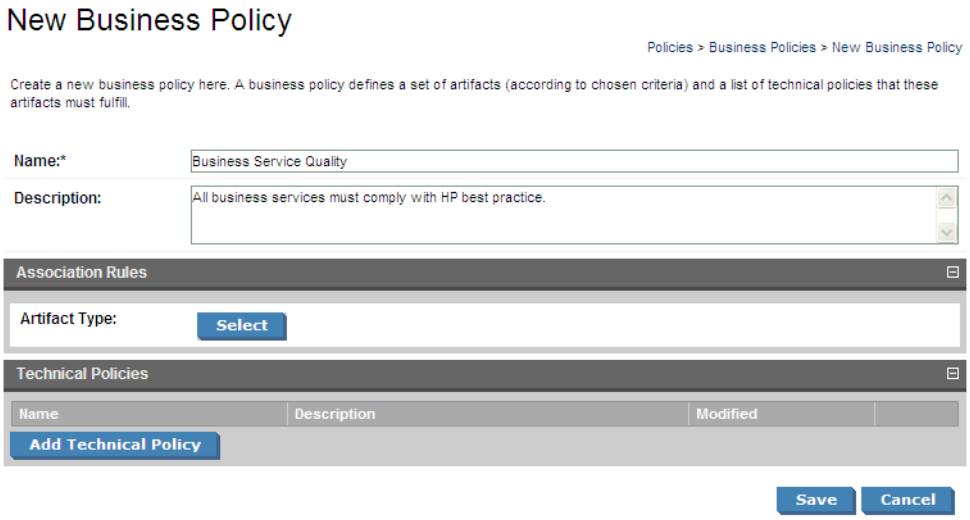
You can create business policies from the menu on the left side of the **Dashboard** and **Policies** tabs and from the business policy list view.

To create a business policy:

1 Do one of the following:

- In the Policies or Dashboard New menu, click **Business Policy**.
- In the list view of business policies, click **New**.

The New Business Policy page opens:



2 Input a name and description for the new business policy.

3 Do any of the following:

- Click **Save** to create a draft policy. You can add association rules and technical policies later by editing the policy.

  For details, see Editing Business Policies on page 174.

- Add Association Rules.

  For details, see Adding Association Rules to a Business Policy.

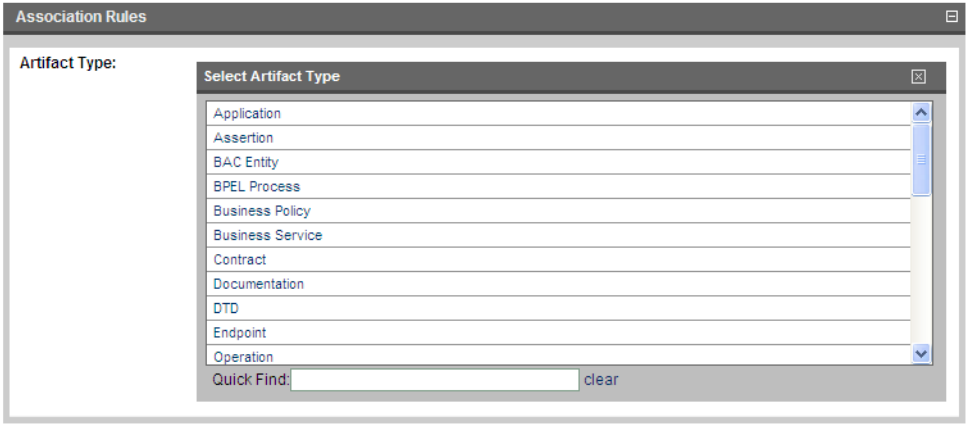
- Add Technical Policies.

  For details, see Adding Technical Policies to a Business Policy.

Adding Association Rules to a Business Policy

1 In the New Business Policy or Edit Business Policy view, in the Association Rules section, click **Select**.

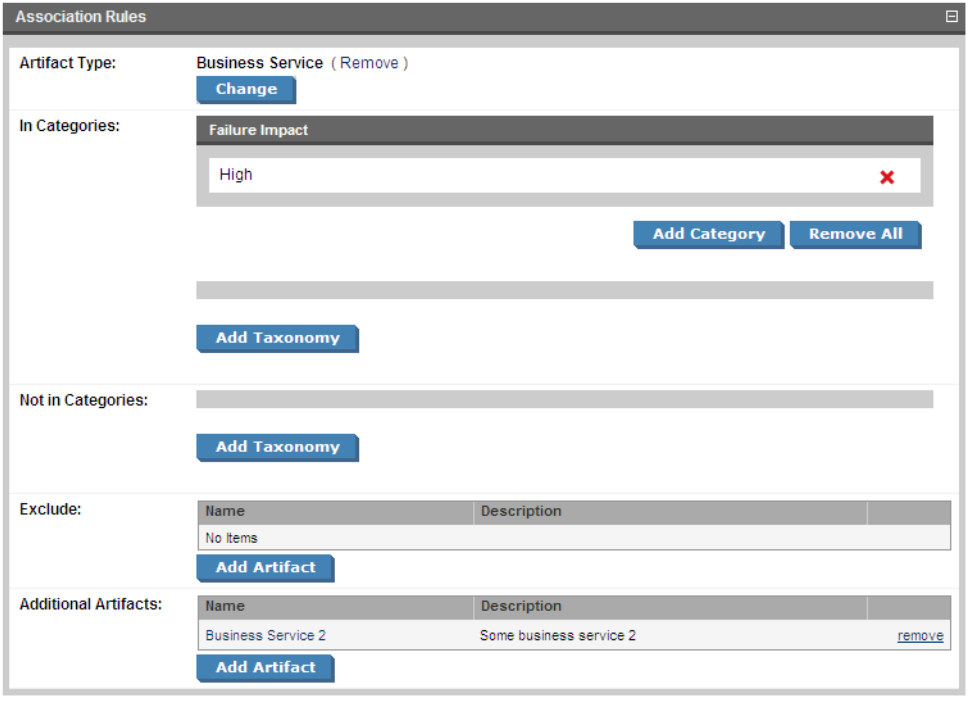
A list of document types appears.



2 Use **Quick Find** or the scroll bar to find the artifact type and then click the artifact type to select it.

By default, the business policy applies to all artifacts of this type.

3 After selecting an artifact type there are a number of options available in the Association Rules section:



These options enable you to further filter the selection of artifacts that the policy applies to as follows:

Option	Use
Artifact Type	Click **Change** to reopen the list of artifact types. Select a new one if required.

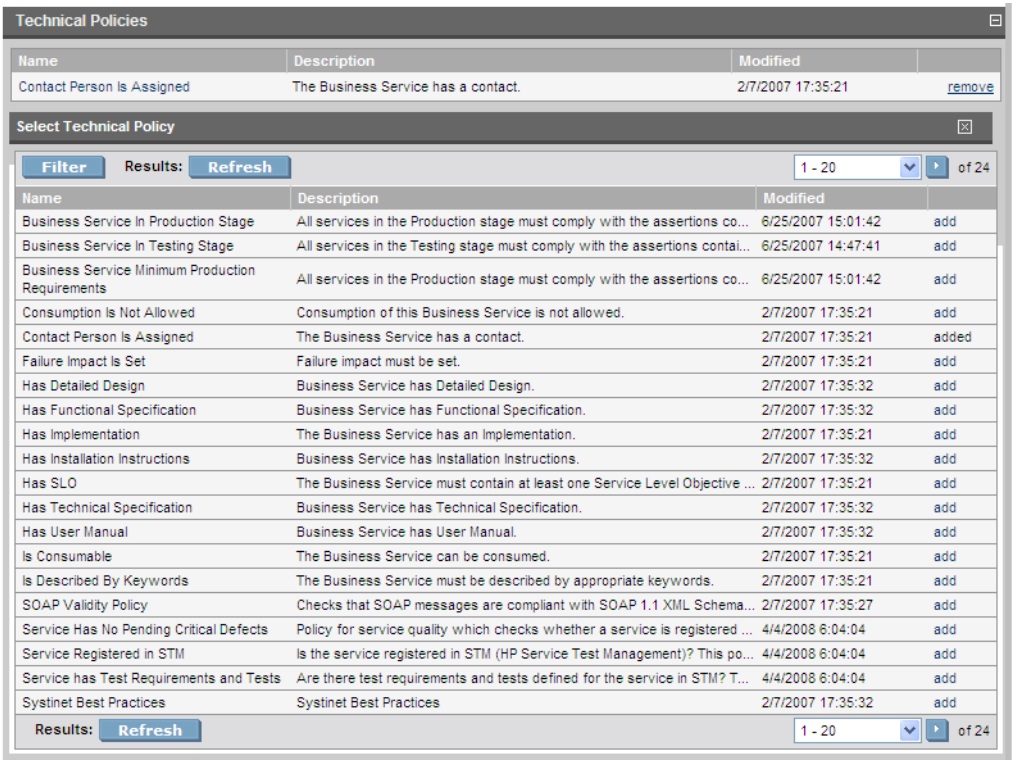
Option	Use
In Categories	Click **Add Taxonomy** to open a list of taxonomies that apply to the selected artifact type. Select a taxonomy to open a list of category values. Click **add** next to a category to apply the business policy to artifacts with that category. After you add category from a particular taxonomy use **Add Category** to add further categories from that taxonomy. The business policy only applies to artifacts with the selected category values.
Not In Category	The functionality is identical to **In Categories**. The business policy does not apply to artifacts with the selected values.
Exclude	Click **Add Artifact** to open a list of all artifacts for the selected artifact types. Use **Filter** to locate the artifact and click **add** next to the artifacts you want to exclude. The business policy does not apply to these artifacts.
Additional Artifacts	The functionality is identical to **Exclude**. Use this feature to add artifacts that would otherwise be excluded by another rule. For example to include a specific business policy regardless of it's Failure Impact category as well as business policies in a Failure Impact category specified in **In Categories**.

4 Click **Save**.

Adding Technical Policies to a Business Policy

1 In the New Business Policy or Edit Business Policy view, in the Technical Policies section, click **Add Technical Policy**.

A list of technical policies appears.



2 Use **Filter** to locate the technical policy and click **add** for the technical polices you want to associate with the business policy.

3 Click **Save**.

Editing Business Policies

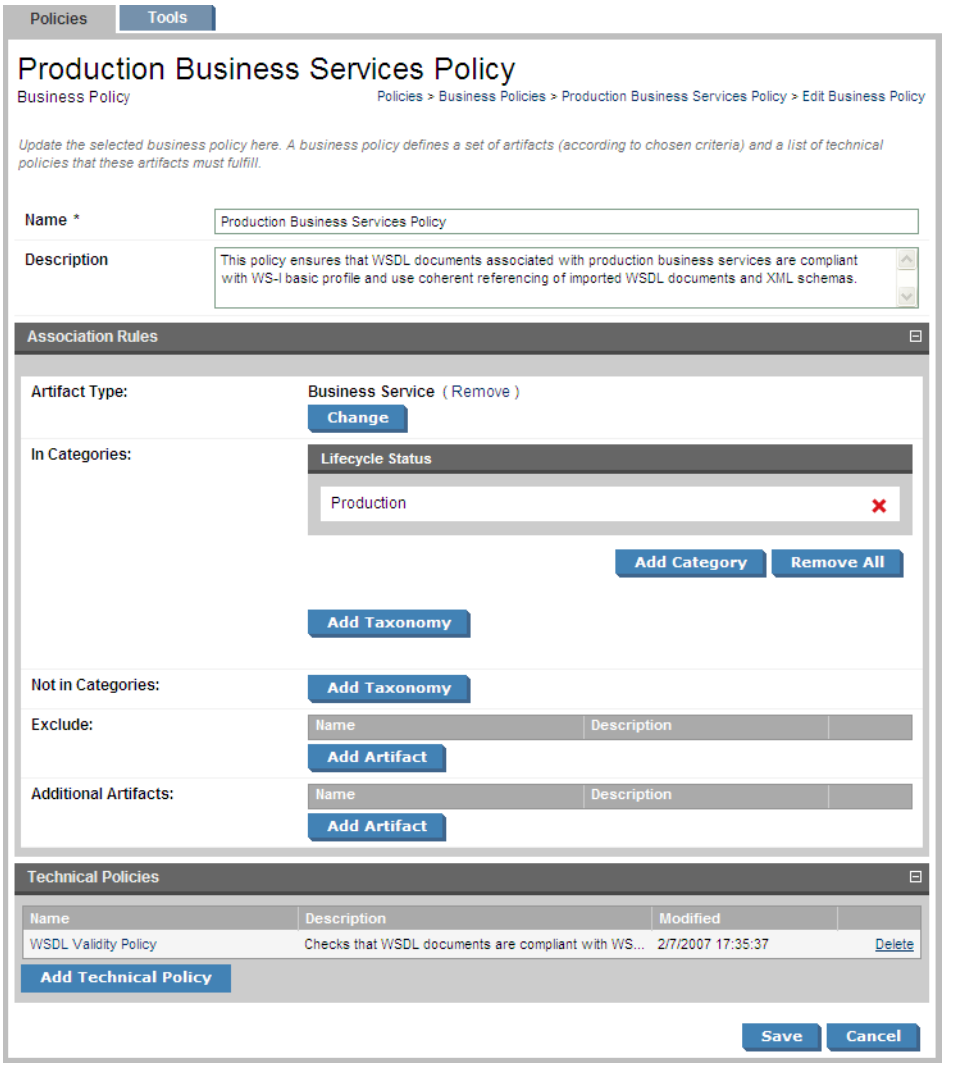
Business policies can be edited from their detail views, described in Business Policy View on page 149.

To edit an existing business policy:

1 In the business policies list view (see Business Policy View on page 149), 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 169, 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 149.

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 148 and Business Policy View on page 149).

- 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.

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

15 Managing Technical Policies

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

Creating Technical Policies

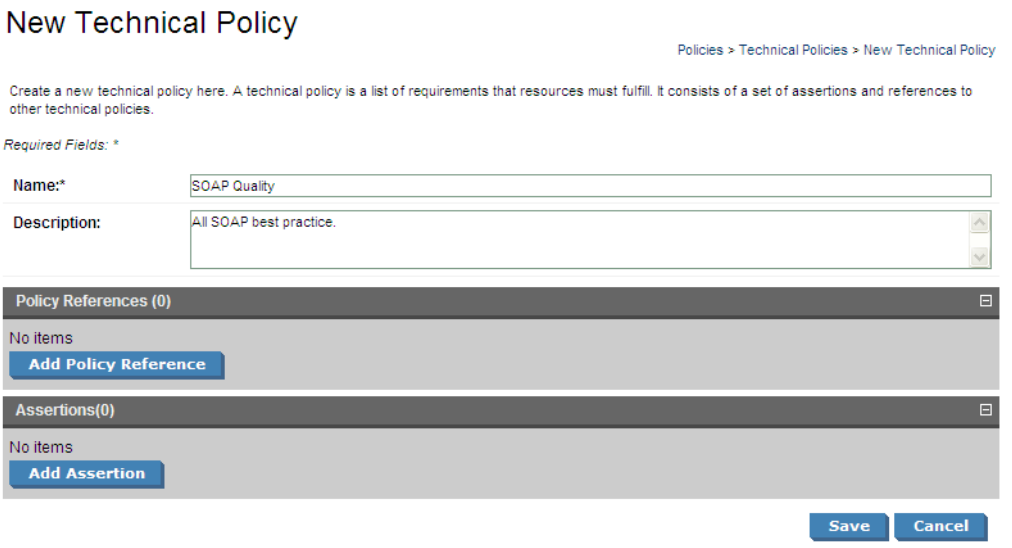
You can create technical policies from the menu on the left side of the Policies tab and from the technical policy list view.

To create a technical policy:

1 Do one of the following:

- In the Policies New menu, click **Technical Policy**.
- In the list view of technical policies, click **New**.

The New Technical Policy page opens:



2 Input a name and description for the new technical policy.

3 Do any of the following:

- Click **Save** to create a draft policy. You can add policy references and assertions later by editing the policy.

  For details, see Editing Technical Policies on page 181.

- Add Policy References.

  For details, see Adding Policy References to a Technical Policy.

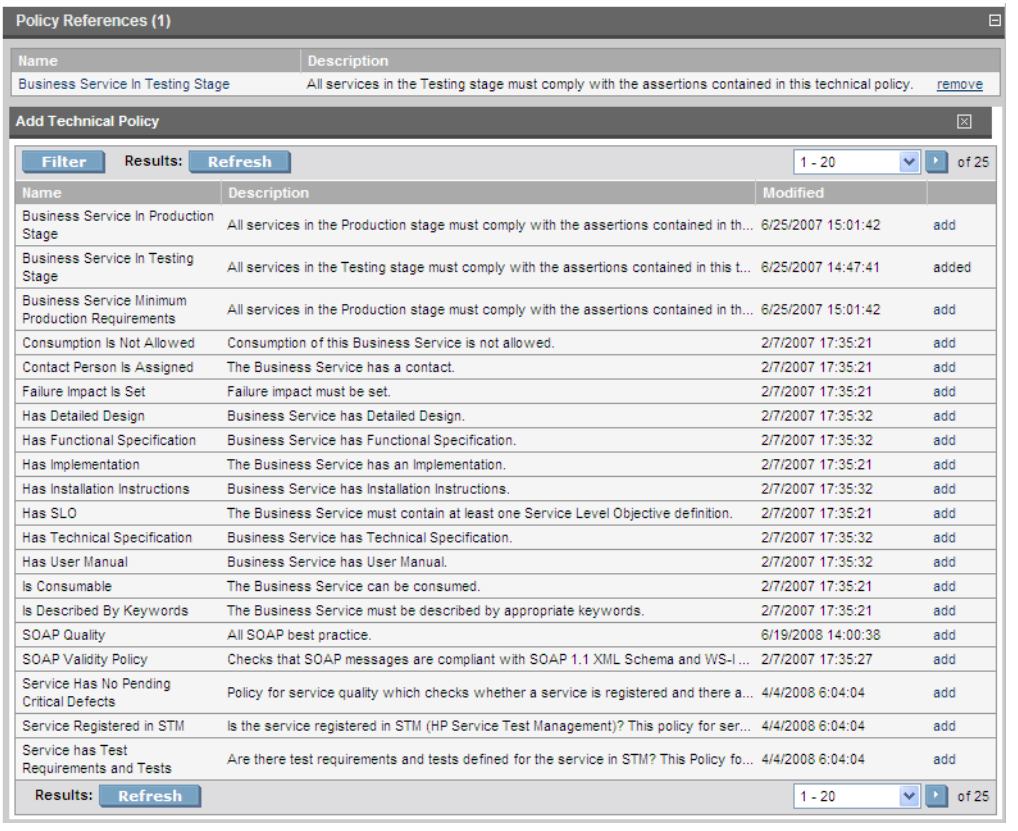
- Add Assertions.

  For details, see Adding Assertions to a Technical Policy.

Adding Policy References to a Technical Policy

1 In the New Technical Policy or Edit Technical Policy view, in the Policy References section, click **Add Policy Reference**.

A list of technical policies opens.



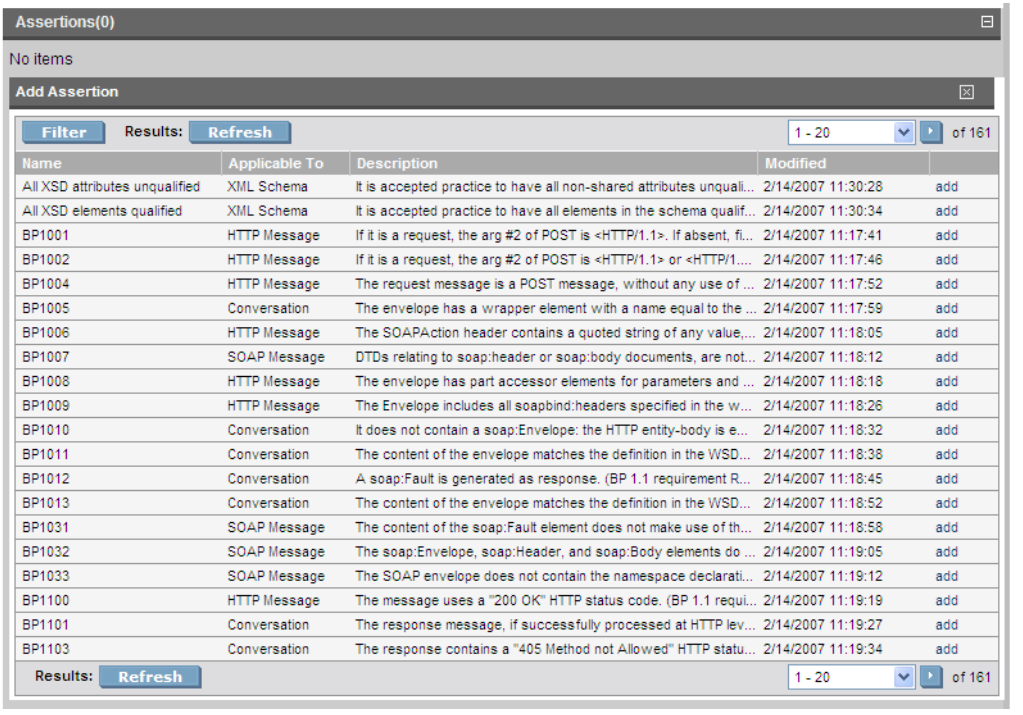
2 Use **Filter** to locate the technical policy and click **add** for the technical polices you want to add references to.

3 Click **Save**.

Adding Assertions to a Technical Policy

1 In the New Technical Policy or Edit Technical Policy view, in the Assertions section, click **Add Assertion**.

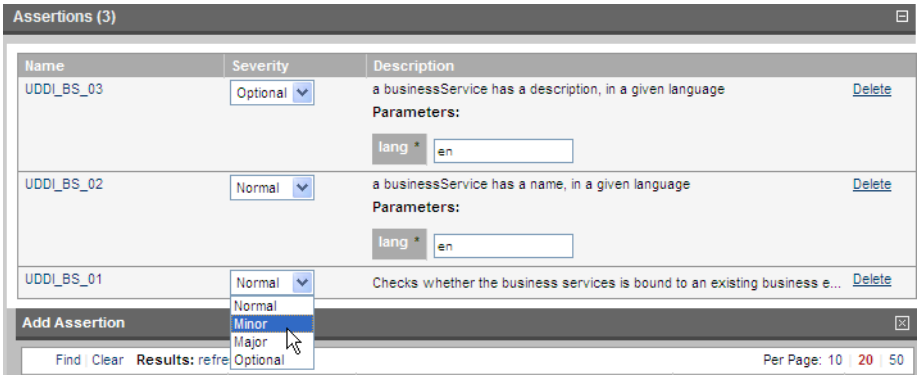
A list of assertions opens.



2 Use **Filter** to locate the technical policy and click **add** for the assertions you want to add.

3 After adding assertions, select a **Severity**value for each assertion.

4 If an assertion includes parameters, you can change or set their values.



Parameters inherit any default values set in the assertion template and any non-optional parameters must be set.

For more details, see "Assertion Schema" in the *HP SOA Systinet Reference Guide* .

5 Click **Save**.

Editing Technical Policies

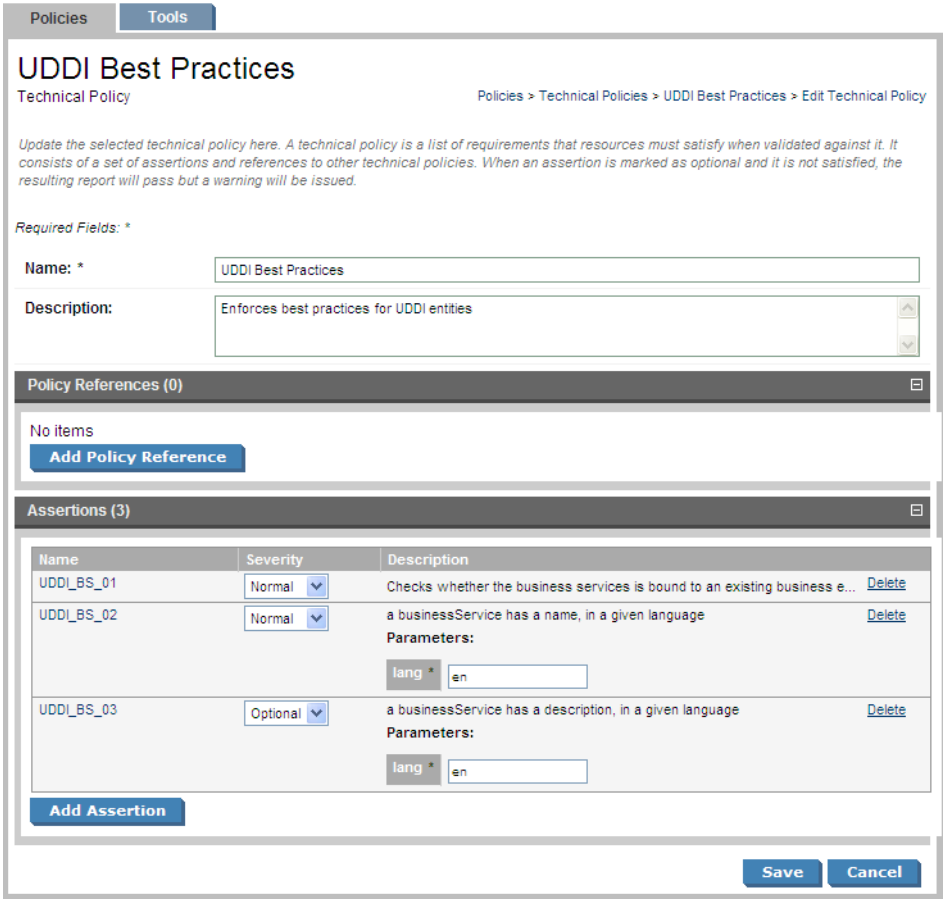
Edit a technical policy to add or delete assertions and policy references or set the value of assertion parameters.

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 148).

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 153). The **Edit** page for that technical policy opens.



4 Add or delete policy references and assertions (see Creating Technical Policies on page 177).

5 To view an assertion's detail view, click its name (see Assertion View on page 155).

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 177.

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 148 and Technical Policy View on page 153).

- 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.

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

16 Validating Resources

Validation is the process of checking one or more resources 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 resource validation, which along with other validation features are described in the following sections:

- Document Validation on page 186

  Validate a resource against all business policies associated with it.

- Business Policy Validation on page 186

  Validate all resources associated with a business policy.

- Resource Compliance on page 187

  Validate a single resource against one or more technical policies, for test purposes.

- Reviewing Documents Manually on page 190

  Some assertions require a manual review of the document to determine its compliance.

- Compliance Trends on page 194

  Monitor the compliance of documents over time.

- Deleting Compliance Reports on page 198

  Deleting reports.

- Validation Client on page 199

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 Tools View on page 223).
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 160.

You can schedule document validation to run automatically as an 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 268 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 159. To run a business policy validation, click **Validate Compliance** in the policy's detail page, as described in Business Policy View on page 149. No further user input is needed.

You may also schedule regular business policy validations as an 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 268 for details. Scheduled validations always have a lower priority than ones you run at the moment.

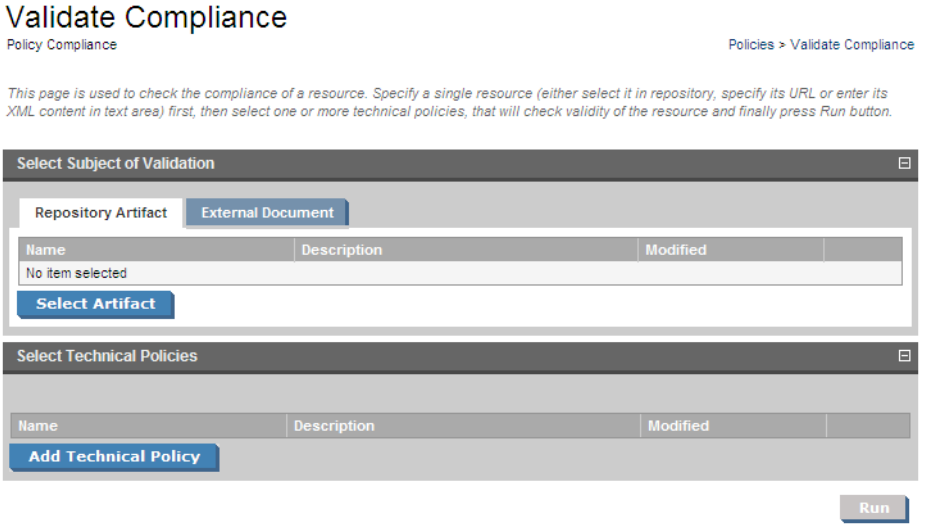
You can run a business policy validation from a remote client with the client `server-validate` tool. See Validating Against Policy On Server (server-validate) on page 203 for details.

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.

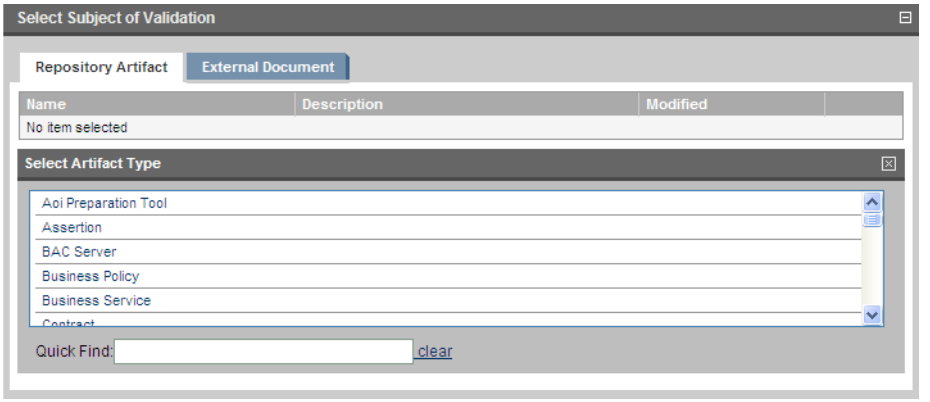
To check the compliance of a single resource:

1 From the **Policies** or **Dashboard** tab menu, or from a technical policy's detail view (see Technical Policy View on page 153), click **Validate Compliance**. The **Validate Compliance** page opens.

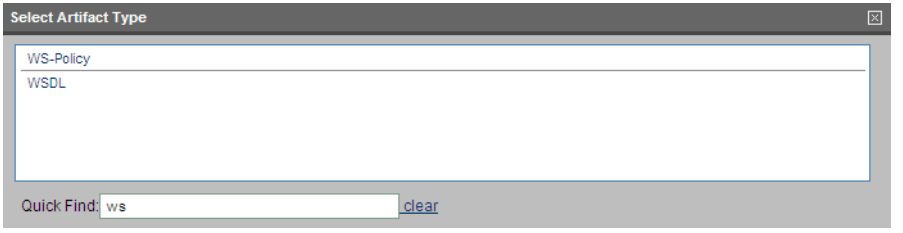


2 Select the subject of validation. This can be either a repository document or an external document. To select a repository document:

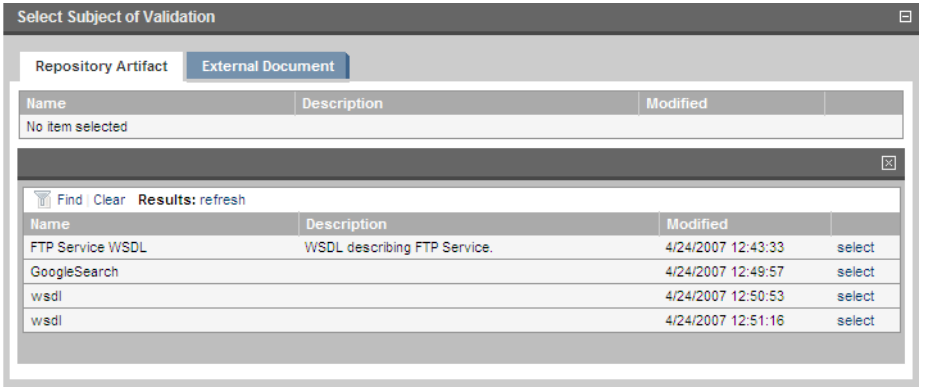
a Click **Select Artifact** in the **Repository Artifact** tab. A list of document types appears.



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



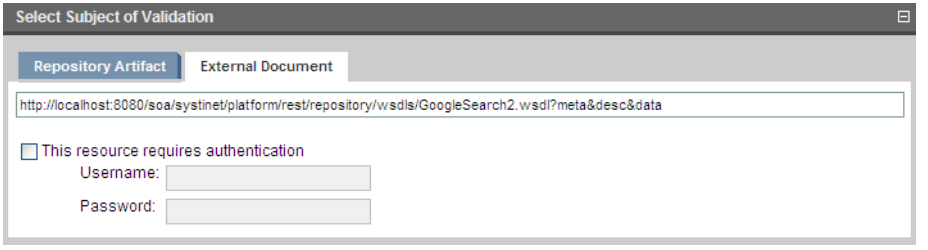
c Select an artifact type by clicking on it. A list appears of artifacts of this type. You can narrow down this list by clicking **Find**, which opens a filter dialog box, and typing a partial name.



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

To select an external document:

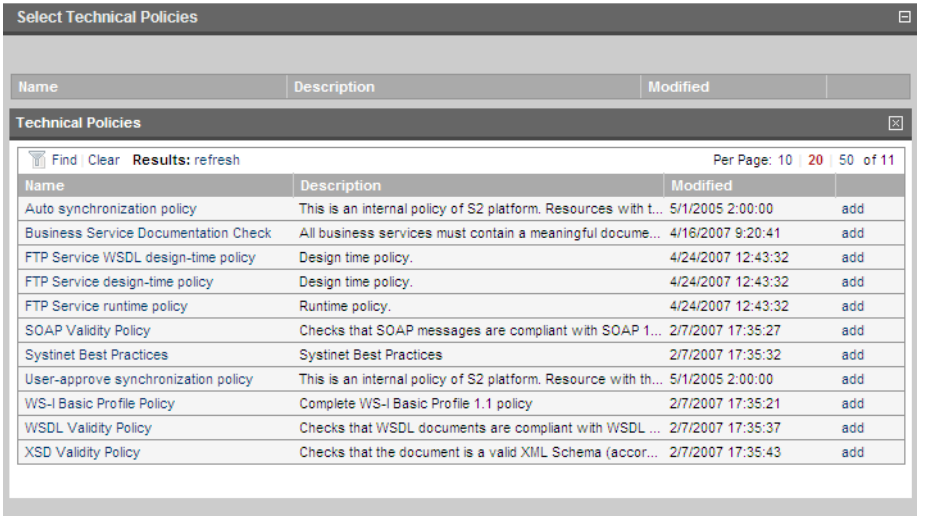
a Click the **External Document** tab to open it.



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.

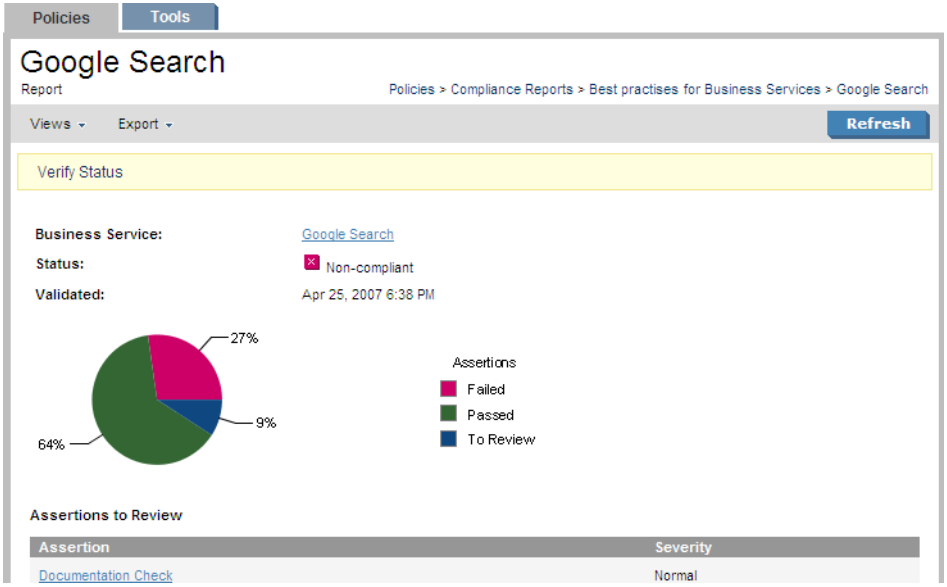
5 Click **Run**. Validation generates a document report as described in Document Reports on page 162.

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:

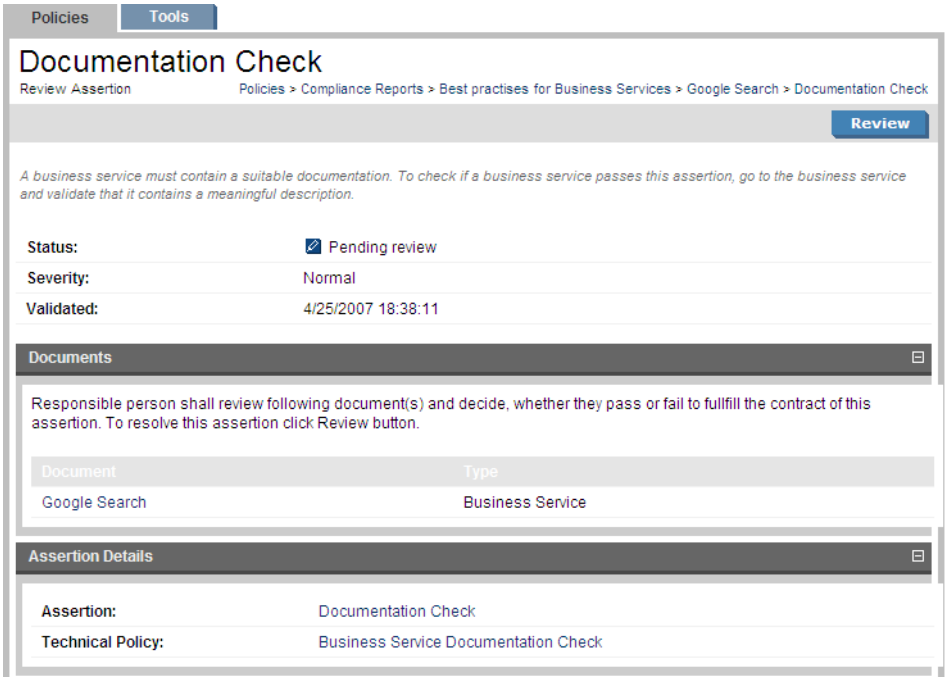
- The **Latest Pending Reviews** and **Pending Reviews Older than Week** areas of interest list the assertions requiring manual document review. See Areas of Interest on page 145.
- The document reports (see Document Reports on page 162) or business policy reports (see Business Policy Reports on page 168) that include the assertion list it under **Assertions to Review**. Figure 53 is from a document report with an assertion pending review.

Figure 53. Google Search Document Report Awaiting Review



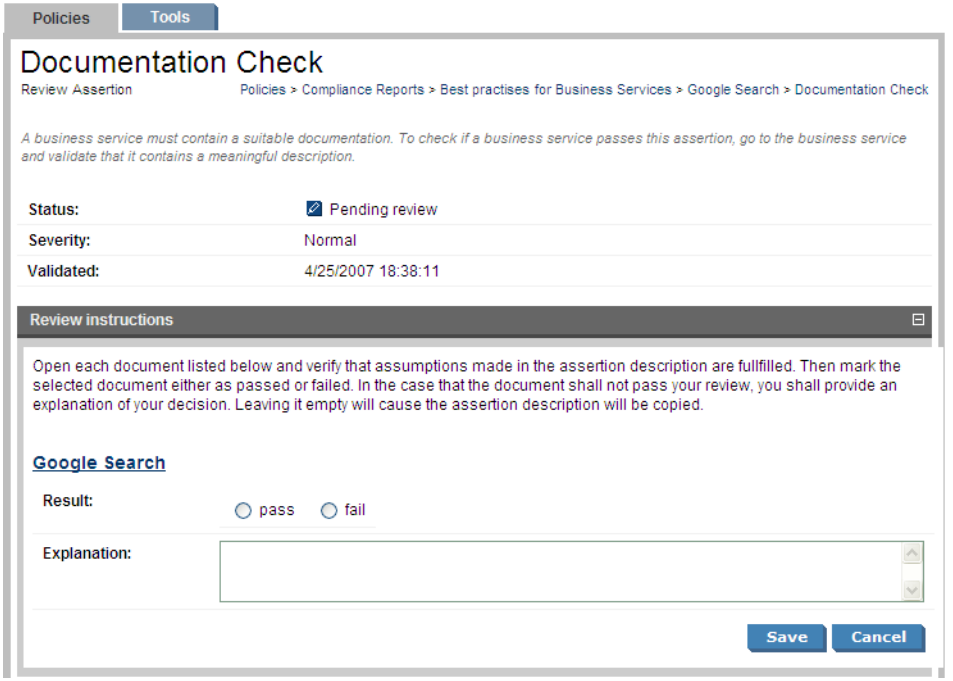
To manually review a document:

1 In either the report (see Figure 53) 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 Tools View on page 223 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 Tools View on page 223 and Service View on page 56), click its name under **Review Instructions**

Depending on the conditions of the assertion, you may want to see an 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.

Compliance Trends

SOA Systinet automatically schedules nightly validation of all governed artifacts in the repository.

Artifacts are validated against all technical policies from the governance processes and against all applicable business policies. For each validated document, a new record is created in the database, giving the separate validation result of business and lifecycle policies, together with their combined validation result.

In addition to the automated validation, you can create your own compliance trend, by defining the following:

- **Artifacts**

  For example, business policies only, lifecycle polices only, or combined,

- **Time Period**

  For example, how many days, weeks, or months should be covered and the end date - either the current date or a specified date in the past.

SOA Systinet uses two algorithms to define compliance trend reports:

- **Period Selection Algorithm**

  Enables you to define a period of time for a compliance check.

  The predefined period is 60 days. If you select a period of time longer than 60 days, SOA Systinet divides the defined period of time into equal sub-periods, using the first available date for each period.

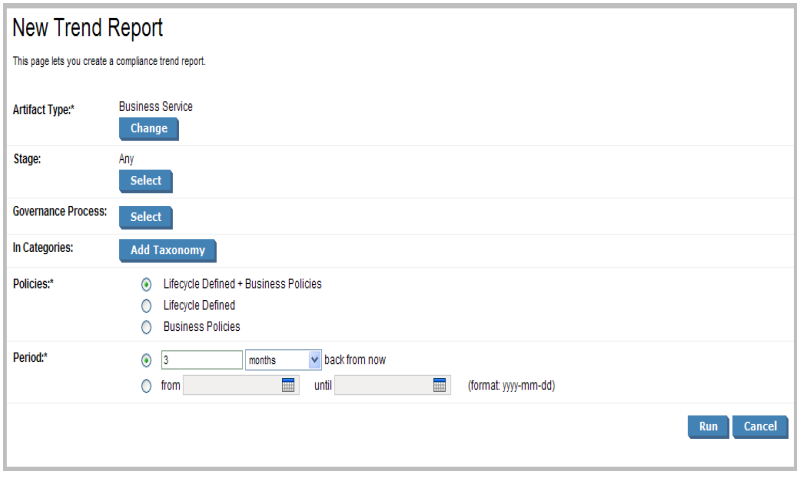
- **Artifact Selection Algorithm**

  Enables you to specify certain criteria for the compliance trend report. For example, artifact type, stage, process, taxonomical properties, and so on.

To create a compliance trend report:

1 In the New menu of the Polices tab, click **Trend Report** to open the New Trend Report Page, as shown in Figure 54.

Figure 54. New Trend Report



2 In the Artifact Type field, the default artifact is Business Service. To change the artifact type, click **Change** to open the Change Artifact Type view.

3 Browse or search for the artifact type you need, and confirm the change.

4 In the Stage field, click **Select** to open the Select Lifecycle Stages view.

5 Select the check-boxes of the lifecycle stages you need, and click **OK**.

6 In the Governance Process field, click **Select** to open the Select Governance Process view, and then do one of the following:

- Click **Select** next to the process you need.

- If no items are listed, click **Filter** to open the Filter window, enter the required parameters, and then click **Search**.

  Matching entries are displayed, with a Name, Description, and Modified date.

- Click **Select** next to the process you need.

7 In the **In Categories** field, click **Add Taxonomy** to open the **Select Taxonomy** view, and then do one of the following:

- Click **add** next to the taxonomies you need from the list.
- Use **Quick Find** to search for the taxonomies you need, and click **add**.

To delete a single category, click the remove character (x), next to the category you want to remove.

8 In the **Policies** field, select which policies you want to validate against.

9 In the **Period** field, define the reporting period in one of the following ways:

- Specify days, weeks, months, or years **back from now**.
- Select the **from** and **until** date from the calendar.

10 Click **Run**.

The result is displayed in the **Trend Report** view.

For every validated document a new record is created in the repository, with the validation results of business policies, lifecycle policies, and their combined result.

The compliance trend report can only use preexisting data obtained from scheduled validation tasks.

11 To save the report, click **Save** to open the Trend Report view.

12 Enter the required parameters and click **Save**.

13 To edit the report, click **Edit** to open the Trend Report view, and repeat the procedure from Step 2.

You can export the Trend Report to the following formats:

- PDF
- CSV

To export the trend report, expand **Export**→ ***required format*** .

An overview of compliance trend reporting is described in the following example:

Example 1: Compliance Trend Report

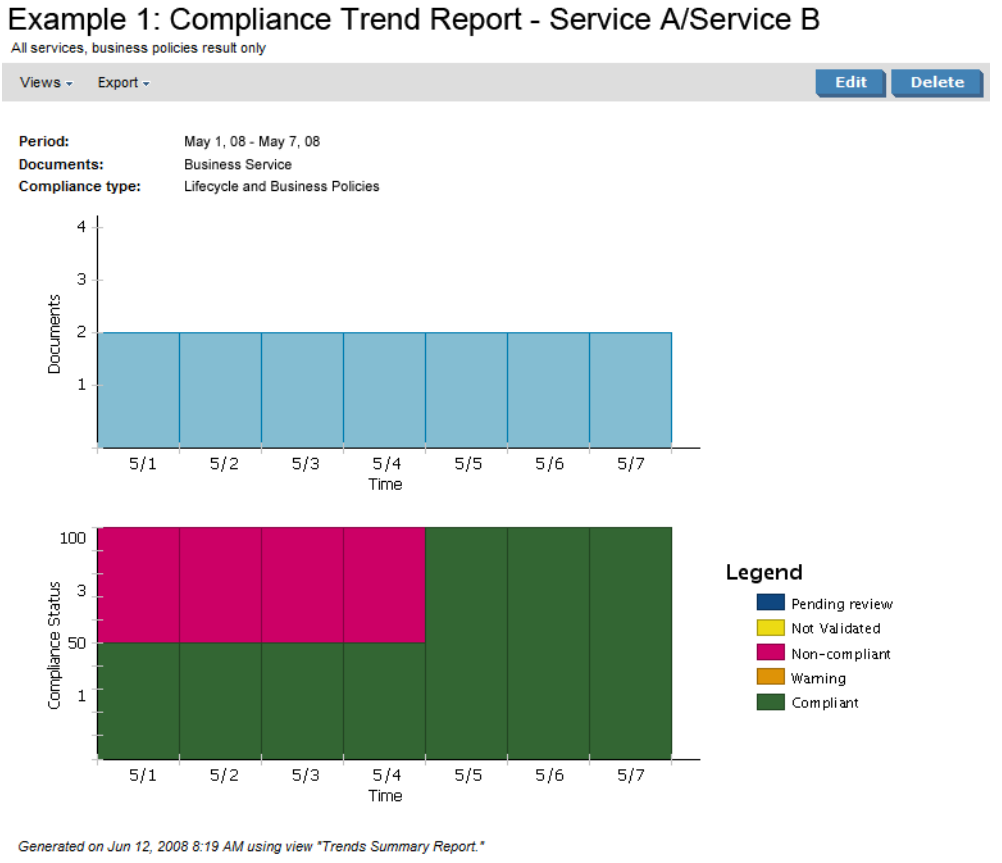
You want to check the compliance of Service A and Service B. Service A was in the initial stage on Monday and Tuesday, prototype stage on Wednesday, testing on Thursday, and production on Friday. The service was not compliant in the initial and prototype stages, but was compliant in the testing and production stages. Service B was in production stage and compliant all week.

You can create several trend reports within this one week period. When you run a trend report for services in their initial stage, you will see that for Monday and Tuesday, it was 100% non-compliant. The remainder of the week has no matching services.

You then filter the trend report to the production stage. The report shows a single service from Monday through Thursday, and two services on the Friday. The report shows 100% compliance.

Finally, you can remove the stage criteria. The report displays both services as 50% compliant from Monday through Thursday, and 100% compliant on Friday, as shown in Figure 55.

Figure 55. Compliance Trend Report: Output



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 and Assertion detail page has a **Reset Compliance Statistics** link in the **Tools** drop down 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.

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 remote documents against policies located on a server. These validations run on the server.

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

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

- Downloading Policies and Assertions (sync) on page 199
- Local Validations (validate) on page 200
- Validating Against Policy On Server (server-validate) on page 203
- Rendering Output from XML Reports (render) on page 204

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 -u** ***SOA Systinet username*** **-p** ***SOA Systinet password***. If SOA Systinet does not require any credentials, enter **sync -noauth**. The `sync` tool gets the hostname and port of the SOA Systinet host from the `SOA_HOME/client/conf/setup/policy-manager.properties` file, created automatically when SOA Systinet is installed.

The property used is determined by the `shared.https.use` property and is either:

- shared.http.urlbase=http\://host\:port/context
- shared.https.urlbase=https\://host\:8443/context

Local Validations (validate)

Validate documents against local copies of technical policies by running the `validate` tool. The syntax is `validate` [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 --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://host:port/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 "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 -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 --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 -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 -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 204.

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 2. Example 2 on page 203 is an example of an ANT task script for launching validate.

Table 2. 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 2: `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` [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` [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 --help**.

Policy URIs

Policy URIs are in the following formats:

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

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 format:

- 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` {--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:

- Chapter 17, Tools UI

  Describes the user interface elements of the **Tools** tab.

- Chapter 18, Managing Content

  Explains the procedures for managing the content of SOA Systinet.

- Chapter 19, Governance Tools

  Describes the use of SOA Systinet governance tools, tasks and reports.

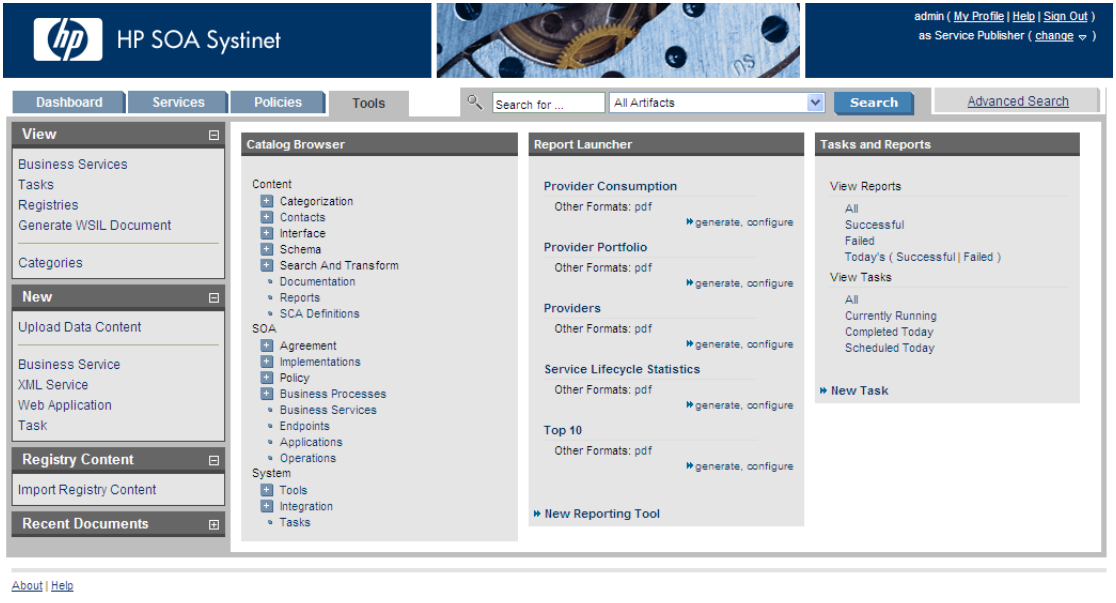
- Chapter 20, Advanced Searches

  Describes the advanced search facilities of SOA Systinet.

17 Tools UI

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 56. 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 210

A description of the items in the **Tools Menu**.

- Catalog Browser on page 213

  The index portlet of artifact types in the repository.

- Tasks and Reports Portlet on page 215

  A portlet to access tasks and the reports on the results of those tasks.

- Report Launcher Portlet on page 216

  An access portlet for customized reporting tools.

The portlets in the **Tools** tab can be moved in the same way as described in Chapter 5, Dashboard UI.

Tools Menu

The Services menu is split into collapsible segments.

Each segment is described in the following sections:

- Tools View Menu on page 211

  A set of links to artifact browse pages showing an index of the artifacts in the repository.

- Tools New Menu on page 212

  A set of links to create new artifacts:

- Registry Content Menu on page 212

  Import content from a UDDI registry.

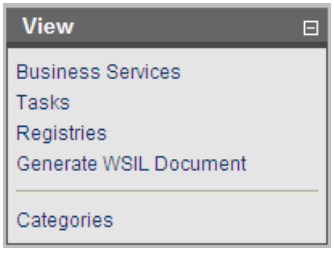
- **Recent Documents**

  Quick links to the last few artifacts viewed.

Tools View Menu

The View menu in the Tools tab provides links to artifact browse pages.

Figure 57. Tools View Menu



The View menu contains the following links:

- Artifact Names

  Click to view an index of that artifact type in the repository.

  For details, see Browse Artifact Pages on page 219.

- **Generate WSIL Document**

  Access a Web Service Inspection Language (WSIL) format query view of the current Tools page.

  This format can be passed to other products, for example MS Visual Studio, for the purpose of service discovery.

  The query for the Tools tab itself generates a view of the published WSDLs in the repository.

- **Categories**

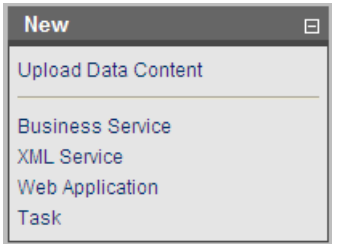
  Browse the repository by taxonomic category.

  For details, see Category Browsing on page 27.

Tools New Menu

The New menu in the Tools provides quick links to create new artifacts.

Figure 58. Tools New Menu



The New menu links to the following artifact creation pages:

- **Upload Data Content**

  Import a service infrastructure from a service definition document.

  For details. see Uploading Service Infrastructure from Definition Documents on page 99.

- Artifact Type Names

  Create a new service artifact of the relevant type.

  For details, see Creating an Artifact on page 236.

- **Task**

  Create a new task to execute a governance tool.

  For details, see Creating a Task on page 268.

Registry Content Menu

The Registry Content menu enables you to import content from a UDDI Registry.

Figure 59. Registry Content Menu

The Registry Content menu contains the following link:

- **Import Registry Content**

  Import a content from a UDDI Registry into the SOA Systinet repository.

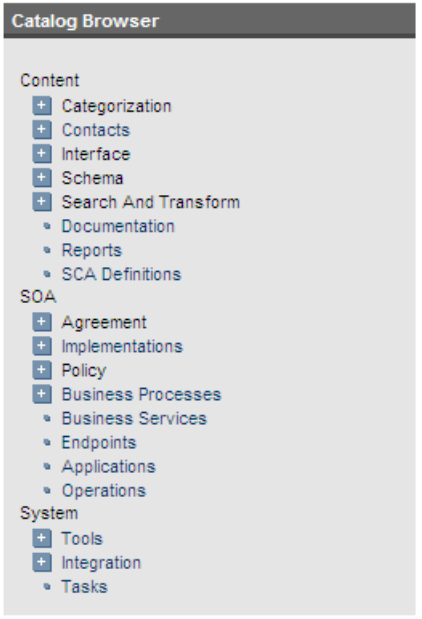
  For details, see Importing Services from Registries on page 103.

Tools Tab Portlets

Catalog Browser

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

Figure 60. 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* :

- **Content**

  Artifact types associated with services such as documentation and metadata.

- **SOA**

  Artifact types for business services, their implementation and policies.

- **System**

  Artifact types related to integration and governance tools and tasks.

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

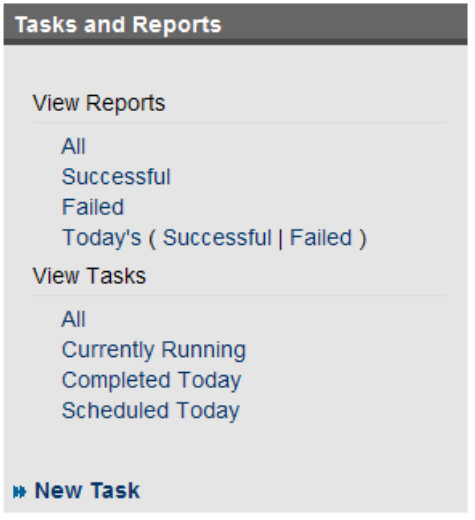
Click an artifact type to open its browse page.

For details, see Tools View on page 223.

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 61. 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 271.
  - **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 268.

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 Software and user created tools with valid report definitions on the reporting server.

Figure 62. Report Launcher Portlet

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

Click **pdf** 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:

- **Provider Consumption**

  Generates an overview of artifact consumption in the repository organized by the owner of the provided artifact..

- **Provider Portfolio**

Generates an overview of the artifacts in the repository that are potentially consumable.

- **Providers**

  Generates an overview of the artifacts in the repository that are available for consumption.

- **Service Lifecycle Statistics**

  Generates a summary of governed artifacts for each stage in the service lifecycle.

- **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.

For details, see Creating a Reporting Tool on page 261.

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 219

  Are the index views of artifacts.

- Tools View on page 223

  Are the detailed view of artifacts in the repository.

- Navigator View on page 231

  Displays a graphical representation of an artifact and its relationships.

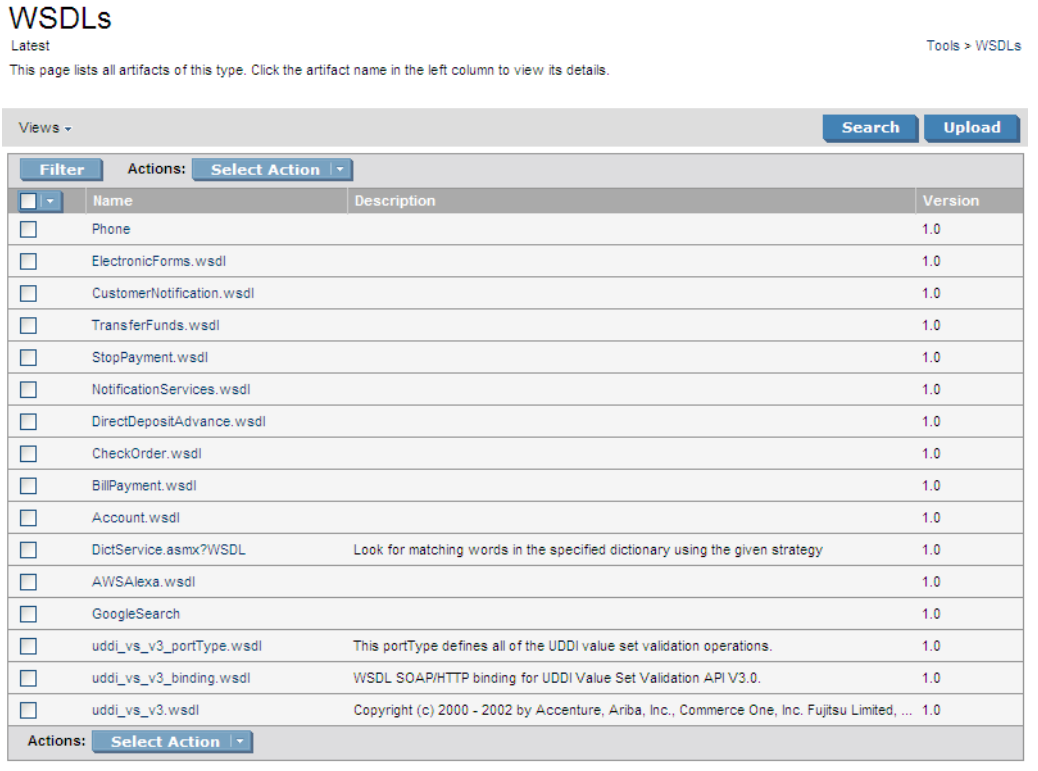
- Revision and Version History on page 233

  Displays previous revisions of artifacts.

Browse Artifact Pages

From the Catalog Browser of the Tools tab, click an artifact type to open the browse artifact page:

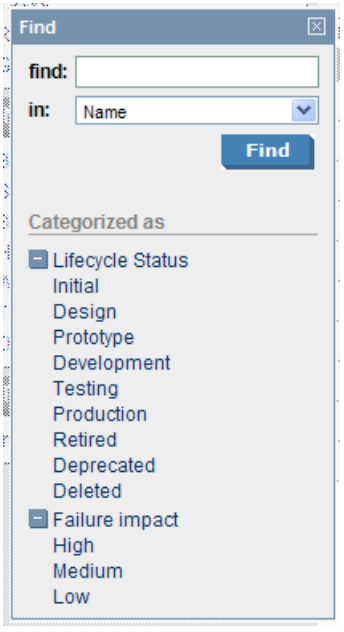
Figure 63. Browse WSDLs Page



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

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

Figure 64. Implementations Filter



To filter the list, click one of the listed taxonomic categories, or enter your search parameter, select a column, and then click **Find**.

Click **Clear Filter** to remove the filter and restore the list of artifacts, or open the Filter menu and select **Edit Filter** to change the filter terms.

The Views menu offers a set of alternative views of the artifact type:

- **Approved**

  Select **Approved** to only show the latest revisions of the artifacts approved in lifecycle management.

  For details, see Chapter 11, Lifecycle Governance.

- **Latest**

Select **Latest** to show the latest revisions of the artifact type collection.

- **Deleted**

  Select **Deleted** to show deleted revisions of the artifact type collection.

- **XML View**

  Opens an 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**

  Open a view of the access permissions for the artifact type collection.

Click an artifact to open its detail view. For details, see Tools View on page 223.

The available functions vary depending on the artifact type and they include:

- **New**

  Open the Create New Artifact page allowing the creation of a new artifact.

  For details, see Creating an Artifact on page 236.

- **Upload**

  Create artifacts based on the content of an external resource and import the document the repository.

  For details, see Uploading Service Infrastructure from Definition Documents on page 99.

- **New Link**

  Create an artifact representing an external resource with only a link to the external resource. The resource is not imported to the repository.

  For details, see Adding Documentation on page 241.

- **Search**

  Create an advanced search for the artifact type.

  For details, see Chapter 20, Advanced Searches.

Browse views also enable you to carry out bulk operations on selected artifacts using the **Actions** menu.

The available bulk operations vary depending on the artifact type.

To perform a bulk operation:

- Select the service artifacts you require, and open the **Select Actions** menu.

  The menu offers the following bulk operations:

  - **Edit Access Rights**

    The owner of an artifact or administrator can edit the permissions of selected artifacts.

    For details, see "Access Rights" in the *HP SOA Systinet Administration Guide*.

  - **Edit Category Bag**

    Change the categorization for the selected artifacts.

    For details, see Categorizing Artifacts on page 240.

  - **Change Owner**

    Change the person or group responsible for the artifact.

    For details, see To change the owner of an artifact:.

  - **Synchronize**

    Perform change management on the selected artifacts.

For details, see Running the Synchronization Tool on page 263.

- **Change Version**

  Create new versions of the selected artifacts.

  For details, see Managing Versions on page 245.

- **Delete**

  Mark the selected artifacts as deleted.

  For details, see Deleting an Artifact on page 237.

- **UDDI Export**

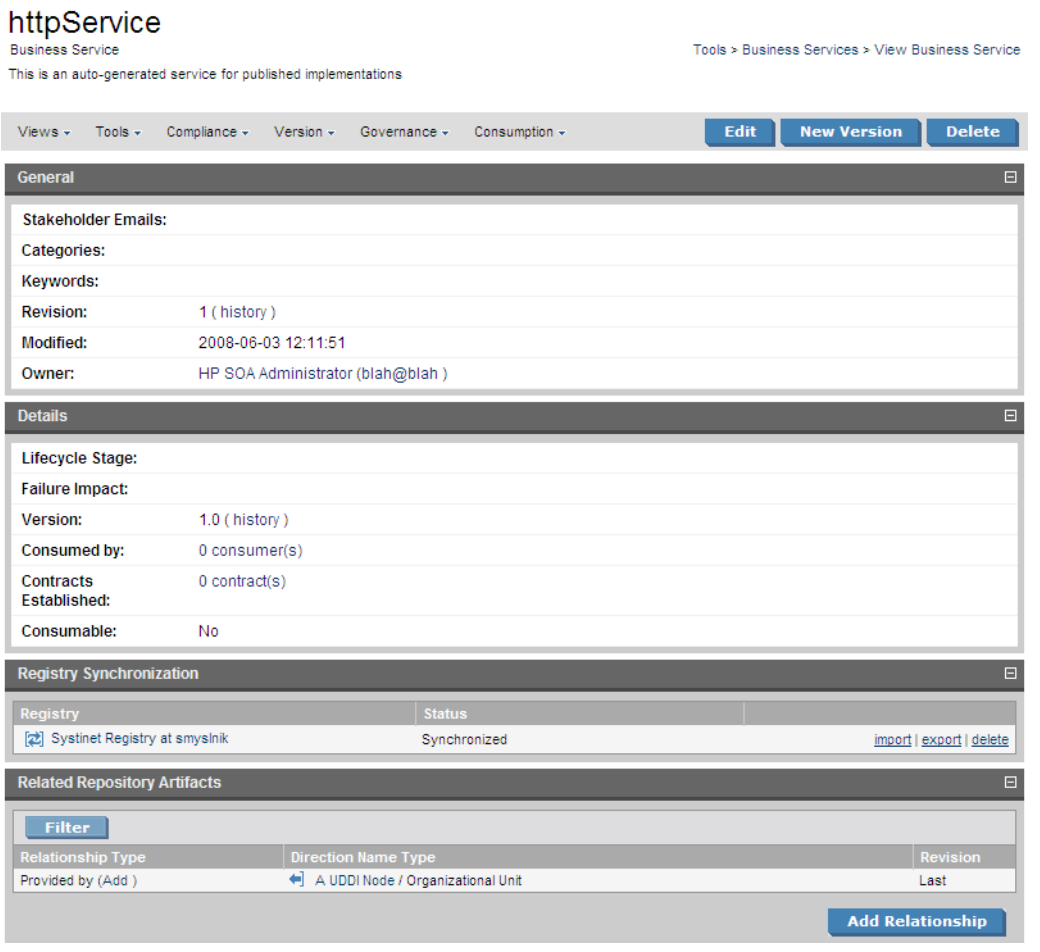
  Export the selected artifacts to an integrated UDDI Registry.

  For details, see Exporting Data To Registry on page 250.

Tools View

Clicking an artifact name in the Tools tab opens a detailed artifact view for that artifact:

Figure 65. HTTP Business Service Details



This detail view contains all the information about that artifact with options to edit, delete and add relationships.

This following sections describe the content and functionality of these pages:

Tools View Context Actions

The grey bar contains a set of context action menus and functions.

The actions vary depending on the artifact but they include:

- **Views**:
  - **Consumer View**

    Switches to the Services view of the last approved revision of the artifact for artifacts subject to lifecycle management.

    For more details, see Chapter 11, Lifecycle Governance.
  - **Services View**

    Switches to the service view of the artifact in the Services tab.

    For details, see Service View on page 56.
  - **Navigator View**

    Opens a graphical representation of the artifact and its relationships.

    For details, see Navigator View on page 231.
  - **Revisions**

    View the revision history of the artifact.

    For details, see Revision and Version History on page 233.
  - **Access Rights**

    Opens a view of the access permissions for the artifact.

For details, see "Edit Access Rights" in the *HP SOA Systinet Administration Guide* .

- **XML View**

  Opens an 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**

    A list of the reports related to this artifact.

    For details, see Reports on page 271.

  - **Dependency Analysis** and **Impact Analysis**

    Execute the impact management tool on the artifact.

    For details, see Impact Tools on page 256.

  - **Add Documentation**

    Add an associated document.

    For details, see Attaching Documentation to Artifacts on page 242.

  - **Change Owner**

    The administrator or owner of the artifact to can transfer ownership to a different user.

    For details, see Changing Artifact Ownership on page 239.

  - **Download Content**

    Create an archive containing all the service infrastructure referenced by a single definition document, for example a WSDL. Any artifacts

This functionality is effectively the reverse operation compared to **Upload Content**. For details of the relevant definition document types, see Uploading Service Infrastructure from Definition Documents on page 99.

- **Compliance**:
  - **Validate Compliance**

    Validate the policy compliance of an artifact.

    For details, see Chapter 16, Validating Resources.
  - **Compliance Status**

    View the compliance status of the artifact.

    For details, see Report Views on page 158.
  - **Effective Policies**

    View the business policies associated with the service artifact.
  - **Reset Compliance Statistics**

    Delete all compliance reports associated with the artifact.

- **Version**:
  - **Versions**

    View the version history for the artifact.

    For details, see Revision and Version History on page 233.
  - Version Navigation

    Open specific next, previous, or last versions of the artifact.

- **Governance**
  - **Start Governance**

    Enter the artifact into a lifecycle process.

    For details, see Starting Artifact Governance on page 125.
  - **Start Promotion**

    Request artifact promotion to the next lifecycle stage.

    For details, see Submitting a Promotion Request on page 127.
  - **View Stage Details**

    View the page showing the details for the current lifecycle stage.
  - **Promotion History**

    View the promotion request and voting details for each previous lifecycle stage.

- **Consumption**:
  - **Pending Requests**

    View the list of outstanding consumption requests for the artifact.
  - **Accepted Requests**

    View the list of accepted consumption requests for the artifact.
  - **Rejected Requests**

    View the list of rejected requests for the artifact.

- **Edit**

  Change the attributes of the artifact.

- **New Version**

  Create a new version of the artifact.

  For details, see Managing Versions on page 245.

- **Delete**

  Mark the artifact as deleted with a further option to purge it from the repository.

Tools View Page Content

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.

- **Governance**

  Service artifacts subject to lifecycle management display the last approved stage and the current stage with options to view the stage details, view changes since the last approved version, and to start promotion to the next lifecycle stage.

  For details, see Chapter 11, Lifecycle Governance.

- **Details**

  Lifecycle, failure impact, version, and contract information for artifacts.

- **Data**

  Artifacts associated with external documents display the location of the associated resource. Click the resource name to view it, click **View Location** to view that repository location, or click **Update** to change the associated resource.

  For artifacts subject to change management the synchronization status is also shown with options to update the cached version.

For details, see Running the Synchronization Tool on page 263.

- **Related Repository Artifacts**

  The relationships that the artifact has with other repository content. **Add Relationship** allows you to associate the artifact with another in the repository.

  For details, see Adding a Relationship on page 237.

- **Service Quality**

  If you integrate SOA Systinet with *HP Service Test Manager* (STM), SOAP Services display a section for service quality statistics from STM.

  This section enables you to register a service with STM and then displays information about requirements, tests, and defects from STM.

  For details, see Service Test Manager Integration Features on page 70.

- **Performance and Availability**

  The content of this section depends on which product you integrate SOA Systinet with.

  - If you integrate SOA Systinet with *HP Business Availability Center* (BAC), this section displays statistics generated by BAC and enables you to open the BAC view of the service artifact.

    For integration details, see "Setting Up BAC/UCMDB Integration" in the *HP SOA Systinet Administration Guide* .

    For feature details, see BAC/UCMDB Integration Features on page 64.

  - If you integrate SOA Systinet with *HP SOA Policy Enforcer* (SPE), this section enables you to open the SPE view of the service artifact if it is shared with SPE.

    For integration details, see "Setting Up SOA Policy Enforcer Integration" in the *HP SOA Systinet Administration Guide* .

    For feature details, see SOA Policy Enforcer Integration Features on page 68.

- **Service Discovery**

  If you import a service artifact from an external source, such as *HP Business Availability Center* (BAC), this section displays the source of the original service and its change management status. There are options to display the discovery details, or import changes.

  For details, see Synchronizing Discovered Services on page 111.

- **Registry Synchronization**

  If you integrate SOA Systinet with UDDI Registries, this section displays each registry and the status of the service artifact compared to that registry. There are synchronization options depending on the relative status of the artifact with each registry.

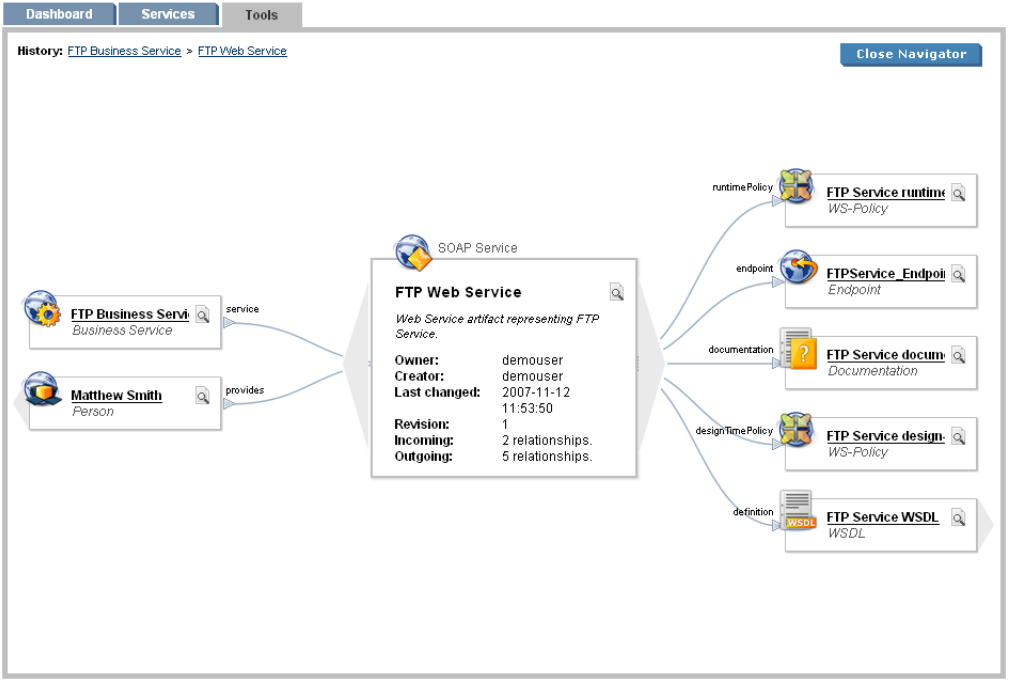
  For details, see Registry Integration on page 248.

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 66. 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 and Version History

During the lifecycle of resources and artifacts stored in the database, their properties or content may change. SOA Systinet supports revisions and versions.

Any update of a resource automatically increments its revision number. A resource may be updated by the Synchronization Tool or by a user changing any property such as the name, description, etc.

The version number is manually controlled.

For details, see Managing Versions on page 245.

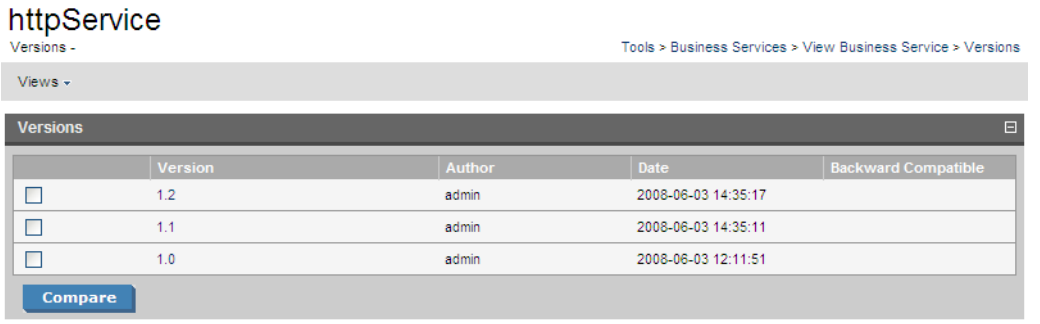
To open the revision history of an artifact:

- Do one of the following:
  - In the Tools view of an artifact, in the General section click **history**, next to the revision number.
  - In the Services view or the Tools view of an artifact, open the View context menu and click **Revision History**.

To open the version history of an artifact:

- Do one of the following:
  - In the Tools view of an artifact, in the Details section click **history**, next to the version number.
  - In the Services view or the Tools view of an artifact, open the Version context menu and click **Versions**.

Figure 67. HTTP Business Service Version History



In the version history, open the Views menu and select **Approved Versions** to only show the list of versions approved in Lifecycle Management.

To compare versions or revisions, select two from the list and click **Compare**.

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

In the view of an older revision or version, click **Latest Revision** to view the latest revision of the artifact or open the Views menu to navigate through revisions.

In the view of an older version, open the Versions menu to navigate through versions.

In the view of an older revision, the Views menu contains the context action **Copy as New Revision**. This enables you to create a new revision of the resource with the content of the old revision you are viewing.

18 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 235.

- **Documentation**

  Many artifacts require additional documents describing their purpose or use. Managing Documentation on page 241 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 244.

- **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.

Managing Artifacts

The main artifact management procedures are:

- Creating an Artifact on page 236
- Editing an Artifact on page 236
- Deleting an Artifact on page 237

- Adding a Relationship on page 237
- Changing Artifact Ownership on page 239
- Categorizing Artifacts on page 240

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.

> By default, the **New** button in browse screens is disabled for artifacts with associated data content. These artifact types have an **Upload** button which uses the publisher functionality.
>
> For details, see Uploading Service Infrastructure from Definition Documents on page 99.
>
> The administrator can enable the creation of these artifact types without uploading the associated data content.
>
> For details, see "Configuration Options" in the *HP SOA Systinet Administrator Guide* .

2 The exact details for each artifact type differ.

Input the artifact details, and then click **Save**.

> To start governance of the artifact, see Starting Artifact Governance on page 125.

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 and Version History on page 233 for details.

Deleting an Artifact

You can delete artifacts individually or in bulk.

To delete artifacts:

1 Do one of the following:

- In Services or Tools browse pages select the artifacts to delete, open the Actions menu and select **Delete**.
- In Services or Tools artifact views, click **Delete**.

The Delete Artifacts page opens.

2 Select **Delete Subartifacts** if you want to delete related secondary artifacts from the same lifecycle process as well.

3 Select **Ignore Incoming References** to delete the artifact even if there are incoming relationships from other artifacts in the repository. For example a SOAP service referenced from a Business Service.

4 Select **Non-Recoverable Deletion** to purge the artifacts from the repository instead of just marking them as deleted.

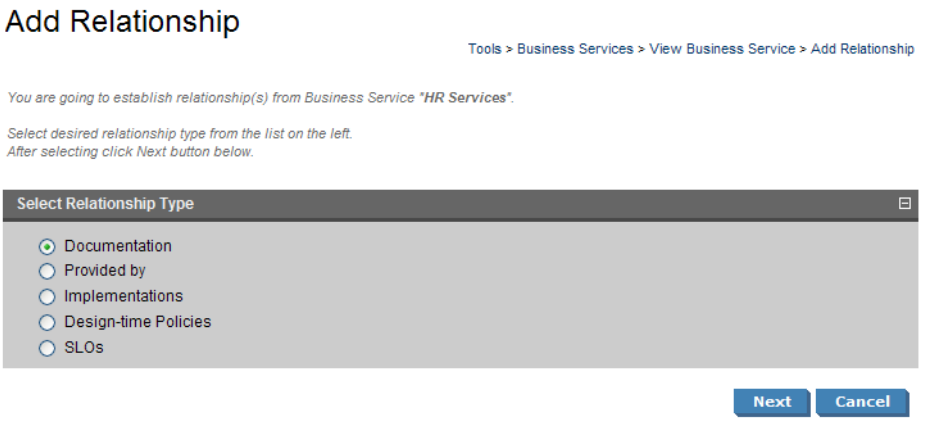
5 Click **Delete** to delete the selected artifacts.

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:

- Use **Filter** function to search for the required artifact.
- Click **New**, **Upload**, or **New Link** to create a new artifact to be the object of the relationship.

  For details, see Creating an Artifact on page 236.
- Click **Upload** to create a new artifact with associated external content to be the object of the relationship.

  For details, see Uploading Service Infrastructure from Definition Documents on page 99.
- Click **New Link** to create a new documentation artifact with a link to external content to be th object of the relationship.

Select the artifacts to associate and then 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 or group.

To change the owner of an artifact:

1 From the View page of any artifact, click **Tools→Change Owner**, to open the Change Owner page.

2 Select the check box to the left of the artifact you need, and click **Next** to open the Select New Owner page.

If the selected artifact is governed by a lifecycle process, select whether to **Restrict to Governed Artifacts**.

3 In the New Owner field, select the **Group** or **User** tab, and in the Search For field, enter the name to search - using an asterisk (*) as a wildcard, and then click **Go**.

Matching names are displayed in the field below.

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

5 In the Summary page, do the following:

- If the artifacts is governed by a lifecycle process, select whether you want to include subartifacts in the change of ownership.

When performing a bulk operation, including subartifacts which are governed by a lifecycle process leads to all subartifacts in the lifecycle dependency tree being changed.

- Select whether you want to send email notifications of the change.

  The original owner and the new owner of the artifact are notified of the change.

6 Click **Finish**.

Changing ownership of artifacts can be performed as a bulk operation.

In order to change ownership of artifacts in bulk, you must be the current owner of each artifact.

To change ownership in bulk, follow the procedure for changing a single artifact from To change the owner of an artifact:, selecting multiple artifacts.

Categorizing Artifacts

SOA Systinet enables you to apply taxonomic categories to artifacts.

To categorize an artifact:

1 In the Tools view of an artifact, click **Edit** to open the edit view of the artifact.

The categories are organized by taxonomy in the General section.

2 In the Edit view, do any of the following:

- To add a category from a new taxonomy. click **Add Category** to open a list of taxonomies. Select a taxonomy, and click **Add** to select a category from that taxonomy.
- To add a category from an existing taxonomy, click **Add** under the taxonomy box, and click **Add** to select the category.
- To remove a category, click the red X next to the category.
- To remove all categories in a taxonomy, click **Remove All** under the taxonomy box.

3 Click **Save** to commit your changes and create a new revision of the artifact.

To categorize a set of artifacts:

1 In a Services list view or Tools browse view for a set of artifacts, select the artifacts to edit.

2 Open the Select Actions menu, and select **Edit Category Bag**.

The Edit Category Bags page opens.

3 In the Edit Category Bags page, do any of the following:

- Select **Include Subartifacts** to apply the changes to related secondary artifacts in the same lifecycle process.
- Select **Update** to amend the current categories, or **Replace all Categories** to remove all existing categories.
- To add or remove categories, use **Add Category** open a list of taxonomies. Select the taxonomy and then click **Add** to add a specific catagory.

4 Click **Save** to make your changes.

Managing Documentation

The main document management procedures are:

- Add a new document to the repository, as described in Adding Documentation on page 241.
- Attach documentation to an artifact, as described in Attaching Documentation to Artifacts on page 242.
- Edit the source document, as described in Editing Documentation on page 243.

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 Tools tab Catalog Browser click **Documentation** to open the Documentation page.

2 Do one of the following:

- Click **Upload** to use the SOA Systinet publisher functionality to create a documentation artifact with associated data content.

For details, see Uploading Service Infrastructure from Definition Documents on page 99.

- Click **New Link** to create a link to a document on a remote location.

  For details, see To create a documentation artifact with a link to external content:.

- Click **New** to create a documentation artifact without cached content or a link to an external document.

  For details, see Creating an Artifact on page 236.

This option is only available if enabled by the administrator.

For details, see "Configuration Options" in the *HP SOA Systinet Administrator Guide* .

To create a documentation artifact with a link to external content:

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

2 Click **New Link** to open the New Link page.

3 In the New Link page, input the following parameters:

Parameter	Definition
URL	The location of the document to link the new artifact to.
Type	Select a document type from the drop-down list.
Link Text	The name of the new documentation artifact.
Description	A description for the new 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**.

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

3 Do one of the following:

- Use **Filter** to search for the required document in the repository.
- Click **New**, **Upload**, or **New Link** to add a new document as described in Adding Documentation on page 241.

4 Select the document from the list and click **Next**.

5 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 236.

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 75.

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.

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

To change the external source document:

1 In the detail view Data section of the documentation, click **Update**.

2 Input or use **Browse** to select a new source document.

3 Click **Save** to upload the new document.

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 definition formats are:

- WSDL documents
- XML schema documents
- DTD documents
- XSLT stylesheets
- SCA Definitions
- BPEL Process Definitions

To publish a resource artifact:

1 In the Tools tab Catalog Browser click the relevant artifact type to open the browse page.

2 Click **Upload** to use the SOA Systinet publisher functionality to create a definition artifact with associated data content.

For details, see Uploading Service Infrastructure from Definition Documents on page 99.

Definition documents are updated and edited in the same way as documentation.

For details, see Editing Documentation on page 243. In the procedure replace documentation with the relevant definition artifact types.

Managing Versions

The following section describes the general approach to versioning of both data and metadata in the SOA Systinet repository. Two versions can be created, depending on the significance of the change to the artifact:

New Branch

A version created as a result of a major change to an artifact, which requires the commencement of a new artifact lifecycle.

When a new major version of an artifact is created, SOA Systinet; creates a new copy of the original artifact, with it's own independent lifecycle. This makes it possible to have multiple versions of the same artifact in different lifecycle stages in the same repository.

For example, version 1.0 of a policy artifact can describe a policy approved for production use, while version 2.0 of the same policy artifact can be in development.

Version Number Update

A version created as a result of a minor change in the data or metadata of the artifact, which does not require the commencement of a new artifact lifecycle. Only the value of the version property is changed and a new revision is created.

To create a new branch version of an artifact:

1. In the Services or Tools view of an artifact click **New Version**.

   The New Version page opens.

2. Select **New Branch**.

3. Enter the version number you want to apply to the artifact and select **Backwards Compatible** if you want to mark the new version as compatible with the current version.

4 If you want to include subartifacts, click the **Include Subartifacts** check-box to open the drop down list of available artifacts. Otherwise, proceed to Step 6.

5 Toggle the check-box next to the artifacts you want to include, to switch between the following options in the **Actions** column:

- **New Version**

  A new version of the artifact will be created.

- **Skip**

  A new version of the artifact will not be created.

- **Reuse**

  The artifact is reused and the new version of the parent artifact contains a relationship, pointing to the subartifact.

  To create a new version for all artifacts, click **Select All**.

  To remove a selection for all artifacts, click **Deselect All**.

6 Click **Save**.

To update the version number of an artifact:

1 In the Services or Tools view of an artifact click **New Version**.

The New Version page opens.

2 Select **Version Number Update**.

3 Enter the version number you want to apply to the artifact (the next version update number is applied by default).

4 If you want the version number update to be applied to subartifacts, click the **Include Subartifacts** check-box to open a drop down list of available artifacts. Otherwise, proceed to Step 6.

5 Select the artifacts you want to include.

To select all subartifacts in the tree, click **Select All**.

Selecting a subartifact changes the status in the Action column to **New Version**. Subartifacts which have not been selected retain the status **Skip**.

6 Click **Save**.

SOA Systinet writes the changes to the repository which are applicable to the specified version:

- **New Branch**

  The artifact is cloned and version fields are set.

- **Version Number Update**

  The artifact version number is updated.

To avoid creating new versions of artifacts on a one by one basis, SOA Systinet enables you to create new versions of artifacts using a bulk operation.

The bulk operation for versioning only enables a minor version number update.

To create new versions for a set of artifacts:

1 In a Services list view or Tools browse view for a set of artifacts, select the artifacts to version.

2 Open the Select Actions menu, and select **Change Version**.

The Change Version page opens.

3 Select **Include Subartifacts** to apply the changes to related secondary artifacts in the same governance process.

4 Input the new version number.

5 Click **Change Version** to apply your changes.

The version history of an artifact is available in the Service and Tools view of an artifact. Open the Version menu and select **Version**.

For details, see Revision and Version History on page 233.

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.

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.

For details, see "Setting Up Registry Integration" in 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 section describes:

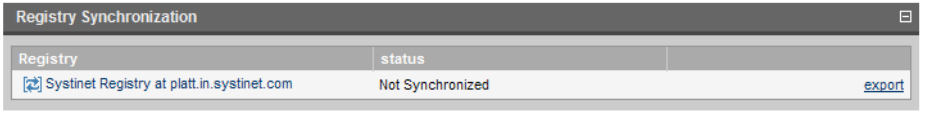
- Registry Synchronization on page 249
- Exporting Data To Registry on page 250
- Deleting Data From a Registry on page 252

Importing Services from Registries on page 103 explains how to import registry data as part of Chapter 10, Service Discovery.

Registry Synchronization

Each artifact that corresponds to a UDDI entity contains a **Registry Synchronization** section in its detail view (see Tools View on page 223):

Figure 68. Registry Synchronization Details



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

Table 3. Synchronization Status

Synchronization Status	Description
Not Synchronized	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	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	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 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.

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**.

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.

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 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**.

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

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.

19 Governance Tools

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

- Tools on page 255

  Are the basic utilities for performing governance actions.

- Tasks and Scheduling on page 267

  Enable the use of a tool on an artifact or set of artifacts with the option of periodic or scheduled execution.

- Reports on page 271

  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 256

  Report the potential impact of a change to an artifact on the other artifacts it depends on or impacts.

- Job Tools on page 258

  Are customized tools created to perform miscellaneous tasks.

- Reporting Tools on page 260

  Use customized reports to query the repository.

- Sync Tools on page 262

  Update the repository with the latest versions of externally sourced documents.

- Policy Compliance Tools on page 267

  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 on page 256
- Impact Reports on page 257
- Creating an Impact Tool on page 258

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 Tools View on page 223 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.

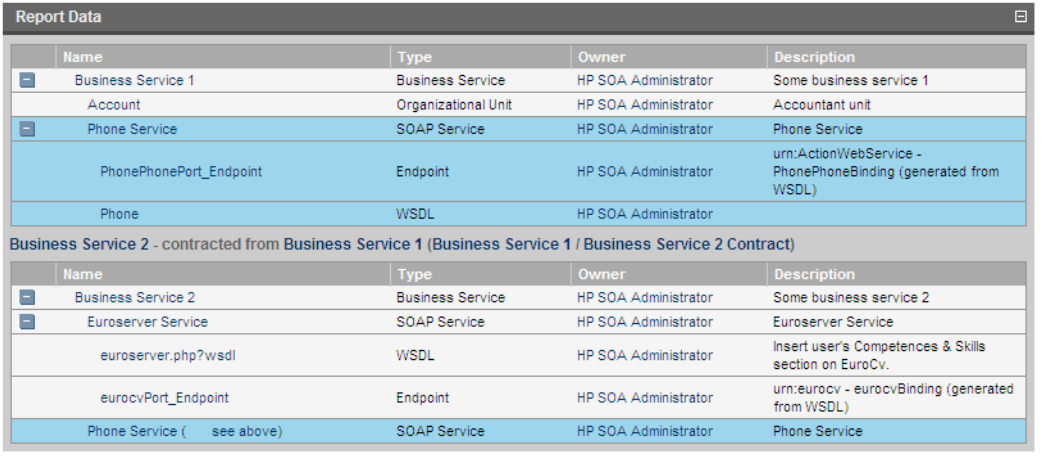
Impact Reports

Impact reports are generated by running the impact tool as described in Running the Impact Management Tool on page 256 or the result of automated tasks as described in Tasks and Scheduling on page 267.

To access impact reports, browse the reports as described in Reports on page 271 and filter for report category **Impact Management**.

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

Figure 69. Impact Report Data



Report Data

Name	Type	Owner	Description
Business Service 1	Business Service	HP SOA Administrator	Some business service 1
Account	Organizational Unit	HP SOA Administrator	Accountant unit
Phone Service	SOAP Service	HP SOA Administrator	Phone Service
PhonePhonePort_Endpoint	Endpoint	HP SOA Administrator	urn:ActionWebService - PhonePhoneBinding (generated from WSDL)
Phone	WSDL	HP SOA Administrator	

Business Service 2 - contracted from **Business Service 1** (**Business Service 1** / **Business Service 2 Contract**)

Name	Type	Owner	Description
Business Service 2	Business Service	HP SOA Administrator	Some business service 2
Euroserver Service	SOAP Service	HP SOA Administrator	Euroserver Service
euroserver.php?wsdl	WSDL	HP SOA Administrator	Insert user's Competences & Skills section on EuroCv.
eurocvPort_Endpoint	Endpoint	HP SOA Administrator	urn:eurocv - eurocvBinding (generated from WSDL)
Phone Service (see above)	SOAP Service	HP SOA Administrator	Phone Service

Figure 69 shows that Business Service 1 is dependent on the Account organizational unit and the Phone Service implementation which also has dependencies on an endpoint and WSDL.

Business Service 1 is also a consumer of Business Service 2, so the dependencies of Business Service 2 are displayed as well.

Note that Business Service 2 also depends on the Phone Service implementation but the breakdown of the Phone Service dependencies is not repeated.

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 268.

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 268.

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 Software 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 267 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 216).

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 260.

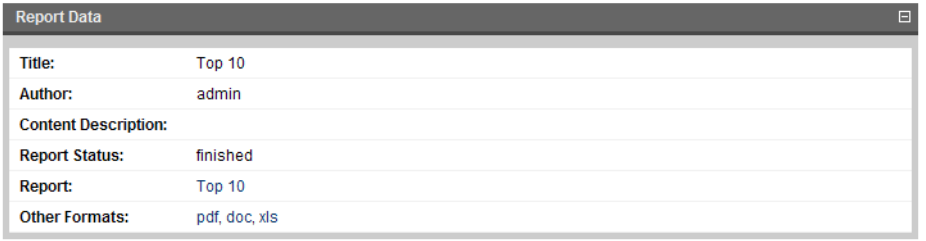
Reporting Tool Reports

Reporting tool reports are generated by running one of the default reporting tools as described in Running a Reporting Tool on page 260 or the result of automated tasks as described in Tasks and Scheduling on page 267.

To access reporting tool reports, browse the reports as described in Reports on page 271 and filter for report category **Reporting**.

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

Figure 70. 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

Parameter	Definition
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 268, or for immediate execution as described in Running a Reporting Tool on page 260.

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 on page 262
- Running the Synchronization Tool on page 263
- Change Management Reports on page 265
- Creating a Sync Tool on page 266

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.

  In order for automatic synchronization to function you must create a scheduled change management task. See Tasks and Scheduling on page 267 for details.

- **Approval Required**

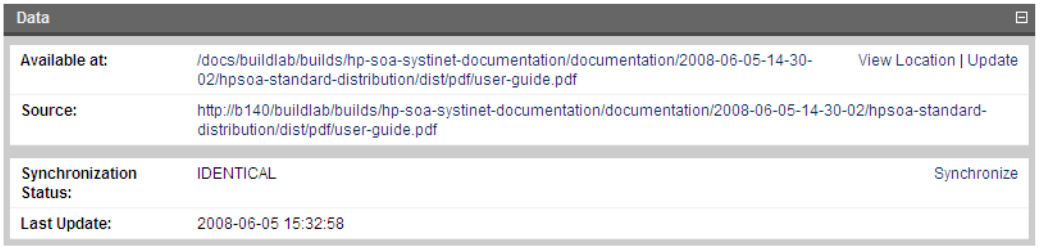
  The resource is marked with an out-of-sync flag and only updated after user approval. If you want to approve the change and update the document, run the change management tool as described in Running the Synchronization Tool on page 263.

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 Synchronization Tool

All artifacts that can be checked or updated have an associated Data section in their Tools detail page. These include WSDLs, XSDs, DTDs and Documentation.

Figure 71. Data Section



The following actions can be performed on artifacts associated with external documents:

- **Available at** functionality is available for resources uploaded from local or remote locations.
  - Resource name

    Click the resource name to open the version stored in the repository.
  - **View Location**

    Opens the repository location where SOA Systinet stores the resource.
  - **Update**

    Updates a cached resource if the original has changed.

- In addition, resources uploaded from remote locations have the following functionality:
  - Source name

    Click the source name to open it in the remote location.
  - **Synchronize**

    The synchronization status is shown. Click **Synchronize** to start the publishing process, and the **Finish** to upload the latest version of the remote resource.

From Service list views and Tools browse pages you can synchronize artifacts in bulk.

Select the artifacts to synchronize, open the Actions menu, and select **Synchronize**.

The change management tool executes with no confirmation required.

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.

Change Management Reports

Change management reports are generated by running the change management tool as described in Running the Synchronization Tool on page 263 or the result of automated tasks as described in Tasks and Scheduling on page 267.

To access change management reports, browse the reports as described in Reports on page 271 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 Synchronization Tool on page 263.

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 72. 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
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 box.

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 268.

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 Chapter 16, Validating Resources.

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 New menu of the Tools tab, click **Task**.
- Alternatively, in the Tools tab, in the Tasks and Reports portlet (see Tasks and Reports Portlet on page 215), 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 saved searches use **Find** to locate the saved search containing the artifacts to associate with the task and check the radio button to select it.

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 269, 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.

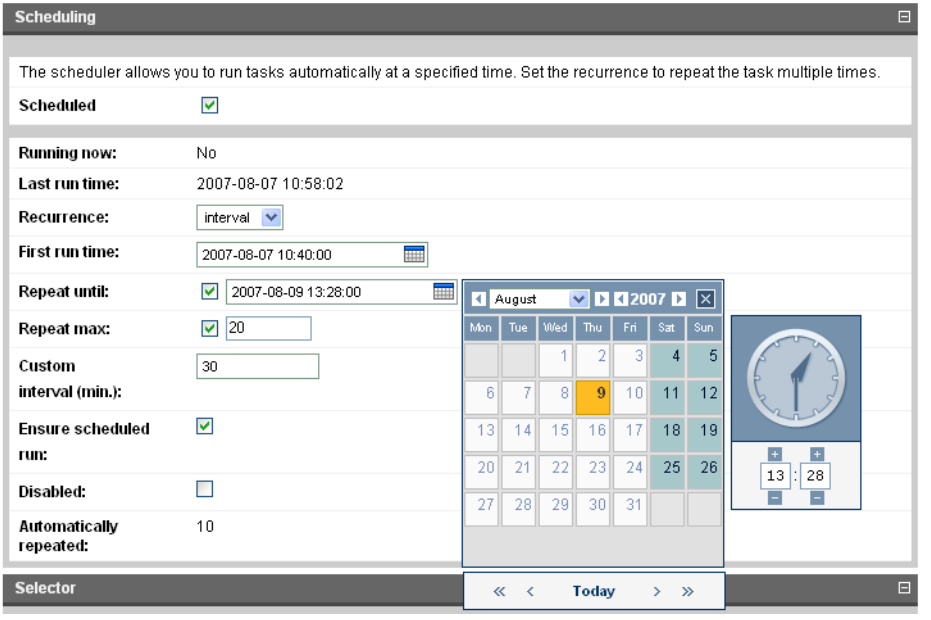
SOA Systinet converts and stores any input time to GMT. If you import scheduled tasks from a data image, review the scheduling to ensure that the tasks execute at the local time that you require.

To schedule a task:

1 Do one of the following:

- In the detail view of the task click **Edit**, and then select **Scheduled**.
- Select **Scheduled** during task creation as described in Creating a Task on page 268.

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.
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.

Parameter	Definition
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 Software 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 268.

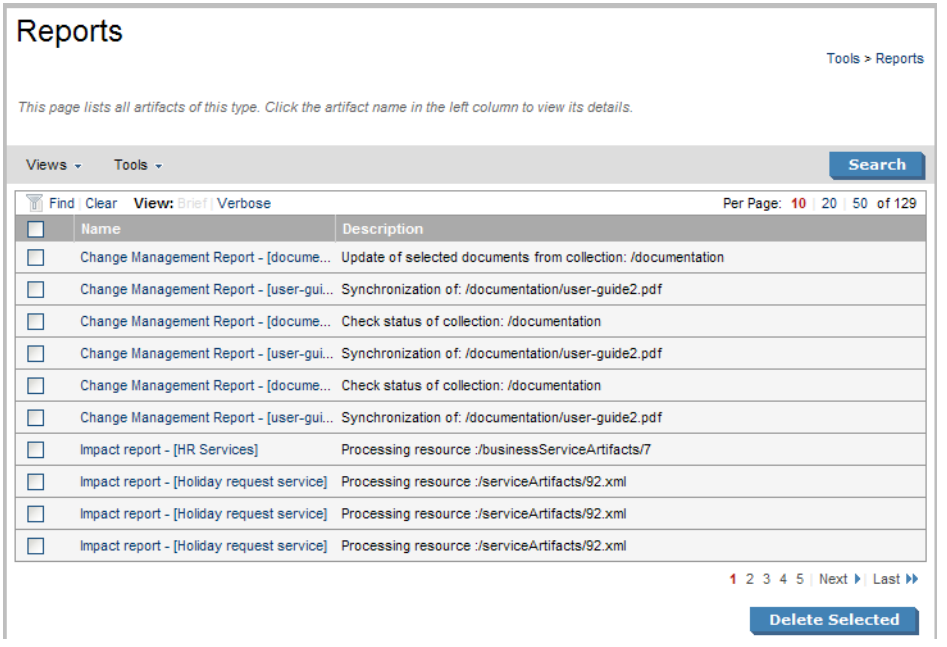
Reports

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 73. 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 255.

20 Advanced Searches

You can use SOA Systinet to create customized queries that search the repository. These searches can be stored and then reused. Saved 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 an Advanced Search

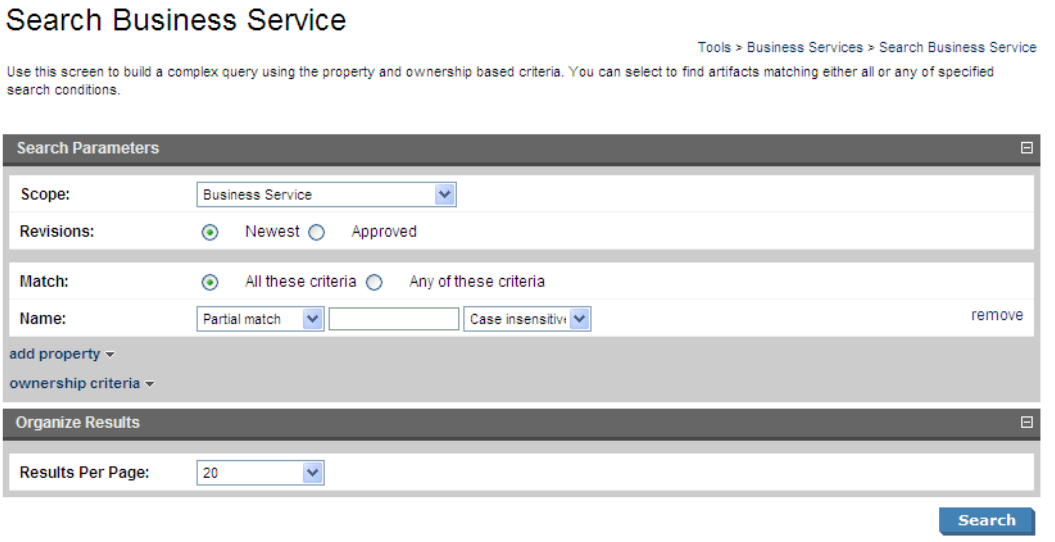
Each advanced search is associated with one type of artifact.

To create an advanced search:

1 Do one of the following:

- Click **Advanced Search** on any page.
- In the Tools browse view of an artifact type click **Search**.

The Search page for the artifact type opens:



2 Select the search parameters in the Search Criteria section:

Parameter	Definition
Scope	The artifact type to search
Revisions	Select one of the following: • **Newest Revisions** Search the latest revision of each artifact. • **Approved Revisions** Search the last approved revision of each artifact.

Parameter	Definition
Match	Do one of the following: • Select **All of these criteria** to find artifacts matching all the specified search criteria. • Select **Any of these properties** to find artifacts matching any one of the specified search criteria.
Search Terms	By default, the page shows search entry criteria for Name. You can add multiple search terms using **Add Property** and **Ownership Criteria**.
Add Property	Select the artifact properties to search from the drop-down list.  The options available depend on the artifact type.
Ownership Criteria	Select the ownership search criteria from the drop-down list.
Results per page	Select the output criteria from the drop-down list.

3 Click **Search** to execute your query and view the results.

4 Optionally, use **Filter** to filter the results or click **Refine Search** to return to Step 2.

5 Optionally, to store the search for later use, click **Save Search** to open the New Stored Search page.

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

Saved search artifacts are displayed in the Saved Searches section of the Services menu and you can also access them from the Tools tab Catalog Browser by expanding the Search and Transform branch, and clicking **Stored Searches**.

Editing a Saved Search

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

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

To modify a saved search:

1. Do one of the following:
   - In the Tools tab Catalog Browser, expand the Search and Transform branch and click **Stored Searches**.

     The Stored Searches page opens.

     Click the name of the stored search to edit.
   - In the Services tab menu Custom Views section, click the name of the search to edit.

   The detail view of the stored search opens.
2. Do one of the follwoing:
   - **To edit the basic search properties:**

     1. In the detail view of the saved 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 saved search, click **Redefine**.
     2. Do any of the following:
        - Click **Remove** to remove criteria from the search.
        - Add new conditions or modify the criteria as described in Creating an Advanced Search on page 273.

3 Click **Search** to execute the modified search.

4 Click **Save Search** to save your changes.

Running a Saved Search

1 Do one of the following:

- In the Tools tab Catalog Browser, expand the Search and Transform branch and click **Stored Searches**.

  The Stored Searches browse page opens.

  Click the name of the stored search to run.

- In the Services tab menu Custom Views section, click the name of the search to edit.

The detail view of the saved search opens.

2 In the detail view of the saved search, click **Run**.

The search results page opens.