HP SOA Systinet

Software Version: 3.10

Administrator Guide

Document Release Date: January 2009
Software Release Date: January 2009

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

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.

In this Guide

The administrator has a number of responsibilities both within SOA Systinet and regarding its maintenance.

This guide contains the following chapters:

- Chapter 1, Administering SOA Systinet

  Administration facilities accessed from the SOA Systinet UI.

- Chapter 2, System Administration.

  Common tasks performed by the system administrator.

- Chapter 3, Setup Tool

  Modify and control the SOA Systinet configuration.

- Chapter 4, Administration Utilities

  Command line tools provided with SOA Systinet.

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.
`java -jar hpsystinet.jar`	User input.
`C:\System.ini`	File names, 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 logon page.

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

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:

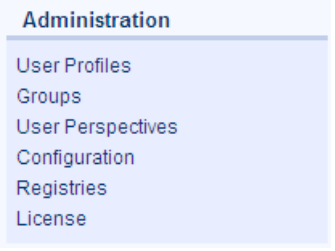
http://h20229.www2.hp.com/passport-registration.html

1 Administering SOA Systinet

The administrator has additional management options within SOA Systinet that are either not visible to other user perspectives or that HP Software recommend only the administrator perform.

Most of the Administrator options are accessed from the Tools page Administration menu, as shown in Figure 1.

Figure 1. Administration Menu



This chapter describes these additional administration functions in the following sections:

- Profile Management on page 10
- Configuration Options on page 18
- Access Rights on page 20
- Integrating with Other Products on page 24
- Managing the License on page 39

Profile Management

SOA Systinet delegates user management to LDAP or an application server user store. Users are represented in SOA Systinet by profiles for artifact ownership and notification purposes.

When users first log on to SOA Systinet, they are authenticated against the external user store. A user profile is created, based on their external account.

This section describes the following profile management functions:

- Managing User Profiles on page 10
- Managing User Groups on page 14
- Managing User Perspectives on page 18

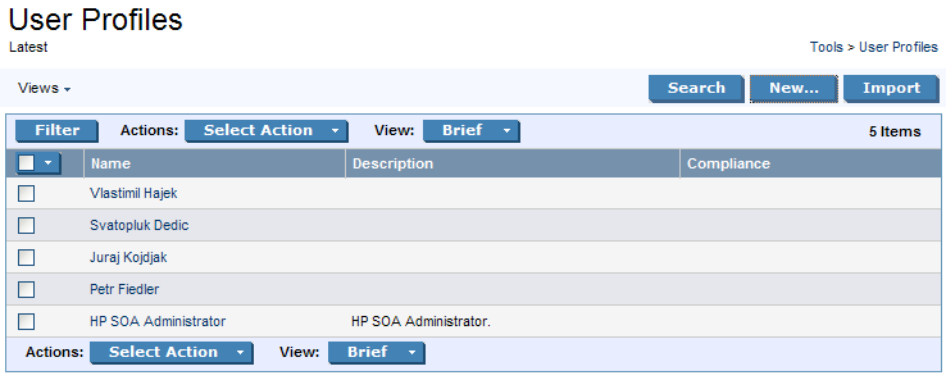
Additionally, the Administrator can manage permissions at the artifact and collection level using the Access Rights context action menu option available in artifact detail and browse views.

For details, see Access Rights on page 20.

Managing User Profiles

From the Administration section of the Tools menu, select **User Profiles** to open the User Profiles page.

Figure 2. User Profiles



Click **New** to create a new user profile.

For details, see Creating Profiles on page 12.

If you are using a non-LDAP/AD external user store then you can click **Import** to create a set of profiles from a CSV file.

For details, see Importing Profiles on page 14.

Click a profile name to view the details for that profile.

Click **Disable** or **Enable** to control the user sign in privileges.

For a disabled user, there is an option in the Tools context menu to **Retire User**. Select this option and then select a new owner to transfer all the artifacts from the retired profile to a new one.

For a retired user, there is an option in the Tools context menu to **Delete User**. Select this option to permanently delete the user profile from the system.

Click **Edit** to change the profile details.

The edit details are the same as the options available to the user with the addition of the Preferences section, enabling you to add administration privileges.

For user profile details, see "Managing Your Profile" in the *HP SOA Systinet User Guide*.

Creating Profiles

A user profile can represent either of the following:

- A user in the user store.
- An external contact.

A profile without a corresponding external account cannot sign in to SOA Systinet. Use this kind of profile for contacts and users who need to be represented in your SOA but who do not need to use SOA Systinet.

To create a profile:

1. In the Tools menu, in the Administration section, click **User Profiles**.

   The User Profiles page opens.

2. Click **New**.

   The New User Profile page opens.

3. Enter the following basic information:

Table 1. Basic Information

Parameter	Definition
Name	Name of the user.
Description	Description for the new user.
Login Name	Log-on name for the new user matching the user store ID. Not required for a contact type profile. You cannot change the log-on name after you create the profile.
Email	Email address for notifications.

4 Enter the following personal information:

Table 2. Personal Information

Parameter	Definition
Contact Role	Select a user role from the drop-down list.
Instant Messenger	Messenger ID. Use **Add** to create multiple entries.
Phone Number	Contact telephone number. Use **Add** to create multiple entries.
Language Code	Language spoken by the new user.
Categories	Use **Add Category** to select taxonomic categories.

5 Optionally, use the Address section to input a mailing address for the user with **Geographical Location** selection.

6 Click **Save** to create the new user profile.

By default, the new profile is not given administrator privileges in the Preferences section. Create the profile and then edit it if you want to the new profile to be an administrator.

Importing Profiles

SOA Systinet enables you to create a set of profiles from a comma separated variable (CSV) file.

To import profiles:

1. In the User Profiles page, click **Import**.
2. Input or browse for the location of the CSV file.
3. Click **Import** to create the user profiles.

The CSV file must meet the following conditions:

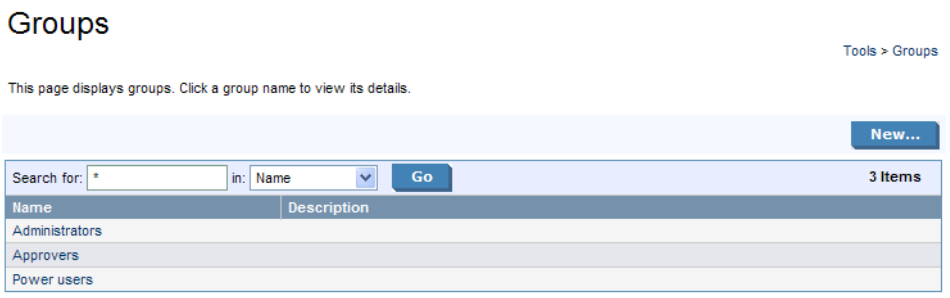
- The parameter names must contain a comma separated list of the parameters in each subsequent line.
- The parameter names must match those listed in the User Profile Import page.
- The parameters, *loginname*, *name*, and *email* must be present.

Managing User Groups

In addition to any groups managed by the external user store, you can manage local groups in SOA Systinet.

In the Administration menu, click **Groups** to open the Groups page:

Figure 3. Browse Groups



To use SOA Systinet to create or edit user groups in SOA Systinet, you must set the appropriate option, as described in Configuration Options on page 18.

Click **New** to create a new user group.

For details, see Creating a User Group on page 15.

To view the details for a group, click the group name.

To change its details or membership, click **Edit**. For details, see Editing a User Group on page 17.

There is an option in the Tools context menu to **Retire Group**. Select this option and then select a new owner to transfer all the artifacts owned by the retired group to a new group or user.

Retire Group only affects group ownership of artifacts, artifacts owned by members of the group, group privileges, and group membership are not affected.

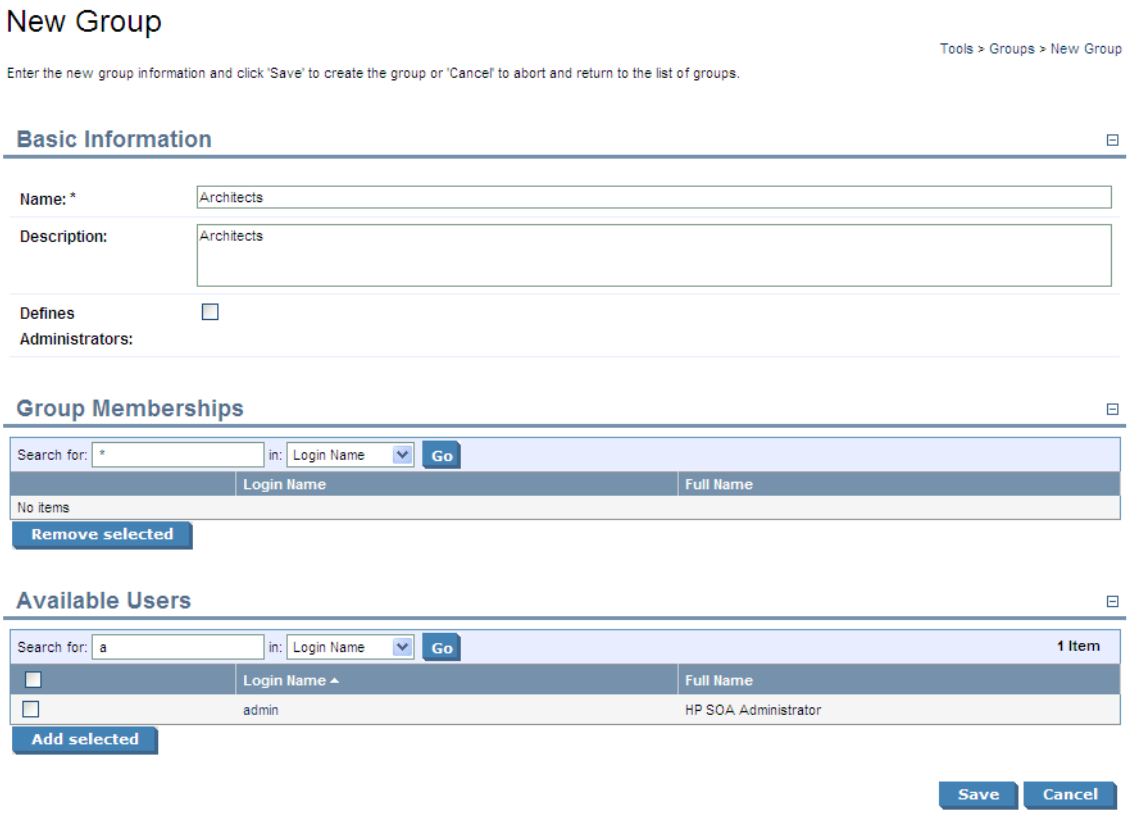
Creating a User Group

You can delegate the ownership of artifacts and voting for lifecycle promotion approval to groups as well as users.

To create a new user group:

1 In the Groups page, click **New** to open the New Group page:

Figure 4. Create New Group Page



2 Input the following parameters:

Parameter	Definition
Name	The name for the new user group.

Parameter	Definition
Description	A description of the user group.
Defines Administrators	Select if the group has Administrator privileges.

3 You can add members to the new group.

In Available Users, use the search function to identify users. Select the users from the list and click **Add Selected** to add them to Group Memberships.

4 You can remove members from the group.

In Group Memberships, use the search function to identify users. Select the users from the list, and click **Remove Selected** to remove them from Group Memberships.

5 Click **Save** to create the new group.

Editing a User Group

User groups frequently change because of staff changes.

To edit a user group:

1 In the Groups page, click the group name to open its detail view.

2 Click **Edit** to open the edit view.

3 Edit the name and description and apply the **Defines Administrator** flag, as required.

4 You can add members to the group.

In Available Users, use the search function to identify users. Select the users from the list, and click **Add Selected** to add them to Group Memberships.

5 You can remove members from the group.

In Group Memberships, use the search function to identify users. Select the users from the list, and click **Remove Selected** to remove them from Group Memberships.

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

Managing User Perspectives

Perspectives offer different views of SOA Systinet according to the needs of the user.

To edit the membership of a perspective:

1 In the Perspectives page, click the perspective name to open its detail view.

2 Click **Edit** to open the Edit Perspective page.

3 Click **Filter** and input a search term to populate the Perspective Membership list.

4 Do any of the following:

- Click **Add** to add new groups.

  Click the red X next to a group to remove it.

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

Configuration Options

SOA Systinet enables you to control to open a page enabling you to control some aspects of SOA Systinet.

To configure SOA Systinet:

1 In the Tools menu, in the Administration section, select **Configuration**.

The Configuration page opens.

2 In the configuration page, set any of the following options:

- **Full Text Search**

  Select this option to enable full text search in the SOA Systinet UI.

  For details, see "Full Text Search" the *HP SOA Systinet User Guide*.

Full-text search must also be enabled on the database. For details, see "Configuring the Database for Full Text Searching" in the *HP SOA Systinet Installation and Deployment Guide*.

By default, SOA Systinet appends a % to search terms. To disable this functionality, see Disabling the Addition of % to Search Terms on page 70.

- **Enable New Button**

  By default, the UI does not offer the option to create new artifacts where there is normally associated external content (for example, documentation or WSDLs).

  Set this option if you want to create new artifacts of this type without the associated content.

- **Self Test Access**

  Enable this option to perform a set of start-up checks.

  For details, see "SOA Systinet Self-Tester" in the *HP SOA Systinet Installation and Deployment Guide*.

- **Group Management**

  Select this option to enable SOA Systinet group management features.

  For details, see Managing User Groups on page 14.

This option is only available when SOA Systinet is integrated with LDAP. If LDAP is not used Group Management is available by default.

- **SSL Certification**

  Select the authentication method to apply to SSL certificates.

The options correspond to those described in "SSL Customization" in the *HP SOA Systinet Installation and Deployment Guide*.

Table 3. Certificate Trust and Customization Categories

Certificate Trust	Customization
Java/JSSE default key/trust stores...	default
Server certificates are always trusted...	skipped
Database key/trust stores...	database
Compositon of database and default...	composite

Access Rights

Access rights are read and write permissions. You can change the access rights for an artifact or a set of artifacts. Changing access rights for a collection of artifacts does not change the access rights for individual artifacts in the collection.

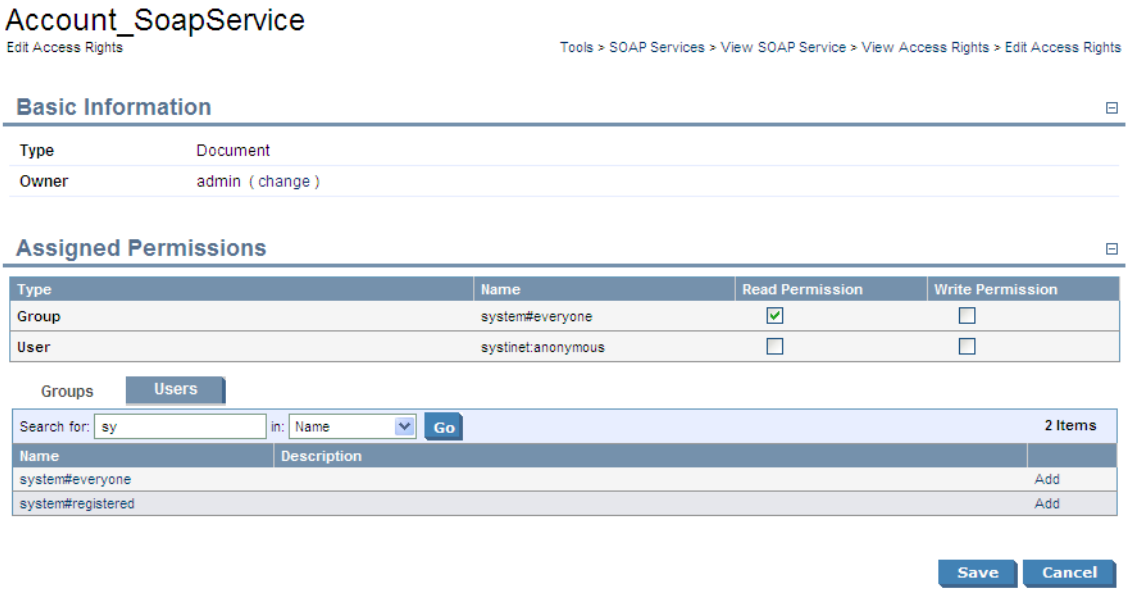
You can also create automatic actions to change access rights as a result of a lifecycle change.

To edit the access rights for a single artifact:

1. From the Tools or Services view of an artifact, open the Views context menu, and select **Access Rights**.

   The View Access Rights page opens for the artifact.

2. Click **Edit** to open the Edit Access Rights page:



3 To grant access rights to a user or group, click **Add** and set the read and write permissions.

To remove access rights from a user or group, clear both permission boxes.

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

To edit access rights for 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 Access Rights**.

The Edit Access Rights page opens.

3 In the Edit Access Rights 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 access rights, or **Replace** to remove the existing permissions and replace them with the selected ones.
- Select **Notify on Completion** to receive an e-mail notification when the task completes.
- Use **Add Group** and **Add User** to select the users and groups to add or remove.

4 Click **Save**.

To define an automatic change access rights action:

1 In the Stage Definition page of a governance process, expand **Add Action** and select **Change Access Rights**.

The Change Access Rights page opens.

For details about setting a Stage Definition, see "Defining Lifecycle Stages" in the *HP SOA Systinet User Guide*.

2 For the Run When field, select the event to trigger the action.

For details, see "Automatic Action Triggers" in the *HP SOA Systinet User Guide*.

3 For Select Operation, do one of the following:

- Select **Update** to add or remove your permission changes to existing access rights.
- Select **Replace** to replace existing access rights with your permission settings.

4 Select **Include Sub-Artifacts** to apply the access right changes to associated secondary artifacts as well.

5 If the trigger is Entering Stage and the operation is Update, select **Restore Access Rights** to create another action for the Leaving Stage trigger to reverse the access right changes.

6 In the Access Rights section, click **Select** next to the access rights change you want to make.

The Select User or Group pane opens.

7 In the Select User or Group pane, do any of the following:

- To add a user:

  1 Select the **Users** tab.

  2 In the **Search for** field, enter the user name to locate (use 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 **Select** next to the user name.

  The selected user is added to the access rights change.

- To remove a user, select the check-box next to their name, and then click **Remove**.

  The selected users are removed from the access rights change list.

- To add a group:

  1 Select the **Groups** tab.

  2 In the **Search for** field, enter the group name to locate (use an asterisk (*) as a wildcard).

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

  4 Click **Select** next to the group.

  The selected group is added to the access rights change list.

- To remove groups, select the check-box next to the group name, and then click **Remove**.

  The selected groups are removed from the access rights change list.

8 Click **OK** to return to the Stage Definition page.

The new Access Rights action is added to the Actions list.

For details about changing the default ACL, see Configuring the Default ACLs on page 67.

Permissions are cumulative. For example, if an individual user without write permission is a member of a group with write permission, the user inherits permission to edit the artifact. Similarly, a user with write permission who is a member of a group without permission retains permission to edit the artifact.

Do not remove write permission from the Contacts collection for the `system#registered` group. This permission is required for the registration of new users.

Integrating with Other Products

You can integrate SOA Systinet with the following products to access the information and content that they provide:

- **UDDI Registry v2 or v3**

  Use a UDDI Registry as the central storage location for your service infrastructure.

  You can import, export, and synchronize your service artifacts with entities in the registry.

- **HP Business Availability Center 7.5**

  Discover services stored in *HP Business Availability Center (BAC)* and *Universal Configuration Management Database (UCMDB)* and enter them into SOA Systinet governance. These discovered services are then monitored for changes and you can synchronize any changes from UCMDB into SOA Systinet.

  Use BAC to monitor the performance of your services.

  You can view information generated by BAC on shared services in SOA Systinet service pages.

- **HP SOA Policy Enforcer 3.00 Patch 1**

Use *HP SOA Policy Enforcer (SOA PE)* to enforce company policy on run-time services.

You can open SOA PE pages and view the information on shared services from SOA Systinet service pages.

- **HP Service Test Manager 9.41**

  Use the *Service Test Manager(STM)* component of HP Quality Center (QC) to track your service testing.

  You can view information generated by STM on shared services in SOA Systinet SOAP Service pages.

  > You must also install `Service Test Add-in for Quality Center 9.50` plug-in on QC clients that use SOA Systinet-STM integration.

Each product requires some setup and configuration in SOA Systinet.

For details, see the following sections:

- Setting Up Registry Integration on page 25
- Setting Up BAC/UCMDB Integration on page 34
- Setting Up SOA Policy Enforcer Integration on page 36
- Setting Up STM Integration on page 37

Setting Up Registry Integration

Before you can perform any registry synchronization, you must configure at least one UDDI Registry Artifact. SOA Systinet can be integrated with both v2 and v3 UDDI API registries.

> The version protocol should not be changed. After an artifact is synchronized (exported/imported) with a UDDI registry v2 entity it should not be synchronized with other UDDI registry v3 entities and vice versa.

The UDDI specification defines interoperable standards for the exchange of data about web services, their interfaces, implementations, deployments and responsible contacts.

For details, see the following website:

www.uddi.org [http://www.uddi.org]

A UDDI registry is an implementation of the UDDI specification, for example HP SOA Registry Foundation. The UDDI specification has three major versions, commonly named v1, v2 and v3. SOA Systinet is interoperable with UDDI v2 and v3 compliant registries.

The UDDI specification defines four major structures:

- **Business Entity**

  A business entity represents a business unit, company, department, and so on. It contains one or more company names, contacts, and provided Business Services. It corresponds to Organizational Unit in the SOA Systinet SDM model.

- **Business Service**

  A business service represents a logical service. Business Service cannot stand alone, it must always be part of a superior Business Entity. It corresponds to an Implementation in the SOA Systinet SDM model.

- Binding Template

  A binding template represents technical services. It includes information needed to create and run client applications. It corresponds to Endpoint in the SOA Systinet SDM model.

- **tModel**

  A tModel represents an arbitrary resource, that cannot be described by the structures above. For example; specification, documentation, (part of) WSDL document, policy or taxonomy. Therefore there is not a common map of tModel to an SDM model artifact.

The mapping for certain types of tModel can be defined in `SOA_HOME/conf/registryconf.xml`.

See www.uddi.org [http://www.uddi.org] for more details.

It is not possible to export a WSDL SOAP service to a non-Systinet UDDI registry unless it complies with technical note Using WSDL in a UDDI Registry, Version 2.0.2 [http://www.oasis-open.org/committees/uddi-spec/doc/tn/uddi-spec-tc-tn-wsdl-v202-20040631.htm], specifically the v2 tModel Structure [http://www.oasis-open.org/committees/uddi-spec/doc/tn/uddi-spec-tc-tn-wsdl-v202-20040631.htm#_Toc76437813]. The registry must have available tModels (XML Namespace, XML local name, WSDL portType Reference).

Registry setup consists of the following steps:

1 Creating a Registry Artifact on page 27

2 Importing Registry Certificates on page 31

3 Synchronizing Taxonomies on page 31

Creating a Registry Artifact

To establish synchronization with a UDDI registry, you must create a registry artifact that contains important data about the registry configuration, such as the API version and API URLs.

To create a registry artifact:

1 Do one of the following:

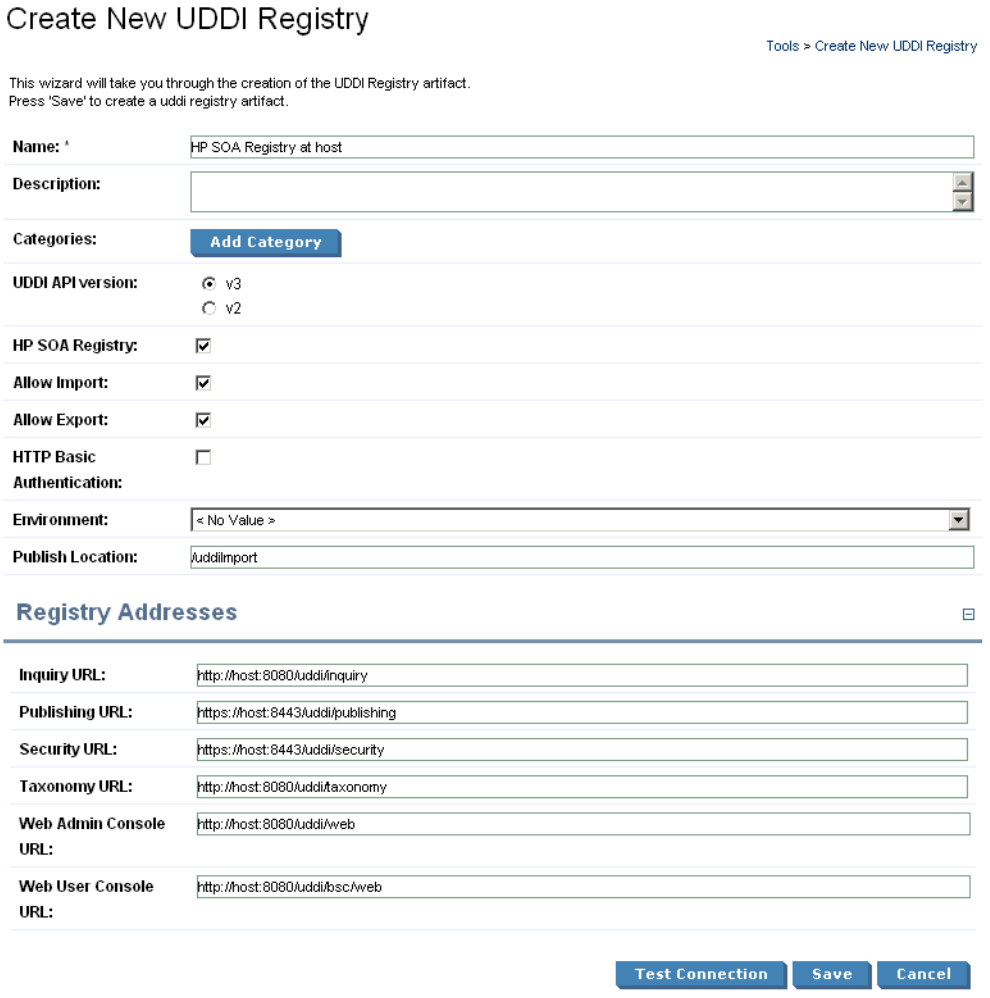
- In the Tools tab Catalog Explorer, expand Integration, and click **Registries** to open the Registries browse page, and then click **New**.
- In the Tools menu Registry Content section, click **Import Registry Content** to open the Import Artifacts from the Registry page, and then click **New Registry**.

The Create New UDDI Registry page opens.

2 Enter the following parameters:

Parameter	Definition
Hostname	The name of the server where the registry is running
HTTP Port	The port for non-secure access to the registry
SSL (HTTPS) Port	The port for secure access to the registry
Application Server Context	If the registry is ported to a J2EE server then input the context name
HP SOA Registry	Select if the registry is HP SOA Registry Foundation

3 Click **Next** to set the registry details:



4 Enter the general details for the registry:

Parameter	Definition
Name	The name of the registry artifact

Parameter	Definition
Description	A description for the new registry
Categories	Click **Add Category** to select a category from the available taxonomies
UDDI API Version	Select v3 or v2  Although you can create a UDDI v2 registry, the integration features are fully compliant with UDDI v3 only.
HP SOA Registry	Select if the registry is a HP SOA Registry Foundation
Allow Import	Select if the registry is a source of data import
Allow Export	Select if the registry is a target for data export
HTTP Basic Authentication	Select if the registry is secured with HTTP Basic Authentication.  This option only applies to the Publishing URL.
Environment	Select the environment from the drop-down list. The environment controls registry export and import functionality for endpoints. The environment set for the registry server is applied to imported endpoints. When services are exported to registry, related endpoints are only exported if their environment setting matches the environment setting for the registry server. Endpoints with no environment setting may be optionally exported.
Publish Location	The repository location to store resource content.

5 If the registry is a HP SOA Registry Foundation the **Registry Addresses** section is populated with addresses based on the input from the previous page in the form `http://<hostname>:<port>/<app_server_context>/inquiry` ..... For other registries you have to type the addresses manually.

6 Click **Test Connection** to verify the connection parameters and that the registry server is running.

In the event of an error, click **Details** to see more information.

If the test returns the error `Secure URL is not trusted` then you must import the SSL certificate for the registry. For details, see SSL Tool on page 89.

7 Click **Save** to create the new registry artifact.

Importing Registry Certificates

If HTTPS is used for SOA Systinet–HP SOA Registry Foundation communication, then it is necessary to import the registry certificates into the application server certificate store.

For details, see "SSL Certification" in the *HP SOA Systinet Installation and Deployment Guide*.

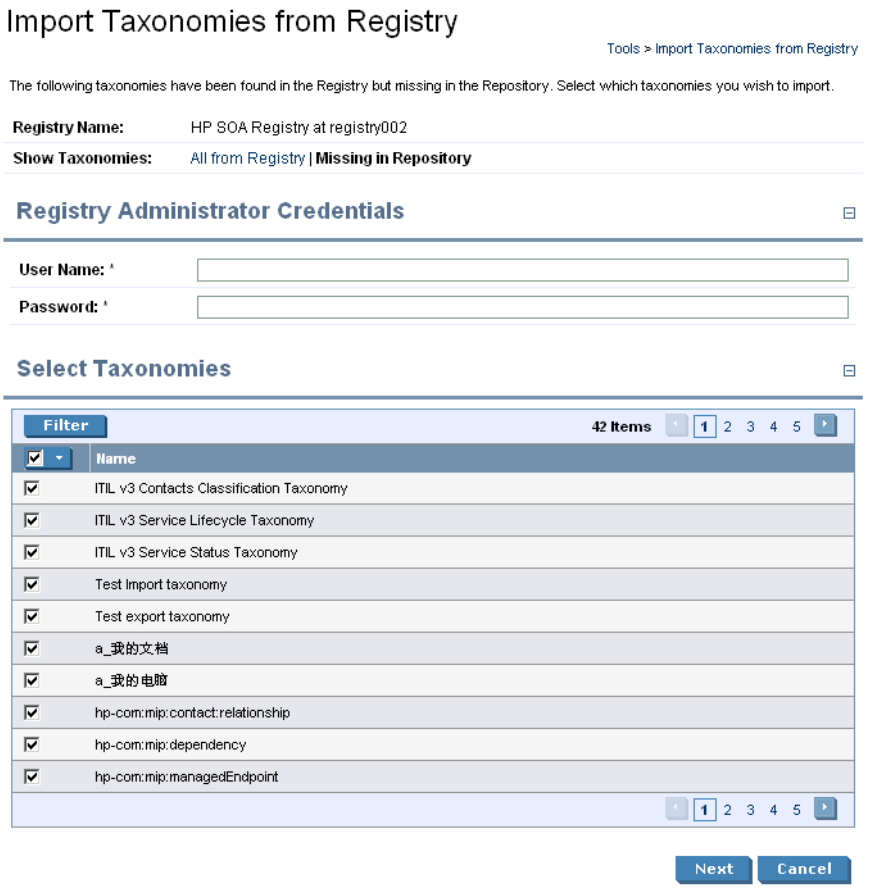
Synchronizing Taxonomies

A general precondition must be fulfilled before registry import/export. Taxonomies with the taxonomic values referenced by the imported/exported data must be present in both the source and target environment. The easiest way is to synchronize the taxonomies between the registry and SOA Systinet. In the case of missing taxonomies during import/export, SOA Systinet outputs an error message about the missing taxonomies and prevents the import/export. If the registry is a HP registry taxonomy synchronization can be done directly from SOA Systinet console.

Only a user with administrator permissions is allowed to perform taxonomy synchronization.

To import taxonomies from a registry:

1 In the detail view of the registry, select **Import Taxonomies** in the **Tools** context menu to open the **Import Taxonomies from Registry** page:

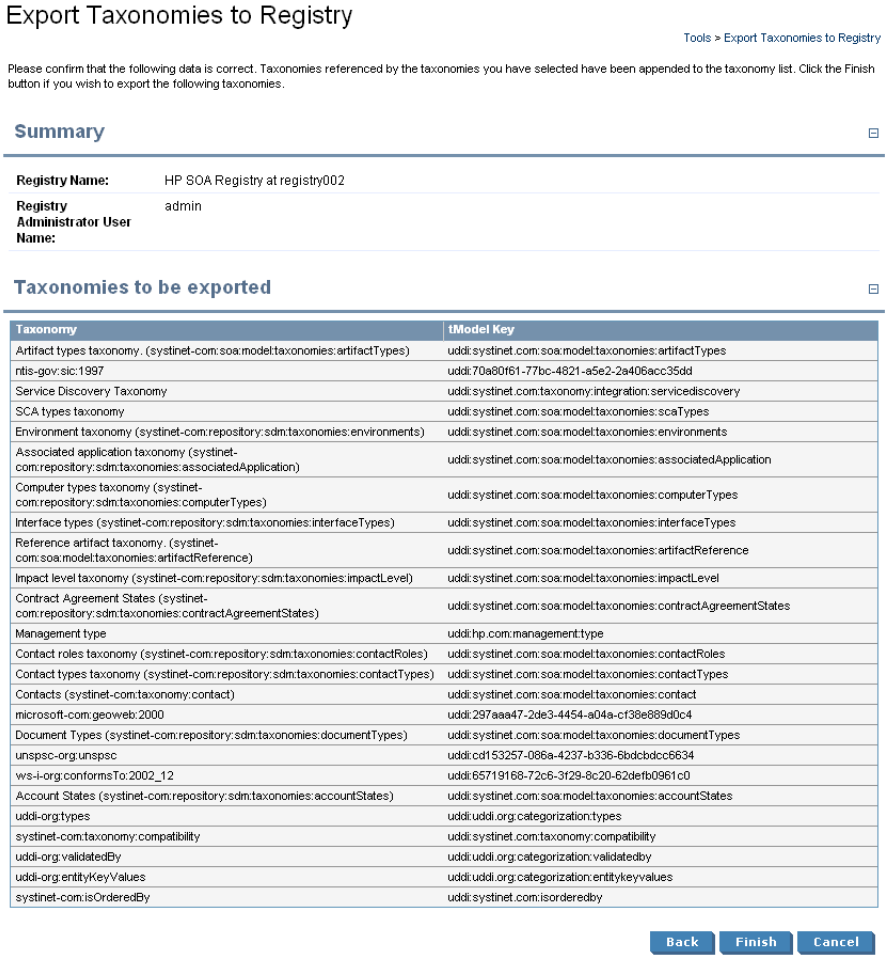


2 Input the registry credentials, de-select any taxonomies that are not required, and then click **Next**.

3 Review the export report that displays a list of imported taxonomies.

To export taxonomies to a registry:

1 In the detail view of the registry, select **Export Taxonomies** in the **Tools** context menu to open the **Export Taxonomies to Registry** page:



Export Taxonomies to Registry

Tools > Export Taxonomies to Registry

Please confirm that the following data is correct. Taxonomies referenced by the taxonomies you have selected have been appended to the taxonomy list. Click the Finish button if you wish to export the following taxonomies.

Summary

Registry Name:	HP SOA Registry at registry002
Registry Administrator User Name:	admin

Taxonomies to be exported

Taxonomy	tModel Key
Artifact types taxonomy. (systinet-com:soa:model:taxonomies:artifactTypes)	uddi:systinet.com:soa:model:taxonomies:artifactTypes
ntis-gov:sic:1997	uddi:70a80f61-77bc-4821-a5e2-2a406acc35dd
Service Discovery Taxonomy	uddi:systinet.com:taxonomy:integration:servicediscovery
SCA types taxonomy	uddi:systinet.com:soa:model:taxonomies:scaTypes
Environment taxonomy (systinet-com:repository:sdm:taxonomies:environments)	uddi:systinet.com:soa:model:taxonomies:environments
Associated application taxonomy (systinet-com:repository:sdm:taxonomies:associatedApplication)	uddi:systinet.com:soa:model:taxonomies:associatedApplication
Computer types taxonomy (systinet-com:repository:sdm:taxonomies:computerTypes)	uddi:systinet.com:soa:model:taxonomies:computerTypes
Interface types (systinet-com:repository:sdm:taxonomies:interfaceTypes)	uddi:systinet.com:soa:model:taxonomies:interfaceTypes
Reference artifact taxonomy. (systinet-com:soa:model:taxonomies:artifactReference)	uddi:systinet.com:soa:model:taxonomies:artifactReference
Impact level taxonomy (systinet-com:repository:sdm:taxonomies:impactLevel)	uddi:systinet.com:soa:model:taxonomies:impactLevel
Contract Agreement States (systinet-com:repository:sdm:taxonomies:contractAgreementStates)	uddi:systinet.com:soa:model:taxonomies:contractAgreementStates
Management type	uddi:hp.com:management:type
Contact roles taxonomy (systinet-com:repository:sdm:taxonomies:contactRoles)	uddi:systinet.com:soa:model:taxonomies:contactRoles
Contact types taxonomy (systinet-com:repository:sdm:taxonomies:contactTypes)	uddi:systinet.com:soa:model:taxonomies:contactTypes
Contacts (systinet-com:taxonomy:contact)	uddi:systinet.com:soa:model:taxonomies:contact
microsoft-com:geoweb:2000	uddi:297aaa47-2de3-4454-a04a-cf38e889d0c4
Document Types (systinet-com:repository:sdm:taxonomies:documentTypes)	uddi:systinet.com:soa:model:taxonomies:documentTypes
unspsc-org:unspsc	uddi:cd153257-086a-4237-b336-6bdcbdcc6634
ws-i-org:conformsTo:2002_12	uddi:65719168-72c6-3f29-8c20-62defb0961c0
Account States (systinet-com:repository:sdm:taxonomies:accountStates)	uddi:systinet.com:soa:model:taxonomies:accountStates
uddi-org:types	uddi:uddi.org:categorization:types
systinet-com:taxonomy:compatibility	uddi:systinet.com:taxonomy:compatibility
uddi-org:validatedBy	uddi:uddi.org:categorization:validatedby
uddi-org:entityKeyValues	uddi:uddi.org:categorization:entitykeyvalues
systinet-com:isOrderedBy	uddi:systinet.com:isorderedby

Back Finish Cancel

2 Input the registry credentials, review the taxonomy list, and then click **Save**.

3 Review the export report which displays the list of exported taxonomies.

Setting Up BAC/UCMDB Integration

SOA Systinet can integrate with *HP Business Availability Center* (BAC) and access the availability data generated by BAC about shared services.

BAC uses HP Universal Configuration Management Database (UCMDB) as a service repository. SOA Systinet can directly access UCMDB for service discovery.

SOA Systinet can integrate with only one BAC/UCMDB server.

If SOA Systinet already contains services discovered from BAC/UCMDB, do not delete the BAC/UCMDB server artifact. You may lose access to service discovery functions and discovered artifacts. If your BAC/UCMDB connection settings change, modify the properties of the existing BAC/UCMDB server. Do not delete it and create a new one.

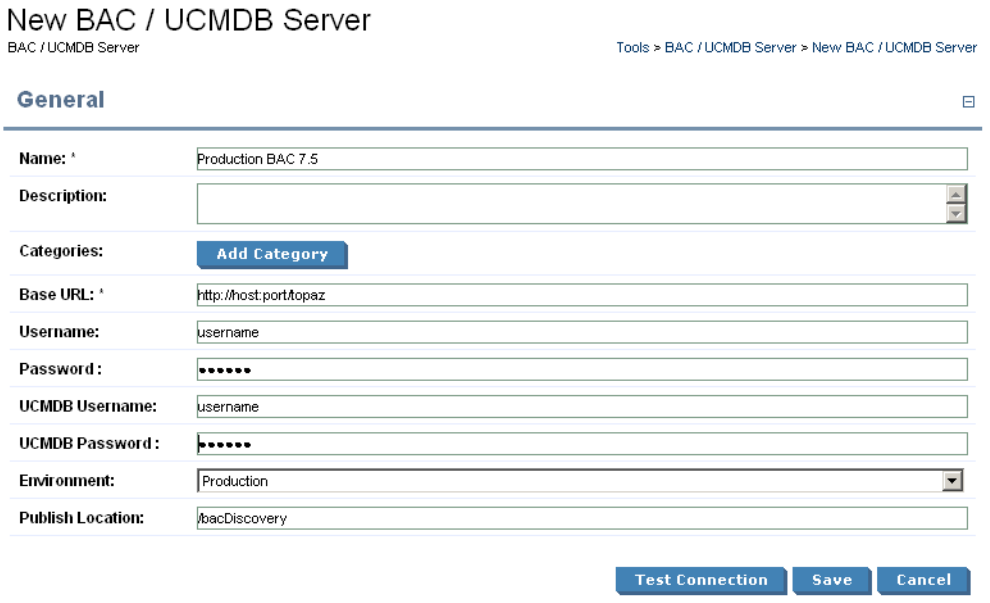
To create a BAC/UCMDB server artifact:

1 In the Tools tab Catalog Browser, expand Integration, and then click **BAC/UCMDB Servers**.

The BAC/UCMDB Servers page opens.

2 Click **New**.

The New BAC/UCMDB Server page opens:



3 Input the following parameters:

Parameter	Definition
Name	The name for the BAC/UCMDB server
Description	A description of the new BAC/UCMDB server
Categories	Click **add category** to select a category from the available taxonomies (administrator perspective only)
Base URL	The address of the BAC/UCMDB server. For example `http://mybacserver.com/topaz`.
Username and Password	Credentials for the BAC server, required to access service availability information from the BAC server.
UCMDB Username and Password	Credentials for the UCMDB server, required for service discovery.

Parameter	Definition
Environment	SOA Systinet uses the selected environment to categorize endpoints during service discovery. The default is `Production`.
Publish Location	The location in the repository to store resource content.

4 Click **Test Connection** to verify the connection parameters and that the BAC/UCMDB server is running.

In the event of an error, click **Details** to see more information.

If the test returns the error `Secure URL is not trusted` then you must import the SSL certificate for the BAC/UCMDB server. For details, see SSL Tool on page 89.

5 Click **Save** to create the new BAC/UCMDB server artifact.

For details about the features available with an integrated BAC/UCMDB server, see the following sections of the *HP SOA Systinet User Guide*:

- "BAC/UCMDB Service Discovery"
- "BAC/UCMDB Integration Features"

Setting Up SOA Policy Enforcer Integration

If you integrate SOA Systinet with *HP SOA Policy Enforcer* (SPE), you can access data about shared services on the SPE server.

SOA Systinet can integrate with only one SPE server.

To create an SOA Policy Enforcer server artifact:

1 In the Tools tab Catalog Browser, expand Integration, and then click **SOA Policy Enforcer Server**

The SOA Policy Enforcer Servers page opens.

2 Click **New**.

The New SOA Policy Enforcer Server page opens.

3 Input the following parameters:

Parameter	Definition
Name	The name for the SOA Policy Enforcer server.
Description	A description of the new SOA Policy Enforcer server
Base URL	The address of the SOA Policy Enforcer server. For example `http://mysoapeserver.com:5002/bse_refresh`.

4 Click **Test Connection** to verify the connection parameters and that the SOA PE server is running.

In the event of an error, click **Details** to see more information.

If the test returns the error `Secure URL is not trusted` then you must import the SSL certificate for the SOA PE server. For details, see SSL Tool on page 89.

5 Click **Save** to create the SOA Policy Enforcer server artifact.

For details about the features available with an integrated SOA Policy Enforcer server, see "SOA Policy Enforcer Integration Features" in the *HP SOA Systinet User Guide*.

Setting Up STM Integration

HP Service Test Management (STM) is a component of HP Quality Center (QC) for testing services.

STM accesses services in the SOA Systinet repository using the REST API SOA Systinet exposes. Automated tests can be generated on service definitions imported from a WSDL.

For details, see the *HP Service Test Manager* documentation.

SOA Systinet can integrate with STM and receive the data generated by STM about shared services.

SOA Systinet can integrate with multiple STM servers.

To create an Service Test Management server artifact:

1. In the Tools tab, in the Catalog Browser, expand Integration, and then click **STM Servers**.

   The STM Servers page opens.

2. Click **New**.

   The Publish STM Server page opens.

3. Input the following parameters:

Parameter	Definition
Name	The name for the STM server.
Description	A description of the new STM server.
Base URL	The address of the STM server. For example `http://mystmserver.com:8080/stm`
Username	Credentials for the STM server.
Password	
STM Domain	The domain containing the testing project in QC.
STM Project	The testing project in QC.
Environment	Select an environment from the drop-down list. Environment categorization is used for export to STM functionality. If the STM server is categorized, when a service is exported, the associated WSDL added to STM is amended to contain any related matching environment categorized endpoints. The default value is `Testing`.

4 Click **Test Connection** to verify the connection parameters and that the STM server is running.

In the event of an error, click **Details** to see more information.

If the test returns the error `Secure URL is not trusted` then you must import the SSL certificate for the STM server. For details, see SSL Tool on page 89.

5 Click **Save** to create the new STM server artifact.

For details about the features available with an integrated STM server, see "Service Test Manager Integration Features" in the *HP SOA Systinet User Guide*.

Managing the License

SOA Systinet employs a licensing system to control the following aspects of an installation:

- Usage limits, including the following:
  - Time limited licenses
  - Concurrent user limited licenses
  - Licensed user limited licenses
- Feature limits, including the following:
  - Contract Manager
  - Policy Manager

The administrator can manage the following aspects of a SOA Systinet license:

- Changing the License on page 40
- Managing Licensed Users on page 40

Changing the License

The administrator can change the SOA Systinet license.

To change the SOA Systinet license:

1. Contact SOA@hp.com [mailto:SOA@hp.com] or your sales representative for a new license key.
2. In the Tools menu Administration section, click **License**.

   The License page opens, displaying the current license.
3. Click **Enter License Key**.

   The Enter License Key page opens.
4. Input the user and license key, and then click **Next**.
5. Confirm the changes to your license, and then click **Finish**.

   The License page opens showing the details of the new license.

Managing Licensed Users

The administrator can modify which users can always access SOA Systinet.

To manage the licensed users:

1. In the Tools menu Administration section, click **License**.

   The License page opens displaying the current license.
2. In the License Conditions section, click **Edit** next to the Licensed User Seats.

   The Edit Licensed Users page opens.
3. In the Edit Licensed Users page, make any changes you want.

   To find out how to add users, see Adding Licensed Users on page 41.

To find out how to remove users, see Removing Licensed Users on page 41.

4 Click **Save** to confirm your changes and return to the License page.

Adding Licensed Users

The administrator can add users up to any license limit.

To add a licensed user.

1 In the Tools menu Administration section, click **License**.

The License page opens displaying the current license.

2 In the License Conditions section, click **Edit** next to the Licensed User Seats.

The Edit Licensed Users page opens.

3 In the All Accounts section, enter a user search term and click **Go**.

A list of users matching the search term appears.

4 Select the users you want, and click **Add Selected**.

The selected users appear in the Licensed Users section.

5 Click **Save** to confirm your additions and return to the License page.

Removing Licensed Users

The administrator can remove licensed users.

To remove a licensed user.

1 In the Tools menu Administration section, click **License**.

The License page opens displaying the current license.

2 In the License Conditions section, click **Edit** next to the Licensed User Seats.

The Edit Licensed Users page opens.

3 In the Licensed Users section, select the users to remove and click **Remove Selected**.

The selected users disappear from the Licensed Users section.

4 Click **Save** to confirm your removals and return to the License page.

2 System Administration

This chapter includes details of tasks that are required to administer an installation of SOA Systinet.

- Using the Audit Log on page 43

  Use the audit log to monitor SOA Systinet.

- Data Migration on page 55

  Migrate data from previous versions of SOA Systinet.

- Configuration Procedures on page 57

  Manage the configuration of SOA Systinet using the command-line utilities.

Using the Audit Log

The audit log enables you to track all the significant events and user actions in SOA Systinet.

The log is available in `systinet_audit.log` in the application server log folder for your deployment.

Each line in the log contains the following comma separated content:

Table 4. Audit Log Content

Content	Description
Time	The date and time of the event.
Category	The application component related to the event.
Event ID	A unique code for the event.
Result	The result of the event, usually `OK` or `FAILED`.
Context ID	The ID of the process related to the event.
Actor	The name of the user identity who performed the action.
Resource ID	The ID of the primary entity or entities involved in the event.
Detail	Readable text with a description of the event.

The entries in the log are described in the following tables organized by category:

- Table 5
- Table 6
- Table 7
- Table 8
- Table 9
- Table 10
- Table 11
- Table 12
- Table 13
- Table 14
- Table 15

- Table 16
- Table 17
- Table 18
- Table 19
- Table 20
- Table 21
- Table 22
- Table 23
- Table 24

Table 5. `application` Events

Event ID	Resource	Result	Description
1	Servlet Context	startup	Application started.
2	Servlet Context	shutdown	Application shut down.

Table 6. `application.license` **Events**

Event ID	Resource	Result	Description
10100		FAILED	Invalid license key. SOA Systinet is unavailable until you enter a valid license key using the Setup Tool.
10101		FAILED	System date change. SOA Systinet is unavailable until you adjust the system date to be consistent with the SOA Systinet installation time.
10102		FAILED	License key for a different product. SOA Systinet is unavailable until you enter a valid license key using the Setup Tool.
10103		FAILED	License key for a different version. SOA Systinet is unavailable until you enter a valid license key using the Setup Tool.
10104		FAILED	License expired on the specified date. Contact <SOA@hp.com> or your sales representative to obtain a new license.
10105		VALID	License due to expire on the specified date. Contact <SOA@hp.com> or your sales representative to obtain a new license.
10106		VALID	License seat assigned to the specified user.
10107		VALID	License seat removed from the specified user.
10111		VALID	Policy Manager is not enabled in the current license.
10112		VALID	The number of current users exceeds the current license limit. Contact <SOA@hp.com> or your sales representative to obtain a new license.
10113		VALID	The number of concurrent users is approaching the license limit. Contact <SOA@hp.com> or your sales representative to obtain a new license.

Table 7. `application.notification` **Events**

Event ID	Resource	Result	Description
10203		FAILED	Unsuccessful notification.

Table 8. `application.notification.email` **Events**

Event ID	Resource	Result	Description
10200		FAILED	E-mail delivery failure with failure details.
10201		OK	E-mail queued for delivery.
10202		OK	E-mail delivery success.

Table 9. `application.security.account` **Events**

Event ID	Resource	Result	Description
10300	Username	CREATED	Specified user account created.
10301	Username	FAILED	Specified user account creation failed.
10302	Username	DELETED	Specified user account deleted.
10303	Username	FAILURE	Specified user account deletion failed.

Table 10. `application.security.acl` **Events**

Event ID	Resource	Result	Description
10400	Resource ID	OK	ACL of specified resources changed.

Table 11. `application.security.ownership.retirement` **Events**

Event ID	Resource	Result	Description
10900	Retired User	OK	User retired and owned artifacts transferred to the specified user or group.

Table 12. `integration.discovery` **Events**

Event ID	Resource	Result	Description
11001	Artifact UUID	MARKED_GOVERNED	Specified artifact entered into governance.
11002	Artifact UUID	FAILED	Entry into governance failure.
11003	Artifact UUID	MARKED_INFRASTRUCTURE	Specified artifact marked as infrastructure.
11004	Artifact UUID	FAILED	Marking as infrastructure failure.
11005	Artifact UUID	MARKED_ROGUE	Specified artifact marked as rogue.
11006	Artifact UUID	FAILED	Marking as rogue failure.
11007	Server UUID	DISCOVERY_STARTED	BAC Discovery started for the specified server.
11008	Server UUID	DISCOVERY_FINISHED	BAC Discovery complete for the specified server with a link to the report.
11009	Server UUID	FAILED	BAC Discovery failed with a link to the report.
11010	Artifact UUID	ARTIFACT_DISCOVERED	The specified artifact was discovered.
11011	Artifact UUID	FAILED	Artifact discovery failure.

Table 13. `integration.export` **Events**

Event ID	Resource	Result	Description
11201	Server Artifact Name	EXPORT_STARTED	Export to the specified server started.
11202	Server Artifact Name	EXPORT_FINISHED	Export to the specified server complete.
11203	Server Artifact Name	FAILED	Export to the specified server failed.
11204	Artifact UUID	ARTIFACT_EXPORTED	Specified artifact exported.
11205	Artifact UUID	FAILED	Specified artifact export failure.

Table 14. `integration.synchronization` **Events**

Event ID	Resource	Result	Description
11101	Artifact UUID	ARTIFACT_UPDATED	Specified artifact updated during synchronization.
11102	Artifact UUID	FAILED	Artifact synchronization failure.

Table 15. `lifecycle.api` **Events**

Event ID	Resource	Result	Description
15001	Artifact UUID	OK or FAILED	Starting governance for the specified artifact.
15002	Artifact UUID	OK or FAILED	Leaving governance for the specified artifact.
15003	Process UUID	OK or FAILED	Governance process automatic action execution.

Table 16. `lifecycle.approval` **Events**

Event ID	Resource	Result	Description
15701	Artifact UUID	OK or FAILED	Promotion started for the specified artifact.
15702	Artifact UUID	OK	Promotion complete for the specified artifact.
15703	Artifact UUID	OK	Promotion failed for the specified artifact.
15704	Artifact UUID	OK	Promotion cancelled for the specified artifact.
15705	Approval UUID	OK or FAILED	Promotion request approval.
15706	Approval UUID	OK or FAILED	Promotion request denial.

Table 17. `lifecycle.process` **Events**

Event ID	Resource	Result	Description
15501	Process UUID	OK or FAILED	Governance process creation.
15502	Process UUID	OK or FAILED	Governance process modification.
15503	Process UUID	OK or FAILED	Governance process deletion.

Table 18. `platform.contract-manager` **Events**

Event ID	Resource	Result	Description
2	Resource Path	fail.denied or success	Contract request creation.
3	Resource Path	success	Contract request deletion.
4	Resource Path	fail.denied or fail or success	Contract request accepted.
5	Resource Path	success or fail.denied	Contract request rejection.
7	Resource Path	fail.denied	Contract creation failure.
9	Resource Path	fail.denied or fail or success	Contract revoked.
10	Resource Path	fail or success	Contract invalidation.

Table 19. `platform.repository.api.legacy` **Events**

Category	Event ID	Resource	Result	Description
.artifactCreate	12200	Artifact Path	FAILED or OK	Artifact creation.
.artifactDelete	12202	Artifact Path	FAILED or OK	Artifact deletion.
.artifactPurge	12205	Artifact Path	FAILED or OK	Artifact purging.
.artifactRemove	12203	Artifact Path	FAILED or OK	Artifact removal.
.artifactSetSecurityproperties	12206	Artifact Path	FAILED or OK	Artifact security modifications.
.artifactUndelete	12204	Artifact Path	FAILED or OK	Artifact undeletion.
.artifactUpdate	12201	Artifact Path	FAILED or OK	Artifact modification.
.collectionCreate	12207	Artifact Path	FAILED or OK	Artifact collection creation.
.collectionDelete	12208	Artifact Path	FAILED or OK	Artifact collection deletion.
.collectionPurge	12209	Artifact Path	FAILED or OK	Artifact collection purging.
.collectionSetSecurityproperties	12211	Artifact Path	FAILED or OK	Artifact collection security modifications.
.collectionUpdate	12210	Artifact Path	FAILED or OK	Artifact collection modification.

Table 20. `platform.rest.atom` **Events**

Event ID	Resource	Result	Description
12701		GET	HTTP GET method invoked by the specified URI.

Table 21. `platform.rest.legacy` **Events**

Event ID	Resource	Result	Description
12501	Request URI	GET	HTTP GET method invoked.
12502	Request URI	POST	HTTP POST method invoked.
12503	Request URI	PUT	HTTP PUT method invoked.
12504	Request URI	DELETE	HTTP DELETE method invoked.
12505	Request URI	HEAD	HTTP HEAD method invoked.

Table 22. `policy-manager.validation` **Events**

Event ID	Resource	Result	Description
13001		OK or FAILED	Validation result deletion.
13002	Validation Result ID	OK or FAILED	Marking a manual assertion as `PASSED`.
13003	Validation Result ID	OK or FAILED	Marking a manual assertion as `FAILED`.
13004	Validation Requests	OK or FAILED	Starting policy validation.
13005		OK or FAILED	Starting scheduled policy validation.
13006	Execution ID	OK or FAILED	Validation cancellation.
13007		OK or FAILED	Starting JMS validation.
13008		OK or FAILED	JMS validation completion.

Table 23. `repository.api.new` **Events**

Category	Event ID	Resource	Result	Description
.artifactCreate	12000	Artifact UUID	FAILED or OK	Artifact creation.
.artifactDelete	12001	Artifact UUID	FAILED or OK	Artifact deletion.
.artifactPurge	12002	Artifact UUID	FAILED or OK	Artifact purging.
.artifactUpdate	12003	Artifact UUID	FAILED or OK	Artifact modification.
.artifactUndelete	12004	Artifact UUID	FAILED or OK	Artifact undeletion.
.changeOwner	12005	Artifact UUIDs	BULK_OPERATION_PARTIALLY_FAILED or FAILED or OK	Changed ownership of the specified artifacts to the specified user.
	12006	Username	FAILED, OK, or FAILED_ACCESS_DENIED	Changed ownership of artifacts owned by the specified user to the new user.

Table 24. `webui.authorization` **Events**

Event ID	Resource	Result	Description
1		login	User sign-in.
2		logout	User sign-out.

Configuring the Audit Log for JBoss

In JBoss it is possible to restrict the categories that SOA Systinet writes to the audit log and also configure the event details.

To configure the audit log categories in JBoss

1 Open `JBOSS_HOME/server/CONFIG_HOME/log/jboss-log4j.xml` with a text editor.

The default configuration is the following:

```
<!-- ============================== -->
<!-- HP SOA Systinet Audit category -->
<!-- ============================== -->
<category name="com.hp.systinet.audit.event" additivity="true">
  <priority value="INFO"/>
  <appender-ref ref="Systinet_AUDIT"/>
</category>
```

2 Make the logging more specific by changing the category.

For example for `lifecycle.api` category events:

```
<category name="com.hp.systinet.audit.event.lifecycle.api" additivity="true">
  <priority value="INFO"/>
  <appender-ref ref="Systinet_AUDIT"/>
</category>
```

3 Add a separate category section for each specific category that you want to log.

4 Save `JBOSS_HOME/server/CONFIG_HOME/log/jboss-log4j.xml`.

To configure the audit event content in JBoss

1 Open `JBOSS_HOME/server/CONFIG_HOME/log/jboss-log4j.xml` with a text editor.

The default configuration is the following:

```
<!-- ======================== -->
<!-- HP SOA Systinet Audit Appender -->
<!-- ======================== -->
<appender class="org.apache.log4j.RollingFileAppender" name="Systinet_AUDIT">
  <param name="File" value="${jboss.server.log.dir}/systinet_audit.log"/>
  <param value="10000KB" name="MaxFileSize"/>
  <param value="10" name="MaxBackupIndex"/>
  <layout class="org.apache.log4j.PatternLayout">
    <!--" is the same as " (")-->
    <param name="ConversionPattern" value=""%d",%X{audit.category}:%X{audit.eventId},
        %X{audit.result},%X{audit.ctxId},"%X{audit.actor}","%X{audit.resource}",%X{audit.detail}%n"/>

  </layout>
</appender>
```

2 Rearrange, remove, and add to the audit event layout conversion pattern as required.

The default configuration contains all the available audit content.

3 Save `JBOSS_HOME/server/CONFIG_HOME/log/jboss-log4j.xml`.

Data Migration

SOA Systinet 3.10 is backwards compatible with SOA Systinet 3.00 data. You can import data images from SOA Systinet 3.00 into SOA Systinet 3.10.

To migrate data from SOA Systinet 3.00 to 3.10:

1 In SOA Systinet 3.00, execute the export command:

3.00_SOA_HOME/bin/export --image *IMAGE*

For more details, see "Export Tool" in the *HP SOA Systinet Administrator Guide 3.00*

2 In SOA Systinet 3.10, execute the import command:

3.10_SOA_HOME/bin/import --image *IMAGE*

For more details, see Import Tool on page 85.

You can also migrate data and configuration options from SOA Systinet 2.52 to 3.10.

To migrate policy data you must apply a patch to SOA Systinet 2.52.

The patch is distributed with SOA Systinet 3.10.

Copy `3.10_SOA_HOME/util/2.52/updates/hp-soa-systinet-policymgr-2.52-update-04.jar` to `2.52_POLICY_HOME/updates` and then execute the command:

2.52_POLICY_HOME/bin/updatetool -i

The patch installs an export tool for policy data.

To migrate data from SOA Systinet 2.52 to 3.10:

1 In SOA Systinet 2.52, execute the platform configuration export command:

PLATFORM_HOME/bin/configurationexport ***configimage***

2 In SOA Systinet 2.52, execute the platform data export command:

PLATFORM_HOME/bin/repositoryexport -i ***platformimage***

3 In SOA Systinet 2.52, execute the SSO export command:

SSO_HOME/bin/export -i ***ssoimage***

4 In SOA Systinet 2.52, execute the reporting export command:

REPORTING_HOME/bin/importexport -e ***reportimage***

5 If you use Policy Manager, in SOA Systinet 2.52, execute the policy export command:

POLICY_HOME/bin/export ***policyimage***

6 In SOA Systinet 3.10, execute the data migration command:

SOA_HOME/bin/migrate --image ***image*** **[OPTIONS]**

Execute **migrate --help** to view the available options for the migrate tool.

If you use password encryption, use the passphrase setup up for SOA Systinet 3.10 if it is different from that of SOA Systinet 2.52.

Use the following options, as required:

- **--252platformInstallDir** ***2.52_SOA_HOME***
- **--252configurationImage** ***configimage***

- **--252platformImage** ***platformimage***
- **--252ssoImage** ***ssoimage***
- **--252reportingImage** ***reportimage***
- **--252pmImage** ***policyimage***

If you use zipped images, they may not contain any intermediate folders. The structure of each zip must be identical to the structure of the image created by the SOA Systinet 2.52 export tools.

The migrate tool creates an image folder matching the output of the export tool.

For details, see Export Tool on page 83.

7 In SOA Systinet 3.10, execute the import tool:

SOA_HOME/bin/import --image ***image***

For more details, see Import Tool on page 85.

Configuration Procedures

System configuration is maintained using the tools described in Chapter 4, Administration Utilities. These tools enable you to reset the parameters set during installation. They also enable you to make additional changes to your installation.

This section describes the processes executed by the provided tools that are not fully described as part of the installation process:

- Applying Extensions on page 58
- Applying Updates on page 61
- Setting Up LDAP Integration on page 63
- Setting Up Siteminder Integration on page 63

- Redeploying the EAR File on page 65
- Changing the System Configuration on page 66

Applying Extensions

You can extend SOA Systinet by adding libraries or JSPs to the deployed EAR files, by modifying the data model, by configuring the appearance of the UI, and by importing prepackaged data.

Extensions to SOA Systinet come from the following sources:

- **Customization Editor**

  Typical extensions created by Customization Editor contain modifications to the data model and artifact appearance, and possibly data required by the customization (taxonomies). They may also contain new web components, which may include custom JSP and Java code.

- **Assertion Editor, Report Editor, and Taxonomy Editor**

  These extensions contain assertion, reporting, and taxonomy data only. They do not involve changes to the data model.

The Setup Tool opens the EAR files, applies the extensions, and then repacks the EAR files.

Apply extensions according to one of the following scenarios:

- Single-Step Scenario on page 58

  The Setup Tool performs all the processes involved in applying extensions, including any database alterations, as a single step.

- Decoupled DB Scenario on page 60

  Database SQL scripts are run manually. The Setup Tool performs the other processes as individual steps that are executable on demand. This scenario is useful in organizations where the user applying extensions does not have the right to alter the database, which is done by a database administrator.

Single-Step Scenario

Follow this scenario if you have permission to alter the database used for SOA Systinet.

To apply extensions to SOA Systinet in a single step:

1 Make sure that all extensions are in the following directory:

```
SOA_HOME/extensions
```

The Setup Tool automatically applies all extensions in that directory.

If you are applying extensions to another server, substitute the relevant home directory for `SOA_HOME`.

2 Stop the server.

3 Start the Setup Tool by executing the following command:

SOA_HOME/bin/setup.bat(sh)

4 Select the **Apply Extensions** scenario, and click **Next**.

The Setup Tool automatically validates the step by connecting to the server, copying the extensions, and merging the SDM configuration.

If you extension does not contain data model changes, select **Apply Extensions Don't Touch DB**.

5 Click **Next** for each of the validation steps and the setup execution.

This process takes some time.

6 Click **Finish** to end the process.

7 Deploy the EAR file:

- **JBoss**

  The Setup Tool deploys the EAR file automatically.

  If you need to deploy the EAR file to JBoss manually, see Redeploying the EAR File on page 65.

- **Other Application Servers**

  You must deploy the EAR file manually.

  For application server-specific details, see "Deploying the EAR File" in the *HP SOA Systinet Installation and Deployment Guide*.

8 Restart the server.

The Setup Tool normally applies ALTER scripts if database changes are required for an extension. If the ALTER script cannot be used, then a DROP and CREATE process may be used instead. In these cases, you must recreate indices on the database.

`SOA_HOME/log/setup.log` contains the following line in these cases:

```
Could not apply alteration scripts, application will continue with slower DB drop/create/restore
scenario. ... .
```

Decoupled DB Scenario

Follow this scenario if the user who applies extensions does not have permission to modify the database.

To apply extensions and modify the database separately:

1 Make sure that all extensions are in the following directory:

```
SOA_HOME/extensions
```

The Setup Tool automatically applies all extensions in that directory.

2 Stop the server.

3 Start the Setup Tool by executing the following command:

SOA_HOME/bin/setup -a.

4 Select the **Apply Extensions** scenario, and click **Next**.

5 Click **Next**, to execute the extension application, and exit the Setup Tool.

6 Provide the scripts from `SOA_HOME/sql` to the database administrator.

The database administrator can use `all.sql` to execute the scripts that drop and recreate the database schema.

7 Execute the Setup Tool in command-line mode to finish the extension application:

SOA_HOME/bin/setup -c

8 Redeploy the EAR file:

- **JBoss**

  The Setup Tool deploys the EAR file automatically.

  If you need to deploy the EAR file to JBoss manually, see Redeploying the EAR File on page 65.

- **Other Application Servers**

  You must deploy the EAR file manually.

  For application server-specific details, see "Deploying the EAR File" in the *HP SOA Systinet Installation and Deployment Guide*.

Applying Updates

Product updates from HP Software are applied to the using the Setup Tool. For more details see Chapter 3, Setup Tool.

To apply updates:

1 Copy the updates to the `SOA_HOME/updates` folder.

2 Stop the application server.

3 Start the Setup Tool by executing **SOA_HOME/bin/setup.bat(sh)**.

4 Choose the **Apply Updates** scenario, and click **Next**.

5 Use **Add** to select the updates to apply, and then click **Next**.

If you applied Step 1, this is not required.

The Setup Tool validates the updates.

6 Click **Next** to apply the updates.

7 Click **Next, and then** click **Finish** to close the Setup Tool or **Setup Again** to restart the Setup Tool.

8 Reapply any required extensions, using the procedure described in Applying Extensions on page 58.

9 Redeploy the EAR file as described in:

- **JBoss**

  Follow the procedure described in Redeploying the EAR File on page 65.

- **Other Application Servers**

  You must deploy the EAR file manually.

  For application server-specific details, see "Deploying the EAR File" in the *HP SOA Systinet Installation and Deployment Guide*.

10 Restart the application server.

Setting Up LDAP Integration

The Setup Tool enables you to integrate LDAP accounts and groups after SOA Systinet installation.

To integrate LDAP using the Setup Tool:

1. Execute **SOA_HOME/bin/setup**, and click **Next**.
2. In the Select Scenarios page, select **Advanced**, and click **Next**.
3. In the Custom Scenario Selection page, select **User Management**, and click **Next**.
4. In the Account Provider Selection page, select **LDAP**, and click **Next**.
5. The Setup Tool continues with the LDAP setup pages identical to the GUI Installation wizard.

   For details, see "LDAP Options" in the *HP SOA Systinet Installation and Deployment Guide*.
6. Do one of the following:
   - Click **Finish** to exit the Setup Tool
   - Click **Setup Again** to perform another task using the Setup Tool.

SOA Systinet logins are case-sensitive by default. If want the login name to be case insensitive you must add the following property to `SOA_HOME/conf/setup/configuration.properties`:

```
shared.um.account.caseInsensitiveLoginName=true
```

You must also ensure that the application server uses matching case-sensitive or -insensitive authentication as well.

Setting Up Siteminder Integration

You can configure SOA Systinet to accept authentication headers or cookies added to HTTP requests after a successful authentication performed by an authentication proxy. The changes affect the configuration properties stored in the SOA Systinet database and the application EAR file.

To integrate Siteminder using the Setup Tool:

1 Execute **SOA_HOME/bin/setup**, and click **Next**.

2 In the Select Scenarios page, select **Advanced**, and click **Next**.

3 In the Custom Scenario Selection page, select **Siteminder Setup**, and click **Next**.

4 In the Account Provider Selection page, select **LDAP**, and click **Next**.

5 In the Siteminder Setup page, select **Enable Siteminder Integration** and then click **Next**.

If you are disabling Siteminder integration, deselect **Enable Siteminder Integration** and click **Next**. Continue with Step 8.

6 Do one of the following:

- Select **Use Cookies** to accept authentication cookies.
- Select **Use Headers** if the user login name is sent in the authentication header.

7 Set the Login Header or Cookie Name and then click **Next**.

8 After deployment validation, click **Next** to start the setup.

The Setup Tool updates your deployment and configuration.

9 After setup completes, click **Next** and do one of the following:

- Click **Finish** to exit the Setup Tool
- Click **Setup Again** to perform another task using the Setup Tool.

10 Redeploy the EAR file as described in:

- **JBoss**

Follow the procedure described in Redeploying the EAR File on page 65.

- **Other Application Servers**

  You must deploy the EAR file manually.

  For application server-specific details, see "Deploying the EAR File" in the *HP SOA Systinet Installation and Deployment Guide*.

11 Restart the application server.

Redeploying the EAR File

After using the Setup Tool to apply extensions or updates, you must redeploy the EAR file to the application server. For JBoss, you can do this using the Setup Tool.

For other application servers, follow the EAR deployment procedures described in the "Deploying the EAR File" in the *HP SOA Systinet Installation and Deployment Guide*.

To redeploy the EAR file to JBoss:

1 Stop the application server.

2 Start the Setup Tool by executing the following command:

SOA_HOME/bin/setup.bat(sh).

3 Select the **Advanced** scenario, and click **Next**.

4 Scroll down, select **Deployment**, and then click **Next**.

When the Setup Tool validates the existence of the JBoss Deployment folder, click **Next**.

5 Click **Finish** to close the Setup Tool.

6 Restart the application server.

Changing the System Configuration

The system configuration can be accessed and manually edited using the Export and Import Tools.

The following sections describe specific procedures for changing the configuration:

Configuring the Browse History

The SOA Systinet UI stores the browsing history on the server. Different branches of the history are also stored when a user opens a new window or a new tab in the browser. There are certain preset limits to prevent memory overflow.

The default limits are 10 history pages and 4 branches.

The history default is effectively 5 pages because most navigation clicks are interpreted as one post and a subsequent get.

To change the browsing history limits:

1. Export the SOA Systinet configuration with the command:

   SOA_HOME/bin/export --image *IMAGE* --components configuration

2. Open *IMAGE*`/configuration/configuration.properties` in a text editor

3 Add the following properties (for example, history depth 30 (15 effective steps) and 6 concurrent windows):

- `platform.webui.max.branch.depth=30`
- `platform.webui.max.branch.count=6`

4 Save `configuration.properties`.

5 Upload the new configuration with:

SOA_HOME/bin/import --image *image* --components configuration

6 Restart the application server.

Configuring the Default ACLs

The repository enables you to configure the default ACL to be set for newly created artifacts.

To change default ACLs:

1 Export the SOA Systinet configuration with the command:

SOA_HOME/bin/export --image *IMAGE* --components security

2 Open *IMAGE*`/security/defaultAcl.xml` in a text editor.

3 Make the changes you require.

For more details about the default ACL, see "Default ACL Configuration" in the *HP SOA Systinet Reference Guide*.

4 Save `defaultAcl.xml`.

5 Upload the new configuration with:

SOA_HOME/bin/import --image *image* --components security

6 Restart the application server.

Configuring Consumer and Provider Artifacts

By default, only a limited set of artifact types are defined as providers and consumers in SOA Systinet. You can change the configuration to add or remove provider and consumer artifact types.

To add a provider or consumer artifact type, you must add properties to the artifact type in the SDM configuration.

Use HP SOA Systinet Customization Editor to add the *consumerProperties* or *providerProperties* property group to the artifact type, and then build and import the extension to SOA Systinet.

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

To change the consumer or provider artifacts:

1. Export the SOA Systinet configuration with the command:

   SOA_HOME/bin/export --image *IMAGE* --components configuration

2. Open *IMAGE*/configuration/configuration.properties in a text editor.

3. Edit the following properties:

   - platform.cm.providers
   - platform.cm.consumers

   Each property is a comma-separated list of artifact localNames (SDM names).

   For details of the localnames for artifact types, see "Artifact Types" in the *HP SOA Systinet Reference Guide*.

You can use the localName of an abstract artifact type to enable all the artifact types that inherit its properties. For example, using implementationArtifact enables webArtifact, soapService, and wsdlService.

For details of the artifact hierarchy, see "Artifacts Taxonomy" in the *HP SOA Systinet Reference Guide*.

4 You can also restrict provider-consumer relationships.

Add the following properties as required:

- `platform.cm.providers.of.`*`consumer`*
- `platform.cm.consumers.of.`*`provider`*

Each property specifies a comma separated list of artifact localnames (SDM names) for a specific provider or consumer artifact.

Adding one of these properties, restricts the provision or consumption of the artifact type to the artifacts stated by the property.

5 Save `configuration.properties`.

6 Upload the new configuration with:

SOA_HOME/bin/import --image *`image`* --components configuration

7 Restart the application server.

Configuring the Compliance Status Cache

When you request the compliance status of an artifact, SOA Systinet either opens the latest version of the report or generates a new one.

Whether SOA Systinet opens the latest version or generates a new one is determined by a caching property in the configuration, which by default is set to one hour.

To change the compliance status cache:

1 Export the SOA Systinet configuration with the command:

SOA_HOME/bin/export --image *IMAGE* --components configuration

2 Open *IMAGE*/configuration/configuration.properties in a text editor.

3 Add the following element:

```
policymgr.reporting.compliance.caching=TIME
```

Replace *TIME* with one of the following values:

- DAY
- HOUR (default value)
- MINUTE
- NONE

  This always generates a new compliance status report.

4 Save configuration.properties.

5 Upload the new configuration with:

SOA_HOME/bin/import --image *image* --components configuration

6 Restart the application server.

Disabling the Addition of % to Search Terms

By default, SOA Systinet appends a % to all full text search terms.

If you want to use full text search but do not want this functionality, you can disable the addition of %.

To disable the addition of %:

1 Export the SOA Systinet configuration with the command:

SOA_HOME/bin/export --image *IMAGE* --components configuration

2 Open *IMAGE*/configuration/configuration.properties in a text editor

3 Modify the following property:

```
shared.db.fulltextsearch.appendpercentage=false
```

4 Save configuration.properties.

5 Upload the new configuration with:

SOA_HOME/bin/import --image *image* --components configuration

6 Restart the application server.

Configuring Archive Publishing

The publishing component enables you to publish archives containing service definition content. For details, see "Publishing Services" in the *HP SOA Systinet User Guide*.

By default, SOA Systinet extracts and processes of the following archive types:

- ZIP
- JAR
- WAR
- EAR
- BPR

You can configure which artifact types SOA Systinet extracts and processes. Any archive types not supported are published as documentation artifacts with attached data content.

To change the supported archive types:

1 Export the SOA Systinet configuration with the command:

SOA_HOME/bin/export --image *IMAGE* --components configuration

2 Open *IMAGE*/configuration/configuration.properties in a text editor.

3 Edit the following property:

- platform.publishing.ui.zipArchiveExtensions=zip,jar,ear,war,bpr

The property is a comma-separated list of archive types.

Remove and add archive extension types as required.

Archive extension types must conform to the ZIP format.

4 Save configuration.properties.

5 Upload the new configuration with:

SOA_HOME/bin/import --image *image* --components configuration

6 Restart the application server.

Configuring the Default BAC Reporting Period

A service shared with Business Availability Center (BAC) shows performance and availability statistics generated by BAC in its detail page.

By default, the statistics are displayed for the past week.

To change the default BAC reporting period:

1 Export the SOA Systinet configuration with the command:

SOA_HOME/bin/export --image *IMAGE* --components configuration

2 Open *IMAGE*/configuration/configuration.properties in a text editor.

3 Modify the following element:

`platform.integration.bac.defaultDataRange=`*`TIME`*

Replace *`TIME`* with one of the following values:

- pastHour
- pastDay
- pastWeek (default value)
- pastMonth
- pastQuarter
- pastYear

4 Save `configuration.properties`.

5 Upload the new configuration with:

SOA_HOME/bin/import --image *`image`* --components configuration

6 Restart the application server.

3 Setup Tool

Included with SOA Systinet is the Setup Tool. You can use it for the following functions, which you select as **Scenarios** when running the tool.

To access the Setup Tool user interface, execute the following command:

SOA_HOME/bin/setup

The Setup GUI opens at the Welcome screen.

Click **Next** to be presented a set of scenarios, as described in the following sections:

- Default Setup Tool Settings on page 76
- Changing the License Key on page 77
- Applying Extensions on page 58
- Updating SOA Systinet on page 77
- Advanced Setup Tool Options on page 78

The Setup Tool can also be used in command line mode.

For details, see Setup Tool Command-Line Options on page 78.

By default, the Setup Tool does not allow you to import data or apply extensions while there is a server running in order to protect data consistency. In some environments (for example, behind a load balancer proxy or using Siteminder) there is always something running at the server endpoint.

To enable the Setup Tool in these environments set the following property in `SOA_HOME/conf/setup/configuration.properties`:

```
install.ignore.running.platform=true
```

Alternatively, execute the Setup Tool with the following command option:

-Dinstall.ignore.running.platform=true

Default Setup Tool Settings

The default use of the Setup Tool is to change the configuration of SOA Systinet setup during initial installation.

In the Scenario Selection page, select **Default**, and then click **Next.**

The individual setup steps match the GUI Installation procedure described in "Using the GUI Installer" in the *HP SOA Systinet Installation and Deployment Guide*, starting with the Password Encryption step and with the following additions:

- **Configure Database**

  Select this additional option in the Database Setup Operations page to connect to a alternative database that is setup for SOA Systinet.

  The options in the Connection Properties page for the **Configure Database** operation are the same as for the **Create Schema** operation.

  For details, see "Database Installation Parameters" in the *HP SOA Systinet Installation and Deployment Guide*.

- **Configuration Table Management**

  Use the options in the additional Configuration Table Management page to control the configuration table during setup to do one of the following:

  - Select **Create** to create a default configuration table if one does not exist.
  - Select **Drop** to delete the existing configuration table and all data.
  - Select **Leave** to keep the current configuration table.

- **Setup Completion**

  At the end of the default scenario do one of the following:

  - Click **Setup Again** to return to the Scenario Selection page.
  - Click **Finish** to exit the Setup Tool.

Changing the License Key

The Setup Tool enables you to change the SOA Systinet license.

To change the license key with the Setup Tool:

1. In the Scenario Selection page, select **Change License Key**, and then click **Next.**.

   The License Information page opens.

2. In the License Information page, do one of the following:

   - Select **Install a 60 day evaluation license**.
   - Select **Enter license details**, and input the license details provided by your sales representative.

   Click **Next**.

3. Click **Next** through each confirmation and progress page, and when the setup is complete, do one of the following:

   - Click **Setup Again** to return to the Scenario Selection page.
   - Click **Finish** to exit the Setup Tool.

Updating SOA Systinet

The Setup Tool enables you to install updates to SOA Systinet, which are downloaded or copied to the `SOA_HOME/updates` directory.

For details, see Applying Updates on page 61.

If the Setup Tool is unavailable you can use the Update Tool instead.

For details, see Update Management Tool on page 90.

Advanced Setup Tool Options

The Advanced scenario enables you to select specific parts of the configuration procedure to suit the needs of a specific task.

To select specific configuration processes:

- In the Scenario Selection page, select **Advanced**, and then click **Next**.

  The Custom Scenario Selection page opens and enables you to select which parts of the configuration you want to execute.

Every part of the configuration process is listed as an individual step. The steps required for a particular process vary depending on what configuration you want to change.

Setup Tool Command-Line Options

The Setup Tool can also be executed as a command line tool.

The setup command is:

SOA_HOME/setup [OPTIONS]

The following options are available:

- **-h, --help [scenarios|steps]**

  Display the available options or list the available scenarios or steps in the console.

- **-c, --console**

  Execute the Setup Tool in console mode.

- **-a, --dbadmin-mode**

  Enables DB administrator mode. The setup stops after creating the DB scripts, allowing the administrator to execute them manually. Continue installation after script execution with **setup -c**.

- **-n, --scenarios** ***SCENARIO***

  Execute only the specified steps in the installation. Use **--help scenarios** to view a list of available scenarios.

- **-p, --steps** ***[comma separated list of steps]***

  Execute only the specified steps in the installation. Use **--help steps** to view a list of available steps.

- **-u, --use-config** ***FILE***

  Use the properties in the specified file to override the default or current configuration properties.

- **--passphrase** ***PASSPHRASE***

  If password encryption is enabled, specify the passphrase to use for encryption.

- **-d, --debug**

  Execute the setup in debug mode. All properties, SQL statements, and installation details are output to `SOA_HOME/log/setup.log`.

4 Administration Utilities

SOA Systinet administration utilities consist of command-line tools located in the `bin` directory of the SOA Systinet installation.

The utilities are summarised in SOA Systinet Utilities on page 81.

This chapter describes the following utilities:

If passwords are encrypted, set the option `--passphrase` *`passphrase`* on the command-line when you launch any tool that requires authentication.

SOA Systinet Utilities

The SOA Systinet utilities are located in `SOA_HOME/bin`. These are either batch `BAT` files or shell `SH` scripts, depending on the server operating system.

If a utility is not in `SOA_HOME/bin`, a relative path is shown for the command in Table 25.

Table 25. Summary of SOA Systinet Admin Utilities

Command	Description
create	Creates a resource using the HTTP interface. For details, see "Proprietary REST Interface" in the *HP SOA Systinet Developer Guide*.
delete	Deletes a specified resource using the HTTP interface and also supports the UNDELETE and PURGE operations. For details, see "Proprietary REST Interface" in the *HP SOA Systinet Developer Guide*.
env	A script used by other SOA Systinet tools to set system variables. Do not execute this script directly.
env-jboss	Called by serverstart to set system variables for the application server. Do not execute this script directly.
export	Creates a data image for specified components of SOA Systinet. For details, see Export Tool on page 83.
get	Gets a resource using the HTTP interface with an option to save it to a specified file. Supports the EXIST operation. For details, see "Proprietary REST Interface" in the *HP SOA Systinet Developer Guide*.
import	Imports a data image for specified components of SOA Systinet. For details, see Import Tool on page 85.
migrate	Converts an image of the repository data from SOA Systinet 2.52 to an image compatible with this version. For details, see Data Migration on page 55.
reset	Resets the data for specified components of SOA Systinet. For details, see Reset Tool on page 88.
../lib/sdm/bin/sdm2dbmap	Creates a report of the relationship between the SDM structure and the database tables. For details, see SDM to Database Mapping Tool on page 89.
serverstart	Calls env-jboss to set critical system variables for JBoss, and then starts the platform application server. For other application servers, use the server start functionality in the application server.
serverstop	Stops the platform application server for JBoss. For other application servers, use the server stop functionality in the application server.
setup	Starts the Setup Tool to reconfigure the platform server. For details, see Chapter 3, Setup Tool. Use `--help` to view the available options.

Command	Description
ssltool	Configures and views your SSL configuration. For details, see SSL Tool on page 89.
update	Updates a specified resource using the HTTP interface. For details, see "Proprietary REST Interface" in the *HP SOA Systinet Developer Guide*.
updatetool	Called by the Setup Tool to install updates to the product. Can be used by itself from the command line. For details, see Update Management Tool on page 90.

If a command requires arguments, running it without arguments displays a help screen, unless otherwise stated.

Export Tool

The **export** command enables you to export the SOA Systinet configuration and data in the database to an image, and then import that data at a later date.

The syntax for export is:

export --image *IMAGE_NAME* [OPTIONS]

The Export Tool includes the following options:

`--image IMAGE_NAME`	The path to the directory where the image is stored.

`--components [COMPONENT]`	The following component options are available: • `all` This is also the default if you omit `--components`. Exports all the configurations and data. • `configuration` The SOA Systinet configuration data. • `content` All SOA Systinet data without the configuration and security data. • `security` The SOA Systinet security configuration.
`--quiet`	Execute the command without a confirmation request.
--executions-flat-limit *N*	Export execution reports in a flat layout with a limit of *N* reports/items.  By default, execution reports are exported in a flat layout up to a predefined number of reports and items. If the limit is exceeded a hashed layout is used instead to prevent potential excess directory errors. Use this command to define your own limit for flat layout exports.

 SOA Systinet must not be running when you execute these commands.

The export creates the directory specified by `IMAGE_NAME`, containing the following, depending on the component options used:

- `image.properties`

A file containing the export execution properties and a list of the data sets exported.

- `configuration`

  A directory containing the configuration data.

- `executions`

  A directory containing the execution report results of asynchronous tasks such as publishing, discovery, and bulk operations.

- `lifecycle`

  A directory containing the lifecycle data.

- `platform`

  A directory containing the service catalog data.

- `policyManager`

  A directory containing the policy data.

- `reporting`

  A directory containing the reporting definitions.

- `security`

  A directory containing the security configuration.

Import Tool

The **import** command enables you to import SOA Systinet configuration and data to the database from an image.

The syntax for import is:

import --image *`IMAGE_NAME`* [OPTIONS]

The Import Tool includes the following options:

`--image IMAGE_NAME`	The path to the directory where the image is stored.
`--components [COMPONENT]`	The following component options are available: • `all` This is also the default if you omit `--components`. Imports all the configurations and data. • `configuration` The SOA Systinet configuration data. • `content` All SOA Systinet data without the configuration and security data. • `security` The SOA Systinet security configuration.
`--quiet`	Execute the command without a confirmation request.
--reset	Executes the **reset** command first, with matching component options.
--platform-force	If an imported service catalog resource is already in the database, it is overwritten.
--platform-bootstrap	Import the service catalog data in bootstrap format.
--platform-update-blacklist	Append imported service catalog resources to the migration blacklist. Useful for bootstrap installation.
--platform-reset-blacklist	Save imported service catalog resources to the migration blacklist.
--platform-ignore-sdm-merge-warn	Continue service catalog data import if the SDM merge check only reports warnings.
--executions-force	If an imported execution report or item is already in the database, it is overwritten.

SOA Systinet must not be running when you execute these commands.

The import checks the directory specified by `IMAGE_NAME`, which contains the following depending on the image:

- `image.properties`

  A file containing the export execution properties and a list of the data sets exported.

- `configuration`

  A directory containing the configuration data.

- `executions`

  A directory containing the execution report results of asynchronous tasks such as publishing, discovery, and bulk operations.

- `lifecycle`

  A directory containing the lifecycle data.

- `platform`

  A directory containing the service catalog data.

- `policyManager`

  A directory containing the policy data.

- `reporting`

  A directory containing the reporting definitions.

- `security`

  A directory containing the security configuration.

If specific components are specified, the other component folders are ignored. If a specified component is not present, the import fails.

Reset Tool

The **reset** command enables you to reset the SOA Systinet data in the database and import the default image.

The syntax for reset is:

reset [OPTIONS]

The Reset Tool includes the following options:

`--components [COMPONENT]`	The following component options are available: • `all` This is also the default if you omit `--components`. Resets all the configurations and data. • `content` All SOA Systinet data without the configuration and security data. • `security` The SOA Systinet security configuration.
`--quiet`	Execute the command without a confirmation request.

SOA Systinet must not be running when you execute these commands.

SDM to Database Mapping Tool

Artifacts in SOA Systinet are stored in the form of XML documents. Their structure is defined by the SOA Definition Model (SDM). Artifacts are serialized into a database over a standard serialization layer. The serialization of data may differ from the norm, based on customer specific extensions or modifications.

The sdm2dbmap tool is a mapping tool that generates a report containing the mapping between your SDM and database tables.

To generate the report, execute the following command:

SOA_HOME/lib/sdm/bin/sdm2dbmap

The mapping report is output to the following file:

```
SOA_HOME/lib/sdm/build/sdm2dbmap.html
```

The output consists of the following parts:

- A top level 1:1 mapping between SDM artifacts and DB tables. Each artifact listed, maps directly to one table.
- A list of artifacts. Each artifact in the report maps each SDM property to a specific column in the table. There are also associated tables and foreign keys, joined using the primary key of the artifact table.
- A report documenting the DB schema for all database tables coming from the SDM. Tables with names ending in _Rev are used to store older revisions.

SSL Tool

The SSL Tool is a combined tool enabling you to setup client-side SSL for a deployed SOA Systinet application. It also enables you to print SSL server certificates, as well as to download the SSL server certificate chain.

The SSL Tool has the following basic actions:

- **serverInfo**

  Prints the SSL requirements for the specified HTTPS URL, and saves the server certificate to a file.

For details, see "Identifying Server SSL Requirements" in the *HP SOA Systinet Installation and Deployment Guide*.

- **keystoreEI**

  Exports or imports SSL certificates to the SOA Systinet database keystore or truststore.

  For details, see "SSL Server Certificate Trust" and "Importing Client Certificates for Two-Way SSL" in the *HP SOA Systinet Installation and Deployment Guide*.

- **customize**

  Change the effective SSL customization.

  For details, see "SSL Customization" in the *HP SOA Systinet Installation and Deployment Guide*.

The syntax for ssltool is:

SOA_HOME/bin/ssltool [ACTION] [options]

Execute **ssltool** with no action or options to view the help with some examples.

Execute **ssltool [ACTION] --help** to view specific help for each type of action with the available options.

Update Management Tool

For minor updates between major releases, the update management tool is available. It can display installed updates, install and uninstall updates, and check each new update to ensure that any prerequisite updates have already been installed.

This tool should only be used when the Setup Tool is unavailable or undesirable.

HP Software deliver updates for SOA Systinet in the form of `update-jar` files. Copy any updates to the `SOA_HOME/updates` folder.

To use the tool navigate, to `SOA_HOME/bin` and execute the following command, with one of the available options:

updatetool [OPTION]

Execute the Update Tool with no options to view the available updates.

The Reset Tool includes the following options:

`--help`	Displays the available options.
`-l, --list`	Lists the currently installed updates.
`-i, --install`	Installs the updates in the `updates` directory.
`-x, --installDontTouchExtensions`	Installs updates that do not require the reapplication of extensions.
`-u, --uninstall` *`UPDATE-NAME`*	Uninstalls the specified update. The specified update must be the latest installed. ➤ Extensions must be reapplied.
`--passphrase` *`PASSPHRASE`*	Specifies the passphrase to use if password encryption is enabled.

➤ Updates are installed to the local version of the EAR, located in the `SOA_HOME/deploy` directory. After the updates are installed, the tool informs you via the console that the EAR must be redeployed.

For some updates, extensions must be reapplied.

For details, see Applying Extensions on page 58.