HP SOA Systinet

Software Version: 3.00

Administrator Guide

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Third-Party Web Sites

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

Copyright Notices

Trademark Notices

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

Contents

About This Guide

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

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

How This Guide is Organized

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

  The principal tool for controlling 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.
`rmdir /S /Q System32`	User input.
`C:\System.ini`	Filenames, directory names, paths and package names.
`a.append(b);`	Program source code.
`server.Version`	Inline Java class name.
`getVersion()`	Inline Java method name.
Shift+N	Combination of keystrokes.
Service View	Label, word, or phrase in a GUI window, often clickable.
OK	Button in a user interface.
New→Service	Menu option.

Documentation Updates

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

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

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

http://h20230.www2.hp.com/selfsolve/manuals

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

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

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

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

Support

You can visit the HP Software Support Web site at:

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

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

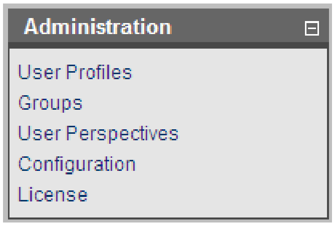
http://h20229.www2.hp.com/passport-registration.html

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 9
- Configuration Options on page 17
- Access Rights on page 18
- Integrating with Other Products on page 21
- Managing the License on page 34

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 a user first logs in to SOA Systinet, they are authenticated against the external user store and 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 13
- Managing User Perspectives on page 16

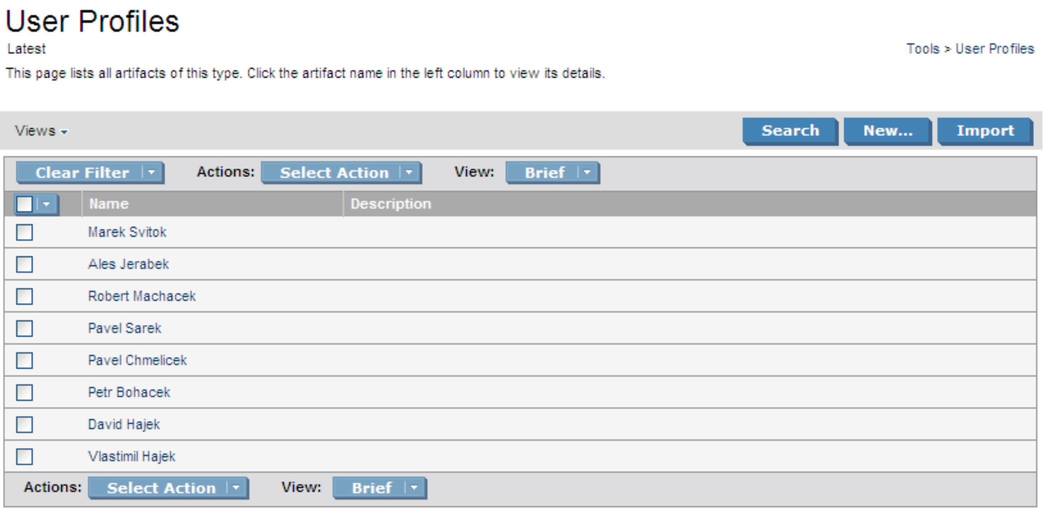
Additionally, the Administrator can manage permissions at the artifact and collection level using the Access Rights context action menu option available in artifact detail and browse views.

For details, see Access Rights on page 18.

Managing User Profiles

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

Figure 2. User Profiles



User Profiles

Latest

Tools > User Profiles

This page lists all artifacts of this type. Click the artifact name in the left column to view its details.

□	Name	Description
□	Marek Svitok	
□	Ales Jerabek	
□	Robert Machacek	
□	Pavel Sarek	
□	Pavel Chmelicek	
□	Petr Bohacek	
□	David Hajek	
□	Vlastimil Hajek	

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

For details, see Creating Profiles on page 11.

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 13.

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 represents two concepts:

- 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 tab Administrator section, click **User Profiles**.

   The User Profiles page opens.

2. Click **New**.

   The New User Profile page opens.

3. Input the profile details which are split into the following sections:

   - **Table 1. Basic Information**

Parameter	**Definition**
Name	The name of the user.
Description	A description for the new user.
Login Name	Input a profile id matching the user store id. Not required for a contact type profile. ➤ It is not possible to change the login name after profile creation.
Email	The email address for notifications.

   - **Table 2. Personal Information**

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

- 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.

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

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

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.

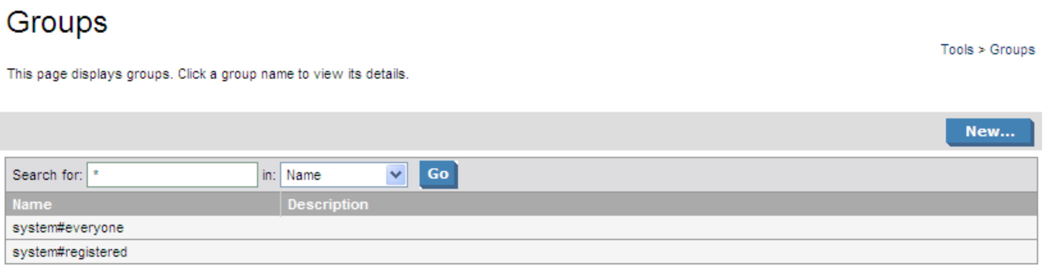
- The parameters, `loginname`, `name`, and `email` must be present.

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



Groups

This page displays groups. Click a group name to view its details.

Name	Description
system#everyone	
system#registered	

To use SOA Systinet to create or edit user groups in SOA Systinet, the appropriate option must be set, as described in Configuration Options on page 17.

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

For details, see Creating a User Group on page 14.

Click a group name to view its details and then **Edit** to change its details or membership.

For details, see Editing a User Group on page 16.

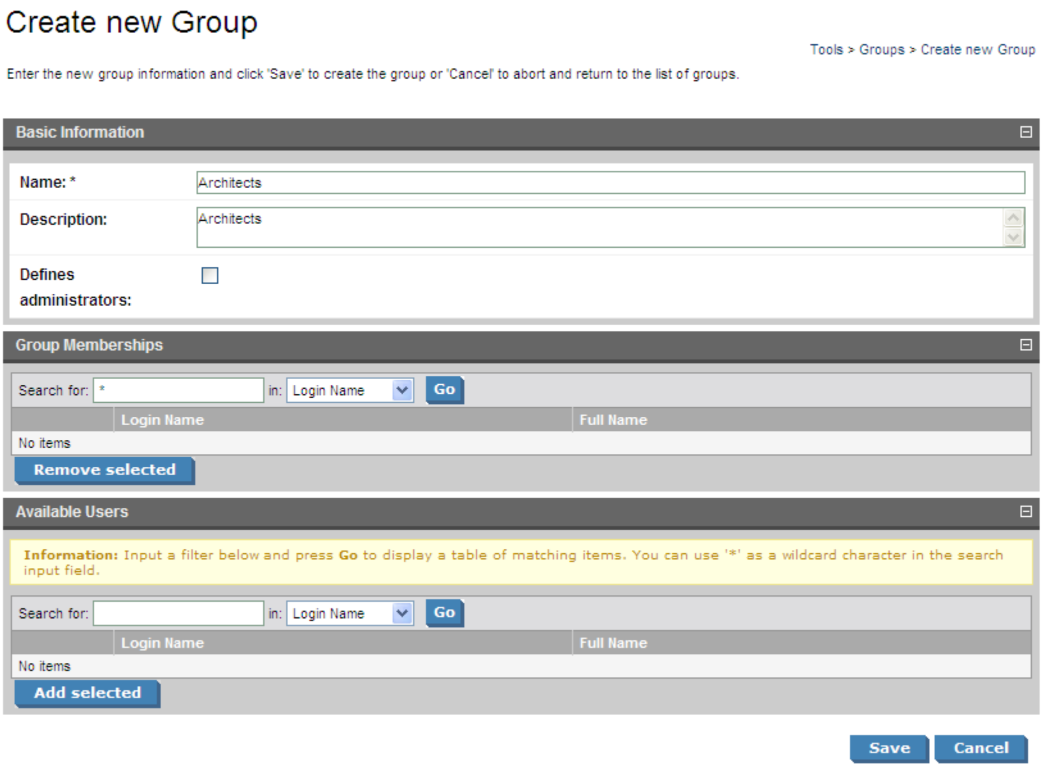
Creating a User Group

Ownership of artifacts and voting for lifecycle promotion approval can be delegated to groups instead of 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



Create new Group

Tools > Groups > Create new Group

Enter the new group information and click 'Save' to create the group or 'Cancel' to abort and return to the list of groups.

Basic Information

Name: * Architects

Description: Architects

Defines administrators: □

Group Memberships

Search for: * in: Login Name Go

	Login Name	Full Name
No items		

Remove selected

Available Users

Information: Input a filter below and press **Go** to display a table of matching items. You can use '*' as a wildcard character in the search input field.

Search for: in: Login Name Go

	Login Name	Full Name
No items		

Add selected

Save Cancel

2 Input the following parameters:

Parameter	**Definition**
Name	The name for the new user group.
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 due to 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. Click **Add** to add new groups or click the cross next to a group to remove it.
5. Click **Save** to confirm your changes.

Configuration Options

In the Tools menu Administration section, select **Configuration** to open a page enabling you to control some aspects of SOA Systinet.

- **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* .

- **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 13.

  > 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* .

  - **Java/JSSE default key/trust stores...** corresponds to **default**.
  - **Server certificates are always trusted...** corresponds to **skipped**.
  - **Database key/trust stores...** corresponds to **database**.
  - **Compositon of database and default...** corresponds to **composite**.

Access Rights

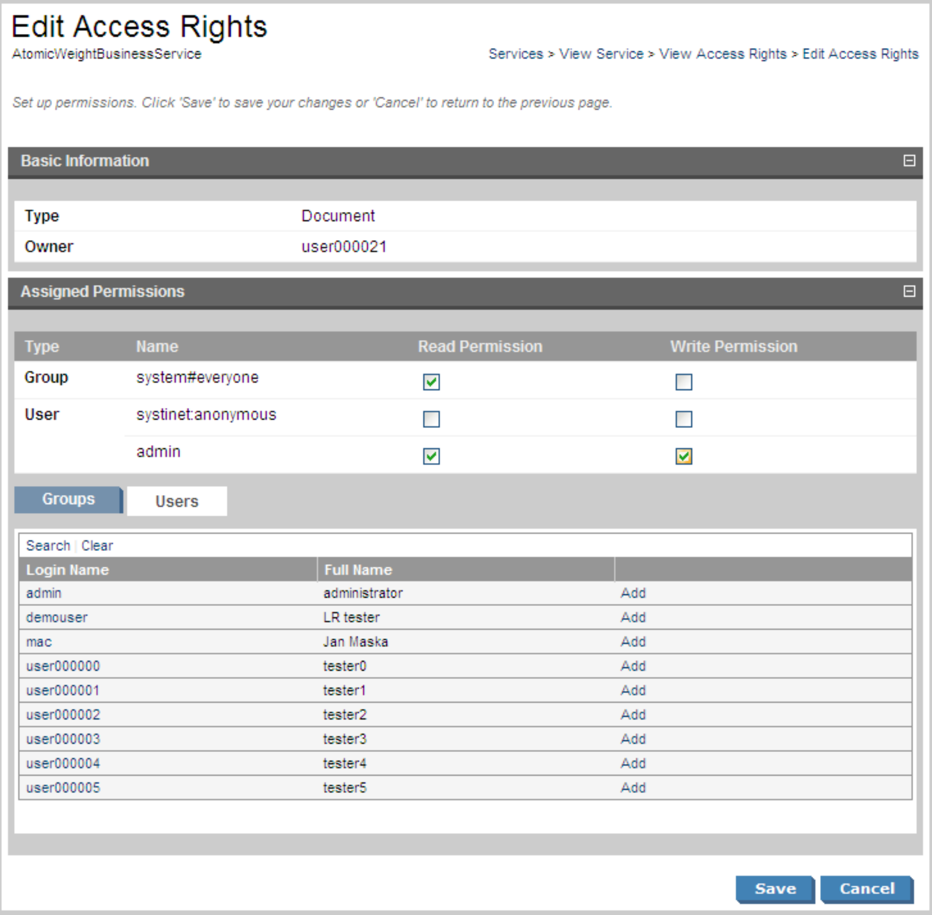
Access rights are read and write permissions. You can change the access rights for an artifact or a collection of artifacts. Changing access rights for a collection of artifacts does not change the access rights for individual artifacts in the collection.

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:



Edit Access Rights

AtomicWeightBusinessService

Services > View Service > View Access Rights > Edit Access Rights

Set up permissions. Click 'Save' to save your changes or 'Cancel' to return to the previous page.

Basic Information

Type	Document
Owner	user000021

Assigned Permissions

Type	Name	Read Permission	Write Permission
Group	system#everyone	☑	□
User	systinet:anonymous	□	□
	admin	☑	☑

Groups | Users

Search | Clear

Login Name	Full Name	
admin	administrator	Add
demouser	LR tester	Add
mac	Jan Maska	Add
user000000	tester0	Add
user000001	tester1	Add
user000002	tester2	Add
user000003	tester3	Add
user000004	tester4	Add
user000005	tester5	Add

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, de-select 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.
- Use **Add Group** and **Add User** to select the users and groups to add or remove.

4 Click **Save**.

For details about changing the default ACL, see Configuring the Default ACLs on page 49.

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 take advantage of 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 (BAC)** and **Universal Configuration Management Database (UCMDB)**

  Discover services stored in BAC/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 (SPE)**

  Use SPE to enforce company policy on run-time services.

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

- **HP Service Test Manager 9.3 (STM)**

  Use this component of HP Quality Center to track your service testing.

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

Each product requires some setup and configuration in SOA Systinet.

For details, see the following sections:

- Setting Up Registry Integration on page 22

- Setting Up BAC/UCMDB Integration on page 30
- Setting Up SOA Policy Enforcer Integration on page 32
- Setting Up STM Integration on page 33

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. Once 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 (see www.uddi.org [http://www.uddi.org]) defines interoperable standards for the exchange of data about web services, their interfaces, implementations, deployments and responsible contacts. A UDDI registry is an implementation of the UDDI specification, e.g. 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 - represents a business unit, company, department, etc. It contains company name(s), contacts and provided Business Services. It corresponds to Organizational Unit in the SOA Systinet SDM model.
- Business Service - represents a logical service. Business Service can not 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 - represents technical services. It includes information needed to create and run client applications. It corresponds to Endpoint in the SOA Systinet SDM model.
- 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:

- Creating a Registry Artifact on page 23
- Importing Registry Certificates on page 26
- Synchronizing Taxonomies on page 27

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:

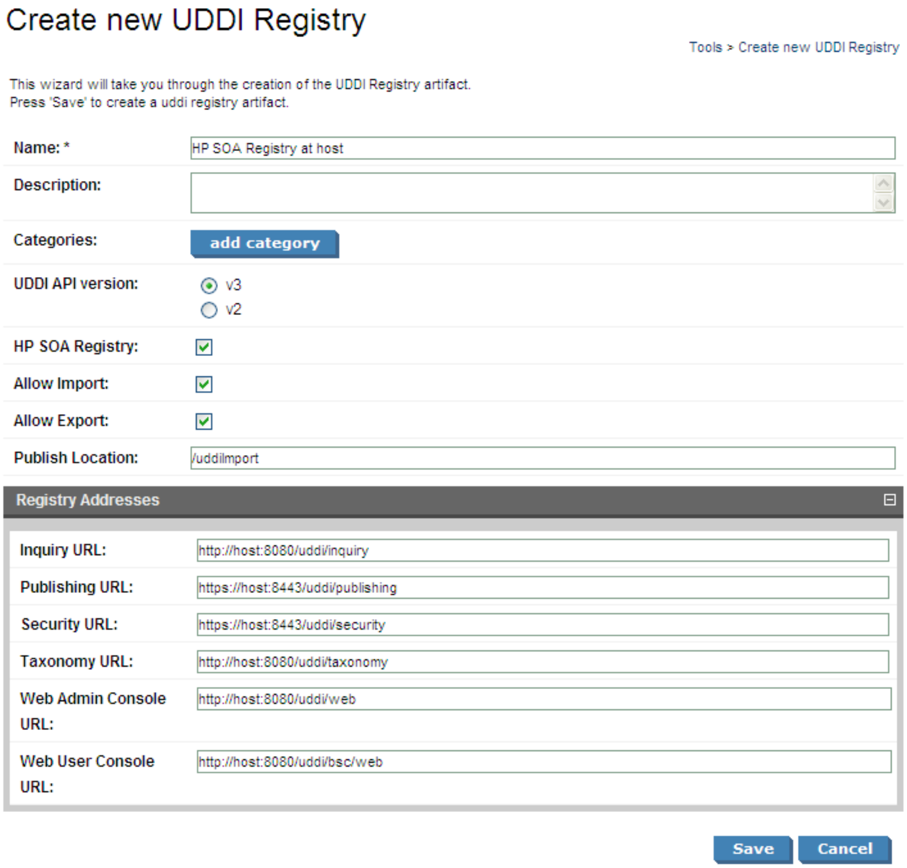
   - In the Tools tab Catalog Explorer, expand Integration and click **Registries** to open the Registries browse page, and then click **New**.
   - In the Tools menu Registry Content section, click **Import Registry Content** to open the Import Artifacts from Registry page, and then click **New Registry**.

   The Create New UDDI Registry page opens.

2 Input 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	Check the box if the registry is HP SOA Registry Foundation

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



Create new UDDI Registry

Tools > Create new UDDI Registry

This wizard will take you through the creation of the UDDI Registry artifact.
Press 'Save' to create a uddi registry artifact.

Name: *	HP SOA Registry at host
Description:	
Categories:	add category
UDDI API version:	● v3 ○ v2
HP SOA Registry:	☑
Allow Import:	☑
Allow Export:	☑
Publish Location:	/uddiImport

Registry Addresses

Inquiry URL:	http://host:8080/uddi/inquiry
Publishing URL:	https://host:8443/uddi/publishing
Security URL:	https://host:8443/uddi/security
Taxonomy URL:	http://host:8080/uddi/taxonomy
Web Admin Console URL:	http://host:8080/uddi/web
Web User Console URL:	http://host:8080/uddi/bsc/web

4 Input the following parameters which are split into two sections:

Enter the general details for the registry:

Parameter	**Definition**
Name	The name of the registry artifact
Description	A description for the new registry
Categories	Click **add category** to select a category from the available taxonomies

Parameter	Definition
UDDI API Version	Select v3 or v2 It is possible to create a UDDI v2 registry but the integration features are only fully compliant with UDDI v3.
HP SOA Registry	Check the box if the registry is a HP SOA Registry Foundation
Allow Import	Check this box if the registry is a source of data import
Allow Export	Check this box if the registry is a target for data export
Publish Location	The repository location to store resource content.

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. The following example is for the Microsoft UDDI registry:

Parameter	Value for Microsoft UDDI
Inquiry URL	http://*hostname*/uddipublic/inquire.asmx
Publishing URL	https://*hostname*:*port*/uddipublic/publish.asmx
Security URL	Varies
Taxonomy URL	Varies
Web Admin Console URL	Varies
Web User Console URL	Varies

5 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 Guide* .

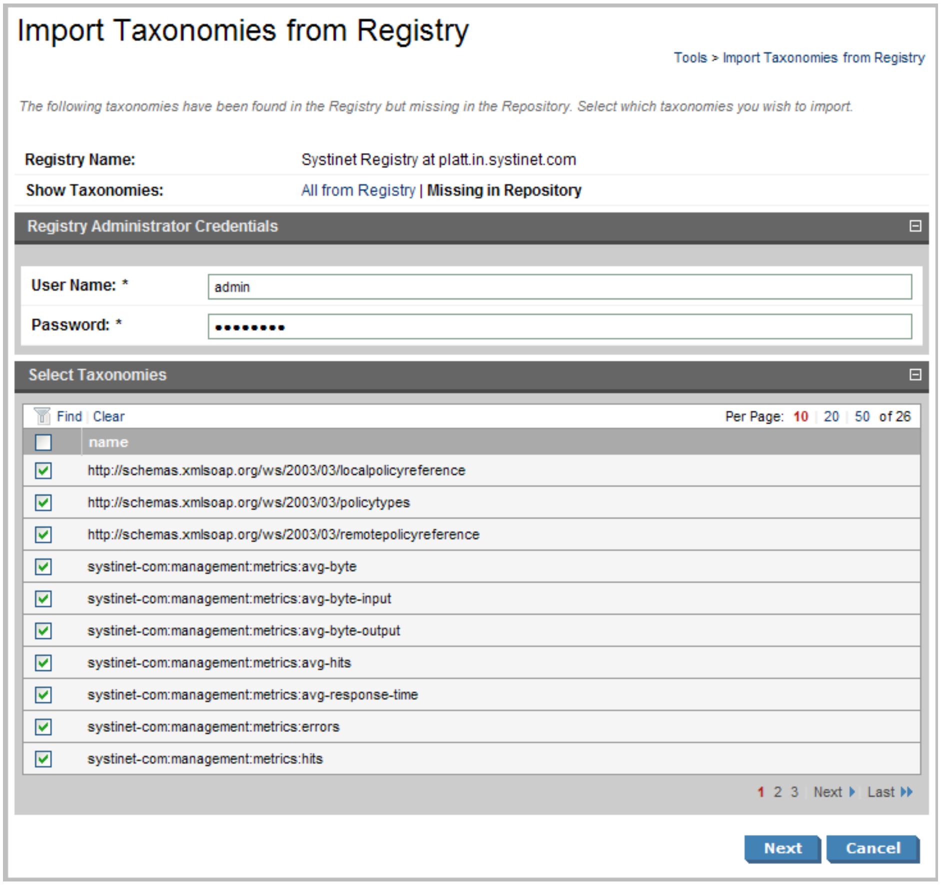
Synchronizing Taxonomies

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.

Note: 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:



Import Taxonomies from Registry

The following taxonomies have been found in the Registry but missing in the Repository. Select which taxonomies you wish to import.

Registry Name:	Systinet Registry at platt.in.systinet.com
Show Taxonomies:	All from Registry | **Missing in Repository**

Registry Administrator Credentials

User Name: *	admin
Password: *	●●●●●●●●●

Select Taxonomies

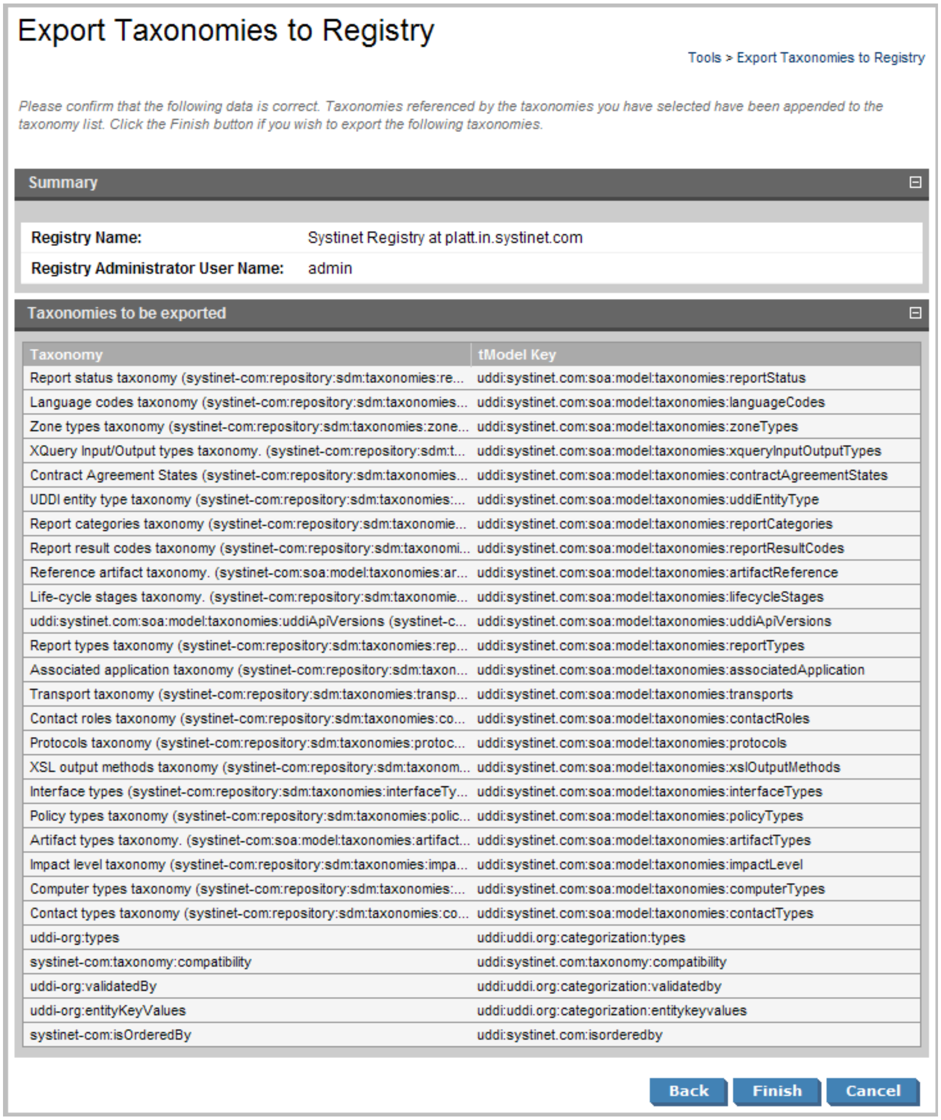
□	name
☑	http://schemas.xmlsoap.org/ws/2003/03/localpolicyreference
☑	http://schemas.xmlsoap.org/ws/2003/03/policytypes
☑	http://schemas.xmlsoap.org/ws/2003/03/remotepolicyreference
☑	systinet-com:management:metrics:avg-byte
☑	systinet-com:management:metrics:avg-byte-input
☑	systinet-com:management:metrics:avg-byte-output
☑	systinet-com:management:metrics:avg-hits
☑	systinet-com:management:metrics:avg-response-time
☑	systinet-com:management:metrics:errors
☑	systinet-com:management:metrics:hits

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

3 Review the export report which 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.

Registry Name:	Systinet Registry at platt.in.systinet.com
Registry Administrator User Name:	admin

Taxonomies to be exported

Taxonomy	tModel Key
Report status taxonomy (systinet-com:repository:sdm:taxonomies:re...	uddi:systinet.com:soa:model:taxonomies:reportStatus
Language codes taxonomy (systinet-com:repository:sdm:taxonomies...	uddi:systinet.com:soa:model:taxonomies:languageCodes
Zone types taxonomy (systinet-com:repository:sdm:taxonomies:zone...	uddi:systinet.com:soa:model:taxonomies:zoneTypes
XQuery Input/Output types taxonomy. (systinet-com:repository:sdm:t...	uddi:systinet.com:soa:model:taxonomies:xqueryInputOutputTypes
Contract Agreement States (systinet-com:repository:sdm:taxonomies...	uddi:systinet.com:soa:model:taxonomies:contractAgreementStates
UDDI entity type taxonomy (systinet-com:repository:sdm:taxonomies:...	uddi:systinet.com:soa:model:taxonomies:uddiEntityType
Report categories taxonomy (systinet-com:repository:sdm:taxonomie...	uddi:systinet.com:soa:model:taxonomies:reportCategories
Report result codes taxonomy (systinet-com:repository:sdm:taxonomi...	uddi:systinet.com:soa:model:taxonomies:reportResultCodes
Reference artifact taxonomy. (systinet-com:soa:model:taxonomies:ar...	uddi:systinet.com:soa:model:taxonomies:artifactReference
Life-cycle stages taxonomy. (systinet-com:repository:sdm:taxonomie...	uddi:systinet.com:soa:model:taxonomies:lifecycleStages
uddi:systinet.com:soa:model:taxonomies:uddiApiVersions (systinet-c...	uddi:systinet.com:soa:model:taxonomies:uddiApiVersions
Report types taxonomy (systinet-com:repository:sdm:taxonomies:rep...	uddi:systinet.com:soa:model:taxonomies:reportTypes
Associated application taxonomy (systinet-com:repository:sdm:taxon...	uddi:systinet.com:soa:model:taxonomies:associatedApplication
Transport taxonomy (systinet-com:repository:sdm:taxonomies:transp...	uddi:systinet.com:soa:model:taxonomies:transports
Contact roles taxonomy (systinet-com:repository:sdm:taxonomies:co...	uddi:systinet.com:soa:model:taxonomies:contactRoles
Protocols taxonomy (systinet-com:repository:sdm:taxonomies:protoc...	uddi:systinet.com:soa:model:taxonomies:protocols
XSL output methods taxonomy (systinet-com:repository:sdm:taxonom...	uddi:systinet.com:soa:model:taxonomies:xslOutputMethods
Interface types (systinet-com:repository:sdm:taxonomies:interfaceTy...	uddi:systinet.com:soa:model:taxonomies:interfaceTypes
Policy types taxonomy (systinet-com:repository:sdm:taxonomies:polic...	uddi:systinet.com:soa:model:taxonomies:policyTypes
Artifact types taxonomy. (systinet-com:soa:model:taxonomies:artifact...	uddi:systinet.com:soa:model:taxonomies:artifactTypes
Impact level taxonomy (systinet-com:repository:sdm:taxonomies:impa...	uddi:systinet.com:soa:model:taxonomies:impactLevel
Computer types taxonomy (systinet-com:repository:sdm:taxonomies:...	uddi:systinet.com:soa:model:taxonomies:computerTypes
Contact types taxonomy (systinet-com:repository:sdm:taxonomies:co...	uddi:systinet.com:soa:model:taxonomies:contactTypes
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

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 receive the data generated by BAC about shared services.

Services can also be imported from BAC/UCMDB.

SOA Systinet can only integrate with 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 then modify the properties of the existing BAC/UCMDB server. Do not delete it and create a new one.

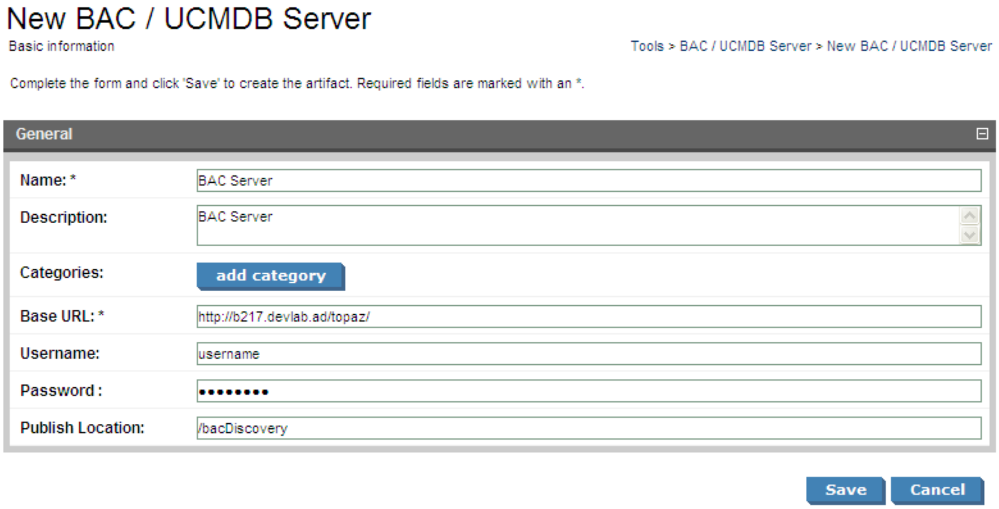
To create a BAC/UCMDB server artifact:

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:



New BAC / UCMDB Server

Basic information

Tools > BAC / UCMDB Server > New BAC / UCMDB Server

Complete the form and click 'Save' to create the artifact. Required fields are marked with an *.

General

Name: *	BAC Server
Description:	BAC Server
Categories:	add category
Base URL: *	http://b217.devlab.ad/topaz/
Username:	username
Password :	••••••••
Publish Location:	/bacDiscovery

3 Input the following parameters:

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

4 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 only integrate with one SPE server.

To create an SPE server artifact:

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

   The browse 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
Username and Password	The credentials to login in to SOA Policy Enforcer
HTTP Basic Authentication	Select to use the credentials to log in instead of anonymous access

4. 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" the *HP SOA Systinet User Guide* :

Setting Up STM Integration

HP Service Test Manager (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 SOA Policy Enforcer server artifact:

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

   The browse 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.

Parameter	**Definition**
Username	Credentials for the STM server.
Password	
STM Domain	The domain containing the testing project in QC.
STM Project	The testing project in QC.
HTTP Basic Authentication	Select to use the credentials instead of anonymous login.

4 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 35

- Managing Licensed Users on page 35

Changing the License

The administrator can change the SOA Systinet license.

To change the SOA Systinet license:

1. Contact 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 36.

To find out how to remove users, see Removing Licensed Users on page 36.

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.

- Data Migration on page 39

  Migrate data from previous versions of SOA Systinet.

- Configuration Procedures on page 41

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

Data Migration

You can migrate data and configuration options from SOA Systinet 2.52 to 3.00.

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

The patch is distributed with SOA Systinet 3.00.

Copy `3.00_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.

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

   SOA_HOME/bin/configurationexport ***`configimage`***

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

SOA_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 3.00, 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 3.00 if it is different to 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 must 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 should create an image folder matching the output of the export tool.

For details, see Export Tool on page 62.

7 In SOA Systinet 3.00, execute the import tool:

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

For more details, see Import Tool on page 64.

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 and also to make additional changes to your installation.

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

- Applying Extensions on page 41
- Applying Updates on page 45
- Setting Up LDAP Integration on page 46
- Redeploying the EAR File on page 47
- Changing the System Configuration on page 47

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 pre-packaged 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 and 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 42

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

- Decoupled DB Scenario on page 44

  Database SQL scripts are run manually, and the setup tool performs the other processes as individual steps that are executable on demand. This 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 47.

- For other application servers, 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/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 47.

   - For other application servers, 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 an update:

1 Copy the update 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**.

   The setup tool automatically validates the step by connecting to the server and applying the update.

5 Click **Finish** to close the setup tool.

6. After applying updates, you need to reapply any required extensions, using the procedure described in Applying Extensions on page 41.

7. Redeploy the EAR file as described in:

   - For JBoss follow the procedure described in Redeploying the EAR File on page 47.

   - For other application servers, 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 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. After the Setup Tool applies your LDAP settings, select **Finish** to exit the Setup tool, or **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.

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 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**.
5. When the setup tool validates the existence of the JBoss Deployment folder, click **Next**.
6. Click **Finish** to close the setup tool.
7. 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 on page 48

- Configuring the Default ACLs on page 49
- Configuring Consumer and Provider Artifacts on page 49
- Configuring the Compliance Status Cache on page 51

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 in order to prevent memory overflow.

The default limits are 10 history pages and 4 branches.

> The history default is effectively 5 pages as 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. For history depth 30 (15 effective steps) and 6 concurrent windows.

   Add the following properties:

   - 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 allows 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 Follow the procedure described in Changing the System Configuration on page 47, making the following changes.

4 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* .

5 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.

6 Save `configuration.properties`.

7 Upload the new configuration with:

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

8 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.

This is determined by a caching property in the configuration which by default is set to an 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

The 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.

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.

The basic use of the Setup Tool is to 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 on page 53
- Change License Key on page 54
- Application Server Change on page 55
- Apply Extension Options on page 55
- Update on page 56
- Advanced on page 56

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

For details, see Setup Tool Command-Line Options on page 56.

Default

The default use of the Setup Tool is to change the configuration of SOA Systinet set up 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:

- The Database Setup Operations page has an additional option to **Configure Database**.

  Select this option 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* .

- After the JDBC Driver step there is an additional Configuration Table Management page with the following options:

  - 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.

- 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.

Change 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, and then click **Next**:
   - Select **Install a 60 day evaluation license**.
   - Select **Enter license details**, and input the license details provided by your sales representative.
3. Click **Next** through each confirmation and progress page, and then do one of the following:
   - Click **Setup Again** to return to the Scenario Selection page.
   - Click **Finish** to exit the Setup Tool.

Application Server Change

The Setup Tool enables you to change the application server used with the product. HP Software only recommend using this option in consultation with an HP field engineer.

In the Scenario Selection page, select **Application Server Change**, and then click **Next**.

The Scenario Selection page opens again, enabling you to choose how to configure the product in conjunction with the application server change.

Apply Extension Options

The Setup tool offers the following extension application methods in the Scenario Selection page:

- **Apply Extensions**

  Use this option to apply your extension and make any associated data changes required by it.

- **Apply Extensions with no DB Impact**

  Use this option when your extension has no impact on any existing database data.

For details, see Applying Extensions on page 41.

Update

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 45.

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

For details, see Update Management Tool on page 69.

Advanced

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

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.

Specific details of which steps to select are described whenever the Advanced scenario is required for procedures in this documentation.

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.

- **-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 59.

This chapter describes the following utilities:

- Export Tool on page 62
- Import Tool on page 64
- Reset Tool on page 66
- SDM to Database Mapping Tool on page 67
- SSL Tool on page 68
- Update Management Tool on page 69

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 in folder `SOA_HOME/bin`. These are either `BAT` batch files or `SH` shell scripts, depending on the server operating system.

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

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

Table 3. Summary of SOA Systinet Admin Utilities

Command	Description
create	Create a resource using the http interface. For details, see "Proprietary REST Interface" in the *HP SOA Systinet Developer Guide* .
delete	Delete 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	Create a data image for specified components of SOA Systinet. For details, see Export Tool on page 62.
get	Gets a resource using the http interface with an option to save it to a specified file and also supports the EXIST operation. For details, see "Proprietary REST Interface" in the *HP SOA Systinet Developer Guide* .
import	Import a data image for specified components of SOA Systinet. For details, see Import Tool on page 64.
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 39.
reset	Reset the data for specified components of SOA Systinet. For details, see Reset Tool on page 66.
../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 67.
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	Configure and view your SSL configuration. For details, see SSL Tool on page 68.
update	Update 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 standalone via the command line. For details, see Update Management Tool on page 69.

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]

With 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.

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 chosen.

- `image.properties`

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

- `configuration`

  A directory containing the configuration data.

- `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 data.

- `security`

  A directory containing the security configuration.

Import Tool

The **import** 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 import is:

import --image *IMAGE_NAME* [OPTIONS]

With 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.

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.

- `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 data.

- `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, then 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]

With 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 an RDBMS 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 which 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 `SOA_HOME/lib/sdm/build/sdm2dbmap.html`, and is split into three parts:

- A top level 1:1 mapping between SDM artifacts and DB tables. Each artifact listed, maps directly to one table.
- The second part contains 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.
- The last part of the report documents 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 intended to enable you to set up 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]

- no option lists the upgrades that are available.
- `--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 named update. This update must be the latest installed.

  Extensions must be reapplied.

- `--passphrase PASSPHRASE` to use the update tool 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 41.