

HP SOA Systinet

Software Version: 2.52, Standard Edition

Administrator Guide

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



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Third-Party Web Sites

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

Copyright Notices

Copyright © 2006-2007, Hewlett-Packard Development Company, L.P.

Trademark Notices

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

Contents

- Welcome to This Guide. 5
 - How This Guide is Organized. 5
 - Document Conventions. 5
 - Documentation Updates. 6
 - Support. 6
- I SOA Systinet Administration. 9
 - 1 User Management. 11
 - Managing User Accounts. 12
 - Managing User Groups. 13
 - Managing User Perspectives. 15
 - 2 SOA Systinet Configuration Options. 17
 - 3 Access Rights. 19
 - 4 Registry Setup and Configuration. 23
 - Creating a Registry Artifact. 24
 - Importing Registry Certificates. 28
 - Synchronizing Taxonomies. 28
- II System Administration. 33
 - 5 Data Migration. 35
 - 6 SSO Partner Management. 37
 - Partner Affiliations. 37
 - Modifying SSO Descriptors. 37
 - 7 Configuration Procedures. 39

Applying Extensions.	39
Applying Updates.	43
Redeploying the EAR to JBoss.	44
Restricting LDAP Group Login.	45
Changing the System Configuration.	46
III Administration Utilities.	51
8 SSO Server Utilities.	53
9 Reporting Server Utilities.	55
10 Platform Server Utilities.	57
11 Policy Server Utilities.	61
12 Setup Tool.	63
13 Update Management Tool.	67
14 Repository Export Tool.	69
15 Repository Import Tool.	71
16 Repository Reset Tool.	73
17 SSO Configuration Tool.	75
18 Reporting Import/Export Tool.	77
Index.	79

Welcome to This Guide

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

How This Guide is Organized

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

This guide contains the following parts:

Part I, “SOA Systinet Administration”. Administration facilities accessed from the SOA Systinet UI.

Part II, “System Administration”. A procedural guide to common tasks performed by the system administrator.

Part III, “Administration Utilities”. A guide to both command line and client tools provided with SOA Systinet.

Document Conventions

The typographic conventions used in this document are:

run.bat make	Script name or other executable command plus mandatory arguments.
[--help]	A command-line option.
either or	A choice of arguments.
<i>replace_value</i>	A command-line argument that should be replaced with an actual value.
{arg1 arg2}	A choice between two command-line arguments where one or the other is mandatory.
<code>rmdir /S /Q System32</code>	Operating system commands and other user input that you can type on the command line and press Enter to invoke. Items in <i>italics</i> should be replaced by actual values.

C:\System.ini	Filename, directory names, paths and package names.
a.append(b);	Program source code.
server.Version	An inline Java or C++ class name.
getVersion()	An inline Java method name.
Shift-N	A combination of keystrokes.
Service View	A label, word or phrase in a GUI window, often clickable.
OK	A button in a GUI window.
New->Service	Menu choice.

Documentation Updates

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

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

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

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

Support

Mercury Product Support

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

- If you work with an HP Software Services Integrator (SVI) partner (http://h20230.www2.hp.com/svi_partner_list.jsp), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.

- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: <http://hp.com/go/hpsoftwaresupport>.
- For the latest information about support processes and tools available for products formerly produced by Systinet, we encourage you to visit the Systinet Online Support Web site at: <http://www.systinet.com/support/index>.
- If you have additional questions, contact your HP Sales Representative.

HP Software Support

You can visit the HP Software Support Web site at:

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

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

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

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

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

Part I. SOA Systinet Administration

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

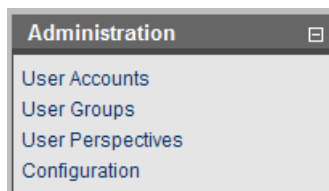
This part describes these additional administration functions:

- [User Management on page 11](#)
- [SOA Systinet Configuration Options on page 17](#)
- [Access Rights on page 19](#)
- [Registry Setup and Configuration on page 23](#)

1 User Management

The administrator has additional management options that are not visible to other user perspectives. In the **Tools** menu there is an **Administration** section:

Figure 1. Administration Menu



Additionally, the administrator can manage permissions at the artifact level using the **Access Rights** context action menu option available in artifact detail views as described in [Access Rights on page 19](#).

▶ **Note:** If LDAP is used for account management then the appropriate LDAP server administration functions should be used for user management and not the SOA Systinet administration functions described in this part of the guide. LDAP user management and SOA Systinet user and group management can be combined if enabled, as described in [SOA Systinet Configuration Options on page 17](#).

This part describes these additional administration functions:

- [Managing User Accounts on page 12](#)
- [Managing User Groups on page 13](#)
- [Managing User Perspectives on page 15](#)

Managing User Accounts

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

Input a search term and click **Go** to find users matching your input.


 **Note:** This search function operates in the same way as described in the Service Discovery section in the HP SOA Systinet User Guide. The search term for user accounts must not be empty.

Figure 2. Browse Accounts

Browse Accounts

[Tools > Browse Accounts](#)


This page displays user accounts. Click a username to view their account details.

[New Account](#)

Search for: in: Full Name ▾ Go

Login Name	Full Name ↕	Description
chuma	chuma	
consumer	consumer	
consumer1	consumer1	
consumer2	consumer2	

The administrator can review user accounts in the **Browse Accounts** page. If the SSO user account store is in the SOA Systinet database the **Browse Accounts** page can be used to access create and edit account options. If the account store is on an LDAP server, this page is read-only, and changes to the user account store must be made by the LDAP administrator.

 **Note:** To use this feature when SOA Systinet is configured to use an LDAP server the **Account Management** option must be selected, as described in [SOA Systinet Configuration Options on page 17](#).

Click **New Account** to create an account, as described in the Creating an Account section of the HP SOA Systinet User Guide.

Click an account name to open the **View Account** page.

This is the same page that any other user would see with the following additions:

- **Group Membership.** This section displays the user groups that the account is a member of.
- **Clone Account.** Select **Clone Account** from the **View** menu to open a page identical to the **Create New Account** page with all the information copied from the user account.
- **Retire Account.** Select **Retire Account** from the **View** menu to transfer the ownership of all artifacts owned by this user to a new user with the same functionality described in the Changing Artifact Ownership section of the HP SOA Systinet User Guide.

Click **Edit** or **Change Password** to change the account details as described in the Managing Your Account section in the HP SOA Systinet User Guide.

Managing User Groups

In the **Administration** section of the tools menu, click **User Groups** to open the **Browse Groups** page:

Figure 3. Browse Groups

Name	Description
system#everyone	The special group that contains all users.
system#intranet	The special group that contains users who are part of intranet domain.
system#registered	The special group that contains all users who are logged in the UDDI registry.

If the SSO user account store is on the SOA Systinet database, the administrator can also create and edit groups from this page.

► **Important:** To use SOA Systinet to create or edit user groups in combination with LDAP user management the appropriate option must be set as described in [SOA Systinet Configuration Options](#) on page 17.

Creating a User Group

User administration can be made easier by organizing users into groups.

To create a new user group:

- 1 Click **New Group** to open the **Create New Group** page:

Figure 4. Create New Group Page

Create new Group

Tools > 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: *	Buyer
Description:	Procurement
Defines administrators:	<input type="checkbox"/>

Group Memberships	
Search for: john	in: Full Name
Go	
Login Name	Full Name
johnuser	John User

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	Check the box if this group has administrator privileges

- 3 You can also select the members of this new group. Use the search function to identify users and click **Add** to select new users from the search list and click the cross next to a user in the group to remove them.
- 4 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 **Browse Groups** page, click the group name to open its detail view.
- 2 Click **Edit** to open the edit view.
- 3 Edit the group parameters as required, and click **Add** to add new members, and click the cross next to a member to remove them from the group.
- 4 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 **Browse Perspectives** page, click the perspective name to open its detail view.

- 2 Click **Edit** to open the **Edit Perspective** page.
- 3 Click **Add** to add new user groups and click the cross next to a group to remove it.
- 4 Click **Save** to confirm your changes.

2 SOA Systinet Configuration Options

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

- **User Self-Registration.** Select this option to make **Register as a New User** an available option at **Sign On**.
- **Full Text Search.** Select this option to enable full text search as described in Full Text Search section in the HP SOA Systinet User Guide.



Note: Full text search must also be enabled on the database as described in the Configuring the Database for Full Text Searching section in the HP SOA Systinet Installation Guide.

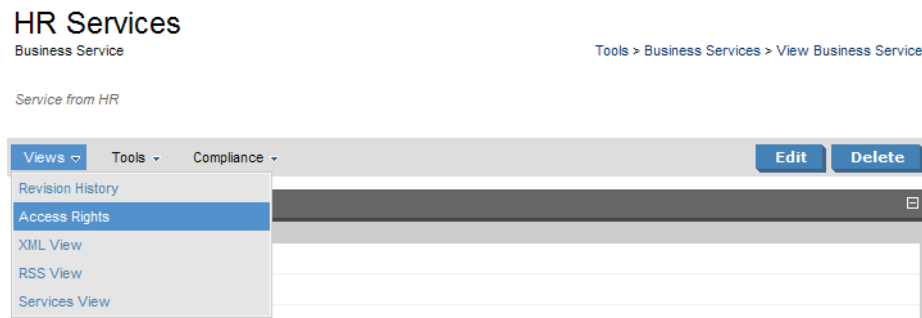
- **Group Management** (Only visible when user accounts are on an LDAP server). Select this option if you are using an LDAP server for user account management and want to use the SOA Systinet user group management features.
- **Account Management** (Only visible when user accounts are on an LDAP server). Select this option if you are using an LDAP server for user account management and want to use the SOA Systinet user account management features.
- **HTTPS Certificate Validation.** SOA Systinet can verify whether SSL certificates are from a trusted authority and whether HTTPS URL hostnames match SSL server certificates. This function is chosen during installation. Only disable certificate validation after installation in a development or evaluation environment, when the only HTTPS communication will be with other SOA Systinet components, HP SOA Systinet Registry, BAC or HP SOA Manager. See the Developer Guide for more information.
- **Self Test Access.** Enable this option to perform the checks described in the Self-Testers section of the HP SOA Systinet Installation Guide.

3 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 an artifact or a collection:

- 1 From the detail or browse view of artifacts, in the **Views** context menu, select **Access Rights** to open the **View Access Rights** page:



- 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User	systemet:anonymous	<input type="checkbox"/>	<input type="checkbox"/>
	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>


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

Save
Cancel

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

 **Tip:** To grant a guest user access rights to the artifact, set the permissions for the **systemet:anonymous** account.

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

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

For information about changing the default ACL, please see [Configuring the Default ACLs on page 48](#).



Note: 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.



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

4 Registry Setup and Configuration

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. For HP Systinet V3 registries there is extra functionality: taxonomy synchronization and Single Sign On (if enabled on the remote Registry).

Be aware that 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 Systinet Registry. The UDDI specification has three major versions, commonly named v1, v2 and v3. SOA Systinet is interoperable with UDDI 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 HP 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 HP 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 HP 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.



Tip: The mapping for certain types of tModel can be defined in PLATFORM_HOME/conf/registryconf.xml.

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



Note: 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) [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) [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 24](#)
- [Importing Registry Certificates on page 28](#)
- [Synchronizing Taxonomies on page 28](#)

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 browse view of registries click **New**.
 - Alternatively, in the **Registry Content** section of the tools menu click **Import Registry Content** to open the **Import Artifacts from Registry** page and then click **New Registry**.

The **Create New UDDI Registry** page appears.

- 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
Systinet's registry	Check the box if the registry is a HP SOA Systinet Registry

- 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: *

Description:

Categories:

UDDI API version: v3 (uddi:systinet.com:soa:model:taxonomies:uddiApiVersions:v3)
 v2 (uddi:systinet.com:soa:model:taxonomies:uddiApiVersions:v2)

Systinet's Registry:

Allow Import:

Allow Export:

Registry Addresses

Inquiry URL:

Publishing URL:

Security URL:

Taxonomy URL:


Web Admin Console URL:

Web User Console URL:

- 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

Parameter	Definition
Categories	Click add category to select a category from the available taxonomies
UDDI API Version	Select v3 or v2  Note: It is possible to create a UDDI v2 registry but the integration features are only fully compliant with UDDI v3.
Systinet's Registry	Check the box if the registry is a HP SOA Systinet Registry
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

If the registry is a HP SOA Systinet Registry 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	<code>http://hostname/uddipublic/inquire.asmx</code>
Publishing URL	<code>https://hostname:port/uddipublic/publish.asmx</code>
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 Systinet Registry communication, then it is necessary to import the registry certificates into the application server certificate store. For details, see the Importing SOA Systinet Registry Truststore in the After Installation part of 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

[Tools > 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: *

Password: *

Select Taxonomies

Per Page: [10](#) [20](#) [50](#) of 26

<input type="checkbox"/>	name
<input checked="" type="checkbox"/>	http://schemas.xmlsoap.org/ws/2003/03/localpolicyreference
<input checked="" type="checkbox"/>	http://schemas.xmlsoap.org/ws/2003/03/policytypes
<input checked="" type="checkbox"/>	http://schemas.xmlsoap.org/ws/2003/03/remotepolicyreference
<input checked="" type="checkbox"/>	systinet-com:management:metrics:avg-byte
<input checked="" type="checkbox"/>	systinet-com:management:metrics:avg-byte-input
<input checked="" type="checkbox"/>	systinet-com:management:metrics:avg-byte-output
<input checked="" type="checkbox"/>	systinet-com:management:metrics:avg-hits
<input checked="" type="checkbox"/>	systinet-com:management:metrics:avg-response-time
<input checked="" type="checkbox"/>	systinet-com:management:metrics:errors
<input checked="" type="checkbox"/>	systinet-com:management:metrics:hits

1 2 3 Next ▶ Last ▶▶

[Next](#) [Cancel](#)

- 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.

Summary

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

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.

Part II. System Administration

This part includes details of tasks that are required to administer an installation of Systinet 2.

- [Data Migration on page 35](#). Migrating data from previous versions of SOA Systinet.
- [SSO Partner Management on page 37](#). Managing Single Sign-On partner domains.
- [Configuration Procedures on page 39](#). Managing the configuration of SOA Systinet using the command-line utilities.

5 Data Migration

You can migrate data and configuration information from SOA Systinet and Policy Manager versions 2.0 and 2.1.

To migrate data from an earlier version of SOA Systinet:

- 1 In the earlier installation of SOA Systinet, run the **repositoryexport** tool. This creates an image of the repository. (See the System Administration chapter of the earlier version's documentation and [Repository Export Tool on page 69](#).)
- 2 If you were using HP SOA Systinet Policy Manager, it stored its assertions in a separate relational database. Export the assertions from that database with the `get` tool of your earlier Policy Manager installation. (See Backup and Restoration in the User's Guide of your earlier Policy Manager documentation for details.) The command will be similar to:

```
OLD_PM_HOME/bin/get [-u administrator_username ] [-p password ] [-r ] [-O target_directory ]  
[http://localhost:9900/systinet/policymgr/rest/assertions/]
```
- 3 Transform the exported data to prepare it for import to SOA Systinet. Use the `migrate` tool with the following syntax:

```
NEW_PLATFORM_HOME/bin/migrate [-s image -d image] [-a assertions]
```
- 4 Run the **NEW_PLATFORM_HOME/bin/repositoryreset** tool on the new database (not required if the installation is brand new and the server has never been started).
- 5 Update the `PLATFORM_HOME/conf/sdm/sdmConfig.xml` file in the new installation if required.



Note: The HP SOA Systinet Customization Editor should be used to make these changes.

- 6 Use the **PLATFORM_HOME/bin/repositoryimport** tool to import data into the new database.

- 7 If you are using the SOA Systinet userstore instead of LDAP in your new installation then use the **SSO_HOME/bin/import** tool to import the userstore data from the image to the database.



Note: If the repositoryimport tool gives a warning about `sdmConfig.xml` being different, possible reasons include:

- The versions of SOA Systinet have different configurations. No update is needed if this is the only reason.
- Your exported `sdmConfig.xml` contains some customizations. In this case you must make the same changes to `sdmConfig.xml` in the new installation using the HP SOA Systinet Customization Editor.
- Changes were made to your exported `sdmConfig.xml` during installation of an application such as HP SOA Systinet Policy Manager. You should *not* merge these changes into `sdmConfig.xml` in the new installation. They will be made automatically if you install the same SOA Systinet application to your new installation of SOA Systinet platform.

6 SSO Partner Management

An SSO partner is any SSO-enabled application. The SSO domain is a set of SSO partners managed by and using one instance of SSO services. Each SSO partner is introduced to the SSO domain by its SSO descriptor. The SSO descriptor is an XML document containing the partner's X509 certificate and the location of its SSO endpoints, which are necessary to integrate this partner to the SSO domain.

Partner Affiliations

In the SSO affiliation, all partners trust each other. The trust is set up by the SSO configuration service exposing its REST interface at the location `/rest/descriptor`, eg. `http://localhost:8080/sso/rest/descriptor`. You can obtain the SSO descriptors of all SSO partners in the affiliation using the HTTP GET operation. The `ssoconfig` tool in `sso/bin` can be used for this, with the `get` option.

To integrate with the SSO affiliation, the SSO partner must know the URL of the SSO configuration service, have its SSO descriptor deployed to the SSO configuration service, and know the private key coupled with the X509 certificate in the SSO descriptor.

Modifying SSO Descriptors

To download and deploy the descriptor of an SSO partner, use the `ssoconfig` tool, located in `SSO_HOME/bin`. This is useful when the location of an SSO partner in the affiliation changes its URL, so that its SSO endpoints are not accessible anymore.

To download and deploy the descriptor of an SSO partner:

- 1 Download the SSO descriptor with the following command:

```
ssoconfig get -e partner_name -s  
http://localhost:8080/sso -d directory
```

- 2 Change the URL in the file `[partner_name].xml`.
- 3 Upload `[partner_name].xml` back to the configuration service with the following command:

```
ssoconfig update -s http://localhost:8080/sso -u admin -p changeit -f partner_name.xml
```

By default, the root URL of your SSO service is `http://localhost:8080/sso`, the administrator credentials are `admin:changeit`, and the name of your partner entered during the product installation is `partner_name` (for example, `urn:systinet2:policymgr:1.2:hostname:8443`).



Note: The partner name may include information about the hostname and port. The name must be preserved even if you change the hostname or port without reinstalling the product.

7 Configuration Procedures

System configuration is maintained using the tools described in [Part III, “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 39](#)
- [Applying Updates on page 43](#)
- [Redeploying the EAR to JBoss on page 44](#)
- [Restricting LDAP Group Login on page 45](#)
- [Changing the System Configuration on page 46](#)

Applying Extensions

SOA Systinet can be extended with libraries that are added into the deployed EAR files. The setup tool opens the EAR files, applies the extensions, and then repacks the EAR files.

Extensions to SOA Systinet come from the following sources:

- The HP SOA Systinet Customization Editor
- HP SOA Systinet Policy Manager extensions used to create assertions in HP SOA Systinet Assertion Editor. These extensions are custom validation handlers. You must apply them to the Policy Manager server in order for Policy Manager to use assertions created with them.

Apply extensions according to one of the following scenarios:

- [Single-Step Scenario on page 40](#) – In this scenario, the setup tool performs all the processes involved in applying extensions, including database alterations, as a single, seamless step.
- [Decoupled DB Scenario on page 41](#) – In this scenario, 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 who applies 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 Ensure that all extensions are in the `PLATFORM_HOME/extensions` directory. The setup tool automatically applies all extensions in that directory.



Note: If you are applying extensions to another server, substitute `PLATFORM_HOME` with the relevant home directory.

- 2 Stop the server.
- 3 Start the setup tool by executing `PLATFORM_HOME/bin/setup.bat(sh)`.



Important: The application server to which SOA Systinet is deployed must not be running.

- 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.
- 5 Click **Next** for each of the validation steps and the setup execution. Note that this takes some time.
- 6 Click **Finish** to end the process.

- 7 For JBoss implementations the EAR file is deployed automatically. For WebLogic, WebSphere and Oracle Application Server, redeploy the EAR file as described in:
 - For WebLogic, follow the procedure described in the Deploying SOA Systinet Components section of the HP SOA Systinet Installation Guide.
 - For WebSphere, follow the procedure described in the Deploying the SSO Service and Creating EAR Files section of the HP SOA Systinet Installation Guide.
 - For OAS, follow the procedure described in the Creating and Deploying SOA Systinet EARs section of the HP SOA Systinet Installation Guide.
- 8 Restart the server.

Decoupled DB Scenario

Follow this scenario if the user who applies extensions does not also modify the database.

To apply extensions and modify the database separately:

- 1 Ensure that all extensions are in the `PLATFORM_HOME/extensions` directory. The setup tool automatically applies all extensions in that directory.



Note: If you are applying extensions to another server, substitute `PLATFORM_HOME` with the relevant home directory.

- 2 Stop the server.
- 3 Start the setup tool by executing **`PLATFORM_HOME/bin/setup.bat(sh)`**.



Important: The application server to which SOA Systinet is deployed must not be running.

- 4 Select the **Advanced** scenario and click **Next**.


5 Scroll down and select the following options:

- Extensions environment setup
- Extensions model execution
- Extensions database prepare
- Extensions database backup

6 Click **Next**, execute the chosen steps, and exit the setup tool.


7 The database administrator runs the following SQL scripts. `INSTALL_HOME` refers to the installation directory of the SOA Systinet component to which you are applying the extensions. **The SQL scripts must be run in this order:**

- `INSTALL_HOME\conf\sql\dbschema_YOUR-DATABASE_drop.sql`
- `INSTALL_HOME\working\sdm-gen\build\rdbms\sql\dbschema_YOUR-DATABASE_create.sql`

 **Note:** For DB2, the token `&1` must be replaced by the tablespace name.

- `INSTALL_HOME\working\sdm-gen\build\rdbms\sql\dbschema_YOUR-DATABASE_insert.sql`

8 Start the setup tool by executing `PLATFORM_HOME/bin/setup.bat(sh)`.

 **Important:** The application server to which SOA Systinet is deployed must not be running.

9 Select the **Advanced** scenario and click **Next**.

10 Select the following options:

- Extensions database SQL sync

- Extensions database restore
- Extensions nonmodel execution
- Extensions environment finalize
- Client package creation

11 Click **Next**, execute the chosen steps, and exit the setup tool.

12 For WebLogic and WebSphere, deploy the new EAR file in the `INSTALL_HOME\deploy` directory.

Applying Updates

Product updates from HP Systinet are applied to the using the setup tool. For more details see [Setup Tool on page 63](#).

To apply an update:

1 Copy the update to the `PLATFORM_HOME/updates` folder.



Note: If you are applying updates to another server substitute `PLATFORM_HOME` with the relevant home directory.

2 Stop the application server.

3 Start the setup tool by executing **`PLATFORM_HOME/bin/setup.bat(sh)`**.



Important: The application server to which SOA Systinet is deployed must not be running.

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 reapply any required extensions using the procedure described in [Applying Extensions on page 39](#).
- 7 Redeploy the EAR file as described in:
 - For JBoss follow the procedure described in [Redeploying the EAR to JBoss on page 44](#).
 - For WebLogic follow the procedure described in the Deploying SOA Systinet Components of the HP SOA Systinet Installation Guide.
 - For WebSphere follow the procedure described in Deploying the SSO Service and Creating EAR Files section of the HP SOA Systinet Installation Guide.
 - For Oracle Application Server, follow the procedure described in the Creating and Deploying SOA Systinet EARs section of the HP SOA Systinet Installation Guide.
- 8 Restart the application server.

Redeploying the EAR to JBoss

After using the setup tool to apply extensions or updates it is necessary to redeploy the EAR file to the application server. For JBoss this can be done using the setup tool.



For other application servers, follow the EAR deployment procedures described in the relevant sections of Deploying SOA Systinet to Application Servers in the HP SOA Systinet Installation Guide.

To redeploy the EAR to JBoss:

- 1 Stop the application server.
- 2 Start the setup tool by executing **PLATFORM_HOME/bin/setup.bat(sh)**.



Important: The application server to which SOA Systinet is deployed must not be running.

- 3 Choose 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.

Restricting LDAP Group Login

You can restrict login rights to users belonging to a subset of LDAP user groups.

To restrict LDAP group login rights:

- 1 Open `SSO_HOME/conf/system/sso.xml` in an editor.
- 2 Find the root `config` element and give it the attribute `updateDB="true"`.
- 3 Add a child `property` element to `config`. Give `property` the attribute `key="groups.allowed"`.
- 4 Give `property` the attribute `value` with the value of a comma-separated list of user groups allowed to log in. For example, if you only want to allow users in groups `g1` and `g2` to log in, write the following `property` element:

```
<config name="sso" updateDB="true">
    <property key="groups.allowed" value="g1,g2"/>
    ...
</config>
```

- 5 Save your changes to `sso.xml`.

- 6 From the directory `SSO_HOME/conf/bin/`, run **`confsync -c ../conf/system`**. The `confsync` tool synchronizes your changes with the SSO configuration in the database.

Changing the System Configuration

The system configuration can be accessed and manually edited using the `configurationexport` and `configurationimport` tools.

To manually change the system configuration:

- 1 Stop the application server with:
`PLATFORM_HOME/serverstop`
- 2 Create an editable configuration file with:
`PLATFORM_HOME/bin/configurationexport config.xml`
- 3 Open `config.xml` for editing.
- 4 Locate and change or add the required parameter. See the following sections for specific changes:
 - [Configuring the Browse History on page 47](#)
 - [Configuring the Default ACLs on page 48](#)
 - [Enabling and Configuring SiteMinder on page 48](#)
- 5 Save `config.xml`.
- 6 Upload the new configuration with:
`PLATFORM_HOME/bin/configurationimport config.xml`
- 7 Restart the application server with:
`PLATFORM_HOME/bin/serverstart`

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.



Note: 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 Follow the procedure described in [Changing the System Configuration on page 46](#) making the following changes.
- 2 Locate the element `/properties/platform/webui/max` which contains the following default data:

```
<upload>
  <size>-1</size>
</upload>
```

- 3 Add elements `branch/depth` and `branch/count`. The result should look like:

```
<upload>
  <size>-1</size>
</upload>
<branch>
  <depth>30</depth>
  <count>6</count>
</branch>
```

For history depth 30 (15 effective steps) and 6 concurrent windows.

- 4 Reimport the altered configuration with the `configurationimport` tool, as described in [Changing the System Configuration on page 46](#).

Configuring the Default ACLs

The repository allows you to configure the default ACL to be set for newly created repository collections and documents (both XML and binary).

To change default ACLs:

- 1 Using the `configurationexport` tool, export the SOA Systinet configuration as described in [Changing the System Configuration on page 46](#).

- 2 Search for these elements:

```
<properties>
  <platform>
    <repository>
      <defaultAclCacheRefreshInterval>60</defaultAclCacheRefreshInterval>
      <defaultDocumentAcl>group:system#everyone:R,childof:/contactArtifacts/:group:system#everyone:R;
group:system#registered:RW,childof:/uddiEntities/:group:system#everyone:R;group:system#registered:RW</defaultDocumentAcl>
      <defaultCollectionAcl>group:system#registered:RW;group:system#everyone:R</defaultCollectionAcl>
    </repository>
  </platform>
</properties>
```

- 3 Make the relevant changes. See Default ACL Configuration in the Reference Guide for more information.
- 4 Reimport the altered configuration with the `configurationimport` tool, as described in [Changing the System Configuration on page 46](#).

Enabling and Configuring SiteMinder

SOA Systinet includes an implementation of the SiteMinder filter. The filter inspects the HTTP headers/session for information issued by a secure SiteMinder. If SiteMinder user information is present, the SSO issues an authentication token (SAML assertion) and related user information (groups, admin role) received for that user (via impersonation). This filter is disabled by default, for performance reasons.

To enable the SiteMinder filter:

- 1 Export the SOA Systinet system configuration, following the procedure described in [Changing the System Configuration on page 46](#).
- 2 Search the configuration file for the `siteminder` element. If it is not present, add a `siteminder` element as a child of `properties/shared`.
- 3 Set the value of the `siteminder`'s child `enabled` element to `true`. The element should look like the following:

```
<properties>
...
<shared>
...
<siteminder>
  <enabled>true</enabled>
</siteminder>
...
</shared>
...
</properties>
```

- 4 Import the altered SOA Systinet configuration, following the procedure described in [Changing the System Configuration on page 46](#), and restart the server.

To disable SiteMinder, follow the same procedure as for enabling StartMinder, except change the value of `enabled` to `false`.

To configure SiteMinder, follow the same procedure as for enabling SiteMinder and add child elements to `siteminder` or change the child element values. The full set of possible elements and their default values follows:

```
<properties>
...
<shared>
  <siteminder>
    <enabled>true</enabled>
    <loginNameHeader>sm-userdn</loginNameHeader>
    <allowCookie>true</allowCookie>
    <allowSessionOptimization>true</allowSessionOptimization>
  </siteminder>
  ...
</shared>
```

```
...  
</properties>
```

Part III. Administration Utilities

SOA Systinet administration utilities consist of command-line tools located in the home directories of each installed server component of SOA Systinet:

- [SSO Server Utilities on page 53](#)
- [Reporting Server Utilities on page 55](#)
- [Platform Server Utilities on page 57](#)
- [Policy Server Utilities on page 61](#)

Some of these utilities are then described individually in chapters:

- [Setup Tool on page 63](#)
- [Update Management Tool on page 67](#)
- [Repository Export Tool on page 69](#)
- [Repository Import Tool on page 71](#)
- [Repository Reset Tool on page 73](#)
- [SSO Configuration Tool on page 75](#)
- [Reporting Import/Export Tool on page 77](#)



If passwords are encrypted, set the option `-Dpassword.encrypted.passphrase=passphrase` on the command-line when you launch any tool that requires authentication. On Windows, the entire option should be in double quotes (" ") and on Unix systems with bash, it should be in single quotes (' ').

8 SSO Server Utilities

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



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

Table 1. Summary of SSO Admin Utilities

Command	Description
configsync	Synchronizes local configuration files with the configuration file on the database.
env-jboss	Called by serverstart to set critical system variables for the application server (see JBoss Server Setup in the HP SOA Systinet Installation Guide for more details).
export [image_directory]	Exports an image of the SSO database to the specified directory.
import [image_directory]	Imports a saved image of an SSO database from the specified directory.
setup	Starts the setup tool to reconfigure the sso server (see Setup Tool on page 63). Use <code>--help</code> to view the available options.
serverstart	Calls env-jboss to set critical system variables and then starts the SSO application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide. Use <code>--help</code> to view the available options.
serverstop	Stops the SSO application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide. Use <code>--help</code> to view the available options.
ssoconfig	Manages SSO entities in the SSO trust domain (see SSO Configuration Tool on page 75). Use <code>--help</code> to view the available options.
updatetool	Called by the setup tool to install updates to the product. Can be used standalone via the command line as described in Update Management Tool on page 67 .

9 Reporting Server Utilities

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


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

Table 2. Summary of Reporting Admin Utilities

Command	Description
<code>env-jboss</code>	Called by <code>serverstart</code> to set critical system variables for the application server (see JBoss Server Setup in the HP SOA Systinet Installation Guide for more details).
<code>importexport</code>	Import data from a local directory or jar file or export data to a given directory (see Reporting Import/Export Tool on page 77).
<code>serverstart</code>	Calls <code>env-jboss</code> to set critical system variables and then starts the reporting application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide . Use <code>--help</code> to view the available options.
<code>serverstop</code>	Stops the reporting application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide . Use <code>--help</code> to view the available options.
<code>setup</code>	Starts the setup tool to reconfigure the reporting server (see Setup Tool on page 63). Use <code>--help</code> to view the available options.
<code>updatetool</code>	Called by the setup tool to install updates to the product. Can be used standalone via the command line as described in Update Management Tool on page 67.

10 Platform Server Utilities

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



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

Table 3. Summary of Platform Admin Utilities

Command	Description
configurationexport <export file>	Exports an image of the configuration table to the specified image file. See Changing the System Configuration on page 46 for specific instructions on procedures using this utility.
configurationimport <export file>	Imports a saved image of the configuration table from the specified image file. See Changing the System Configuration on page 46 for specific instructions on procedures using this utility.
create	Create a resource using the http interface (see the REST Interface section in the HP Systinet Developer Guide).
delete	Delete a specified resource using the http interface and also supports the UNDELETE and PURGE operations (see the REST Interface section in the HP Systinet Developer Guide).
env	A help script to set system variables. We recommend using the setup tool instead.
env-jboss	Called by serverstart to set critical system variables for the application server (see JBoss Server Setup in the HP SOA Systinet Installation Guide for more details).
get	Gets a resource using the http interface with an option to save it to a specified file and also supports the EXIST operation (see the REST Interface section in the HP Systinet Developer Guide).
migrate	Converts an image of the repository data from versions of SOA Systinet prior to 2.50 to an image compatible with this version. See Data Migration on page 35 for details.
repositoryexport	Exports an image of the repository database (see Repository Export Tool on page 69).
repositoryimport	Imports a saved image of the repository database (see Repository Import Tool on page 71).
repositoryreset	Drops and recreates the database and then imports data from a saved image. (see Repository Reset Tool on page 73).
serverstart	Calls env-jboss to set critical system variables and then starts the platform application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide.

Command	Description
serverstop	Stops the platform application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide. Use <code>--help</code> to view the available options.
setup	Starts the setup tool to reconfigure the platform server (see Setup Tool on page 63). Use <code>--help</code> to view the available options. Use <code>--help</code> to view the available options.
update	Update a specified resource using the http interface (see the REST Interface section in the HP Systinet Developer Guide)
updatetool	Called by the setup tool to install updates to the product. Can be used standalone via the command line as described in Update Management Tool on page 67 .

11 Policy Server Utilities

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


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

Table 4. Summary of Policy Admin Utilities

Command	Description
<code>env-jboss</code>	Called by <code>serverstart</code> to set critical system variables for the application server (see JBoss Server Setup in the HP SOA Systinet Installation Guide for more details).
<code>resetvalidationdata</code>	Deletes all compliance reports. It has no specific or required options but it inherits the common ANT script options. By default, <code>resetvalidationdata</code> prompts you to type yes to confirm that you want to delete all reports. You can override the prompt by running <code>resetvalidationdata</code> with the <code>-Dquiet=yes</code> option.
<code>serverstart</code>	Calls <code>env-jboss</code> to set critical system variables and then starts the policy application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide .
<code>serverstop</code>	Stops the policy application server. For production environments we recommend the procedure described in the Launching SOA Systinet section in the HP SOA Systinet Installation Guide . Use <code>--help</code> to view the available options.
<code>setup</code>	Starts the Setup tool to reconfigure the policy server (see Setup Tool on page 63). Use <code>--help</code> to view the available options. Use <code>--help</code> to view the available options.
<code>updatetool</code>	Called by the setup tool to install updates to the product. Can be used standalone via the command line as described in Update Management Tool on page 67 . For most use cases, it is superseded by the Setup tool.

12 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:

- **Default** – change the configuration of SOA Systinet that was set up at installation. This is the *default* use of the setup tool. You can run the setup tool as a GUI wizard or you can use a prepared configuration file. You can also use the UI wizard to create a reusable configuration file. The use is identical to the installation procedure. See the HP SOA Systinet Installation Guide for details.
- **Application Server Change** – change the application server used with the product. HP only recommend using this option in consultation with an HP field engineer.
- **Apply Extensions** – install extensions to SOA Systinet contained in the `PLATFORM_HOME/extensions` directory as described in [Applying Extensions on page 39](#).
- **Apply Updates** – install updates to SOA Systinet, which are downloaded or copied to the `PLATFORM_HOME/updates` directory as described in [Applying Updates on page 43](#).
- **Advanced** – reconfigure individual components of SOA Systinet. This is identical to the **Advanced** installation scenario. See the HP SOA Systinet Installation Guide for details.

The setup tool can also reconfigure the SSO server to use LDAP accounts. See the LDAP Accounts Integration section in the HP SOA Systinet Installation Guide for details.




Note: In SOA Systinet, the platform, Policy Manager, SSO, and reporting servers each have their own setup tools. Their uses are entirely analogous. The instructions for the setup tool apply equally to the platform, policy, and reporting setup tools. Substitute `SSO_HOME`, `PM_HOME`, or `REPORT_HOME` for `PLATFORM_HOME`.


To run the setup tool execute the **setup** script for your OS from `PLATFORM_HOME/bin`. By default, this script runs the UI wizard.

There are a number of options for the **setup** command. List them all by entering **setup --help**:

- Run setup noninteractively with **setup --silent**. In this case, Setup uses a previously generated properties file that contains the installation configuration. You can specify the configuration properties file with the **--use-config** option. Otherwise setup uses `PLATFORM_HOME/conf/setup/configuration-properties.xml`.

 **Important:** When you created the installation configuration properties file, Setup unpacked the installation JAR file into the directory you specified in the GUI. If you want Setup to unpack the JAR to that same location during installation, delete the installation directory you created when creating the configuration file. Setup cannot overwrite an existing installation directory.

- Create and save an installation/setup properties configuration file without executing it by running **setup --save-config config_filename** (give an arbitrary name, or absolute path, in place of `config_filename`). You can use this configuration file later with the **--use-config** option.

 **Note:** When you run setup without this option, the configuration properties are still saved, in the file `PLATFORM_HOME/conf/setup/configuration-properties.xml`. However, this file has the lowest priority when you run setup again. A file you create with the **--save-config** option has the highest priority.

You can use the following options only when running setup in the console, with the `--silent` option:

- Run setup with a prepared configuration file by entering **setup --silent --use-config config_filename**. If you do not specify `config_filename`, the setup tool uses the default `PLATFORM_HOME/conf/setup/configuration-properties.xml` file. Values in this file might be overridden by values in the database configuration table. You can only use a prepared configuration file with noninteractive installation/reconfiguration.

The scenario used to create the configuration file is applied when it is used. For example, if the configuration was saved from an Advanced scenario where the only step was Database Setup, when that configuration file is used again, it will be an Advanced scenario where only Database Setup is executed.

- Choose the setup scenario with the **--scenario scenario_name** option. The possible values for `scenario_name` are as follows:

Default	A complete reinstallation of SOA Systinet over the current installation
Apply Extensions	Installs extensions to SOA Systinet contained in the <code>PLATFORM_HOME/extensions</code> directory
Apply Updates	Installs all available updates, from <code>PLATFORM_HOME/updates</code>

- To force the advanced reconfiguration scenario, where you choose which individual steps of the installation process to execute, use the **--steps** (*comma-separated list of steps*) options. The exact name of each step must be used. These names may differ from the step names used in the installation wizard, as follows:

Name	Installation Step
Password Encryption Setup	Password Encryption Setup
RDBMS Setup	Database Setup
CFG_DB_Setup	Configuration Table Setup
Server Properties	Endpoint Properties
SSO SP Creation	SSO Identity Setup
Repository Import	Repository import
uiPerspectiveImport	UI Perspective Import
Reporting Client Setup	Reporting Server Connection
Application server (JBoss only)	Application Server Properties
Create datasource (JBoss only)	Datasource Setup
Application Server SSL setup (JBoss only)	SSL Setup
Create JMS queue (JBoss only)	JMS setup
SMTP_Properties	SMTP Properties
Ear_Processing	All Extensions steps

Name	Installation Step
Enterprise Application deployment (JBoss only)	Deployment
Client_Package	Client Package Creation

- Display debug information with **--debug**.

Examples:

setup(.sh) --save-config config.xml runs the Setup UI wizard and saves the results as the configuration file `config.xml`, in the same directory as the Setup tool script (`PLATFORM_HOME/bin` by default. If you wanted to save the file in `PLATFORM_HOME/conf/setup`, like the default configuration file, you would run **setup(.sh) --save-config ../conf/setup/config.xml**. This command does not perform the `setup.config`

setup(.sh) --silent --use-config ../conf/setup/config.xml executes the previously created reinstallation configuration file `PLATFORM_HOME/conf/setup/config.xml`.


setup(.sh) --silent --use-config ../conf/setup/config.xml --steps "RDBMS Setup" only executes the **Database Setup** step from the installation configuration at `PLATFORM_HOME/conf/setup/config.xml`.

setup(.sh) --silent --use-config ../conf/setup/config.xml

setup(.sh) -Dpassword.encryption.passphrase=*myPassphrase* --silent --use-config ../conf/setup/config.xml executes the previously created reinstallation configuration file `PLATFORM_HOME/conf/setup/config.xml` where passwords have been encrypted with the passphrase `myPassphrase`.

13 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.

 **Note:** This tool should only be used when the setup tool is unavailable or undesirable.

Note: In SOA Systinet, the platform, Policy Manager,, SSO, and reporting servers each have their own updatetools. Their uses are entirely analogous. The instructions for the updatetool apply equally to the platform, policy, and reporting updatetools. Substitute SSO_HOME, PM_HOME or REPORT_HOME for PLATFORM_HOME.

HP Systinet delivers the update in the form of an `update-jar` file. Copy it to the `PLATFORM_HOME/updates` folder.

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


updatetool [OPTION]

no option lists the upgrades that are available

`-l, --list` lists the currently installed updates

`-i, --install` installs the updates in the `updates` directory

`-u, --uninstall update-name` uninstalls the named update. This update must be the latest installed.

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

Any extensions must be reapplied as described in [Applying Extensions on page 39](#).

14 Repository Export Tool

The **repositoryexport** tool exports the following into an image in the specified location:

- All resource data and metadata
- Configuration files

The command line is:

```
repositoryexport -i image | -z zip [ option ...]
```

The options are:

- s silent mode which does not report progress
- q quiet mode which does not request confirmation



Important: SOA Systinet must not be running while running this script.

15 Repository Import Tool

The **repositoryimport** tool is used to import an image of the repository into the database.

The command line is:

```
repositoryimport [ option ...]
```

The options are:

`-i image` | `-url url` | `-z zip` path on the local filesystem or a URL location of an image or zipped image to import

`-s` silent mode which does not report progress.

`-q` quiet mode which does not request confirmation.

`--ignore` if an imported resource is already in the database the imported version is ignored.

`--force` if an imported resource is already in the database, it is overwritten.

`--bootstrap` import the image in bootstrap format.

`--update-blacklist` append imported resources to the migration blacklist, useful for bootstrap installation.

`--reset-blacklist` save imported resources to the migration blacklist.

`--ignore-sdm-merge-warn` does not abort if SDM merge check reports warnings only.

`--migrate` perform online phase of the migration process at the end of the import



Important: SOA Systinet must not be running while running this script.

Important: After using `repositoryimport` you must refresh the database indexes to reflect the new data. Refer to your database product documentation for details or see the *Configuring the Database for Full Text Searching* section of the *HP SOA Systinet Installation Guide*.

16 Repository Reset Tool

The **repositoryreset** tool executes the following operations:

- Drops the database.
- Creates a new database.
- Imports data (default or from an external location)

The command line is:

```
repositoryreset [ option ...]
```

The options are:

- s silent mode which does not report progress
- q quiet mode which does not request confirmation



Important: SOA Systinet must not be running while running this script.

Important After using repositoryreset you must refresh the database indexes to reflect the new data. Refer to your database product documentation for details or see the Configuring the Database for Full Text Searching section of the HP SOA Systinet Installation Guide.

17 SSO Configuration Tool

The **ssoconfig** command manages SSO entities in the SSO trust domain.

The ssoconfig tool can be used for the following operations:

- Obtaining a list of SSO descriptors for all the partners in the domain as described in [Partner Affiliations on page 37](#).
- Downloading and modifying SSO partner descriptors as described in [Modifying SSO Descriptors on page 37](#).

The syntax for ssoconfig is:

```
SSO_HOME/bin/ssoconfig [ACTION] [-f FILE | -e ENTITY_ID | -d DIR] [-s SSO_CONFIG_SERVICE_URL] -u ADMIN_USERNAME -p ADMIN_PASSWORD
```

Where *ACTION* is one of:

get	Downloads either a single entity configuration (if -e option is used) or all entity configurations to the specified directory
create	Creates a new SSO entity configuration
update	Updates an existing SSO entity configuration
delete	Deletes an existing SSO entity configuration

The remaining options are:

-f, --file	The path to the file, where the entity configuration is stored
-e, --entity-id	The entity ID of the managed entity
-d, --dir	The output directory for entity configurations
-s, --server-url	The URL of the SSO server

-u, --username	The administrator name for the SSO server
-P, --password	The password for the SSO server

Examples:

ssoconfig get -d partners/ip -e ip -s http://localhost:8080/sso -u admin -p ch angeit outputs the SSO descriptor of the partner called ip to the directory `partners/ip`.

ssoconfig get -d partner -s http://localhost:8080/sso -u admin -p changeit outputs all SSO descriptors to the directory `partner`.

ssoconfig create -f new_entity.xml -s http://localhost:8080/sso -u admin -p ch angeit creates a new SSO partner based on the content of `new_entity.xml`.

ssoconfig update -f newer_entity.xml -s http://localhost:8080/sso -u admin -p changeit updates an SSO partner with the content of `newer_entity.xml`.

ssoconfig delete -e platform -s http://localhost:8080/sso -u admin -p changeit deletes the platform SSO partner.

18 Reporting Import/Export Tool

The **importexport** command enables you to export the data in the reporting database to an image and then import that data at a later date.

The syntax for importexport is:

importexport [OPTION] [IMPORT_DIR | IMPORT_JAR | EXPORT_DIR]

With options:

-i, --import <i>import_path_or_jar</i>	The path to the file where the image is stored
-e, --export <i>path</i>	The path to save the exported data image
-f, --force	If the imported resource is already in the database then overwrite it
-q, --quiet	Execute the command with less feedback
-l, --logfile <i>logfile</i>	Create a log file containing the feedback of the execution

Examples:

importexport --import com.systinet.reporting.ext.policymgr.2.5.jar Imports the data from the jar file to the reporting database.

importexport --import /opt/systinet/reporting/data/exported Imports the data from the image file to the database

importexport --export C:\systinet\reporting\data\exported Creates an image of the reporting database at the specified location

Index

A

- access
 - rights, 19
- ACL
 - configuration, 48
 - editing, 19
- artifact
 - security, 19
- authorization
 - groups, 45

C

- configuration
 - tool, 63
- customization
 - SDM, 35

D

- data
 - migration, 35
- deploy
 - extension, 39

E

- extension
 - deployment, 39

I

- import

- extension, 39
- registry certificate, 28

L

- LDAP
 - groups, 45
 - login, 45
- login
 - groups, 45

M

- migration
 - data, 35
 - SDM, 35

P

- permissions
 - assigning, 19

R

- registry
 - certificate import, 28
- repositoryexport
 - tool, 69
- repositoryimport
 - tool, 71
- repositoryreset
 - tool, 73
- rights
 - access, 19

S

- SDM
 - customization, 35
 - migration, 35
- security

- permissions, 19
- SiteMinder, 48
- SSO
 - configuration, 75, 77
 - partner, 37
 - domain, 37
 - new URL, 37
- ssoconfig
 - tool, 75, 77
- synchronize
 - taxonomy, 28

T

- taxonomy
 - synchronization, 28
- tool
 - configuration, 63
 - setup, 63
 - update, 67
- tools
 - repositoryexport, 69
 - repositoryimport, 71
 - repositoryreset, 73
 - ssoconfig, 75, 77

U

- update management
 - tool, 67