HP Systinet

Software Version: 4.10

Installation and Deployment Guide

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.

Copyright Notice

© Copyright 2003 - 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document 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

Visit the HP Software Support Online web site at:

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

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support 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 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 register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Chapter 1

In this Guide

This guide describes how to set up an environment and deploy HP Systinet to it.

Tip: An alternative interactive installation guide is available. This guide enables you to select your deployment environment and installation options and then view only the installation and deployment instructions relevant to you. To view the guide open the `Interactive_ Install.htm` file alongside this PDF on the installation media.

This guide contains the following chapters:

- "Prerequisites and Supported Platforms" (on page 12)

  Design your environment for HP Systinet.

- "Preparing Databases" (on page 19)

  Set up and configure your database for Systinet.

- "Setting Up Application Servers" (on page 29)

  Configure your application server for Systinet.

- "Preparing LDAP and SiteMinder" (on page 69)

  Set up LDAP and SiteMinder for Systinet.

- "Using the GUI Installer" (on page 72)

  Use the GUI Installer to install Systinet.

- "Deploying Systinet" (on page 116)

  Configure your environments and deploy Systinet.

- "Upgrading HP SOA Systinet" (on page 137)

  Migrate extensions and data from previous versions of Systinet.

- "Starting and Configuring Systinet" (on page 142)

  Start Systinet and perform UI-based final configuration.

Chapter 2

Prerequisites and Supported Platforms

Before installing HP Systinet you must make sure that the environment you want to install to is appropriate and suitable for your needs.

The following sections describe the requirements and options available:

Design Your Deployment

- **Development**

  If you are a developer, CIO, or other IT manager who wants to learn the functions of Systinet, this is the correct type of deployment for you. It should be on one machine and preferably on one J2EE server instance. The simplest approach is to deploy Systinet to the JBoss application server.

  Use the installation wizard to deploy the product to JBoss, following the default settings. Server configuration for JBoss is handled within this wizard and in the serverstart and serverstop scripts.

  If you use an application server other than JBoss, the installation wizard creates an EAR file, which you then deploy using the application server tools. You must also modify server classpaths, configure JMS, and set Java properties yourself.

- **Production**

  Deploying Systinet for use in a production environment is complex. Systinet is likely to be clustered and linked to a database and directory service on separate machines. If you are

creating such a deployment, you should already have a set of tools and procedures for deploying J2EE applications and managing relational databases.

When you deploy Systinet to a production environment, you may need additional configuration options that are not available in the GUI installer.

Prerequisites - Hardware

Distributed production environments require the following hardware:

- For each physical node, an Intel Xeon processor, 8 GB RAM, 4 GB disk space, 1000 Mbit/s network, network bandwidth of 1 Gb/sec or higher.

Example Configuration:

For a production environment with 500 concurrent users, HP recommends the following minimum example configuration:

- HP ProLiant BL280c G6 E5506 2G (1P)

- Intel® Xeon® E5506 (4 core, 2.13 GHz, 4 MB L3, 80W)

- 8GB RAM – assuming 64-bit OS and JDK

- HP 60GB 1.5G SATA 5.4K SFF HDD - 379306-B21

- 1GbE NC362i 2 Ports

For larger configurations, extend the deployment appropriately or consult HP Professional Services.

Warning: SPARC machines are not suitable for Systinet deployments.

For development and evaluation purposes, Systinet can run on a single machine, even on a notebook.

The hardware requirements in this case are:

- Intel Core 2 Duo processor, 4 GB RAM, 3 GB free disk space, a 64 bit operating system and a network card that supports 100 Mb/sec.

- Network bandwidth of 100Mb/sec or higher.

- Finalized installation requires 3GB of disk space with the admin requiring twice as much in order to effectively work with deployments; approximately 6GB of dedicated HDD space . Admin must also account for up to 2GB for JBOSS and database engine.

Prerequisites - JDK Software

Each machine runningHP Systinet requires a Java SE Development Kit (JDK) and your selected Java 2 Platform Enterprise Edition (J2EE) application server. The application server must use this JDK.

HP Systinet supports the following JDKs:

- Oracle (Sun) JDK 1.6

- HP JDK 1.6

- IBM JDK 1.6

Caution: HP recommends using a 64-bit operating system in conjunction with a 64-bit JDK. 32-bit operating systems may not provide sufficient memory for this version of HP Systinet.

The JAVA_HOME environment variable must be set to point to the Java JDK used by the host J2EE application server.

To Ensure the Correct JDK is Used:

1. Open a command prompt (cmd in Windows) or a terminal session (UNIX/Linux).

2. Execute echo %JAVA_HOME% (Windows) or echo $JAVA_HOME (UNIX/Linux)

3. Do one of the following:

   - If JAVA_HOME points to JDK 1.6 then proceed with installation.

   - If JAVA_HOME does not point to JDK 1.6 then reset the JAVA_HOME environment variable to a valid JDK 1.6.

Warning: If you have both a JDK and JRE installed, JAVA_HOME must point to the JDK.

Recommended Environments

HP recommends the following environments:

- Weblogic, Oracle DB, Oracle (Sun) JDK

- JBoss EAP, Oracle DB, Oracle (Sun) JDK

- WebSphere, IBM DB2, IBM JDK

Supported Database Types

Systinet supports the following databases:

- Oracle 10.2.0.4

- Oracle 11g (11.1.0.6.0)

- Oracle 11g (11.2.0.3.0)

- Microsoft SQL 2005 (SP2)

- Microsoft SQL 2008 (SP2)

- DB2 9.1 (Fix Pack 5)

- DB2 9.7 (Fix Pack 2)

HP Systinet supports deployment to the following database and driver combinations:

Supported Database Drivers

Database	DB Version	Driver Packages	Driver Version	Driver Class
Oracle Database	10.2.0.4	ojdbc14.jar, orai18n.jar	10.2.0.4	oracle.jdbc.driver. OracleDriver
	11.1.0.6	ojdbc6.jar, orai18n.jar	11.1.0.6	

Database	DB Version	Driver Packages	Driver Version	Driver Class
	11.2.0.3.0	ojdbc6.jar, orai18n.jar	11.2.0.3.0	
IBM DB2*	9.1 (FP 5)	db2jcc.jar, db2jcc_license_cu.jar	3.7.73	com.ibm.db2.jcc.DB2Driver
	9.7 (FP 2)			
Microsoft SQL Server	2005 SP2 (9.00.3042)	sqljdbc.jar	1.2	com.microsoft.sqlserver.jdbc. SQLServerDriver
	2008 SP2 (10.00.4000.00)	sqljdbc4.jar	3.0	

Caution: For both versions of DB2, use the drivers supplied with 9.1. Drivers from 9.7 cause exceptions such as "The database returned no natively generated identity value."

Note: The next major release of HP Systinet after 4.10 will discontinue support of the IBM DB2 database.

Supported Application Servers

Systinet can be deployed to the following application servers:

- Oracle WebLogic Server 11g R1

- Oracle WebLogic Server 10g R3

- IBM WebSphere 7.0.0.7

- JBoss 5.1 GA

- JBoss EAP 5

- JBoss 4.2.2 GA

- JBoss EAP 4.3.0

Note: The next major release of HP Systinet after 4.10 will discontinue support of the IBM WebSphere and Oracle WebLogic application servers.

Prerequisites - Operating Systems

The server running Systinet must use a supported operating system. For a list of supported operating systems please refer to the documentation of the application server of your choice.

HP recommends the following operating systems:

- Windows 2003 and Windows 2008

- Linux (RedHat or Suse)

- HP-UX

- AIX

- Solaris

Caution: HP recommends using a 64-bit operating system in conjunction with a 64-bit JDK. 32-bit operating systems may not provide sufficient memory for this version of Systinet.

Prerequisites - Browsers

Client machines accessing Systinet must use a supported browser. Systinet supports the following browsers:

- Microsoft Internet Explorer 8 and 9

- Mozilla Firefox 20

Prerequisites - Mail Clients

If you want HP Systinet to send automatic notifications, you must use a supported mail client. HP Systinet supports the following mail clients:

- Microsoft Outlook 2003 and 2007

- Mozilla Thunderbird 2

- GMail

Supported LDAP Implementations

When you install HP Systinet, you can select to use an external LDAP server to retrieve information about users and groups.

HP Systinet uses LDAP for authentication and to obtain user and group information.HP Systinet accesses this information as read-only and never modifies it.

HP Systinet supports the following LDAP implementations:

- Sun ONE Directory Server 5.2

- Sun Java System Directory Server 6.3

- Microsoft Windows Server 2008 Active Directory

Prerequisites - Adobe Flash

Client machines accessing Systinet require Adobe Flash Player version 10.0 or newer.

Supported Product Integrations

HP Systinet supports integration with the following products:

Product	Version	Features
UDDI Registry	v3	Import/export/synchronize data. Import/Export taxonomies (HP SOA Registry Foundation only).

Product	Version	Features
HP Business Service Management (BSM)	9.13, 9.20, 9.21	uCMDB service discovery. Service entry to governance/synchronization. BSM health report monitoring. **Note**: HP Business Availability Center (BAC) 8.02 is no longer supported.
HP Universal CMDB 9.05	9.05	uCMDB service discovery. Service entry to governance/synchronization.
HP Application Lifecycle Management	11.5	Service test monitoring for ALM 11.5
Layer7	6.1, 7.0	
DataPower	5.0.0.-5	

Deploying to Environments without a JDK

The HP Systinet installation framework supports deployment of HP Systinet to production environments that cannot use a JDK, but only a JRE.

In order to achieve this, two deployments are necessary, a staging environment called `Build` and a production environment called `Target`. The user responsible for installation is required to apply updates and extensions, and to compile JSPs on the Build machine that must use a JDK. Once the Build machine customization is complete, the results are transferred to the Target deployment.

This scenario requires a Build machine as the staging environment and a Target Deployment as the production environment.

The Build environment should mimic the Target deployment as much as possible:

- Install the application server and HP Systinet to the same folders as required for the Target.

- Install the same version of the JDK as the JRE version on the target deployment. `JAVA_HOME` can differ from the Target deployment environment variable.

- The Build machine must use the same OS family as the Target deployment. This is required to generate compatible start scripts.

Note: This process has been tested with JBoss only.

Note: When installing and setting up the application server in the Build environment:

- For WebLogic domain, enter the full hostname (including domain) and port numbers for the target environment.

- When possible (JBoss and WebLogic), it is useful to install the application server to the same folder where you intend to install HP Systinet.

Chapter 3

Preparing Databases

This section describes database administration tasks for HP Systinet. The database administrator must perform tasks at the time of installation and may also have tasks when HP Systinet is updated, extensions are applied, or data is migrated.

Before you can install HP Systinet the database administrator must set up the database.

Read "Database Installation Types" (on page 19) first for information about the different database installation scenarios which vary according to the required level of access to the database.

Note: Database administrators must make sure that common users are granted permissions in new tables.

Caution: For performance reasons, HP recommends verifying the network performance between the location of the application server and the location of the database. Check the traceroute to the database; HP recommends a maximum response time of 10ms, 1 hop is optimum, 2 hops is ok.

The database specific sections describe database specific prerequisites and procedures describing how to create the various user types required by the different database installation scenarios.

- "Set Up Oracle Database" (on page 20)
- "Set Up IBM DB2" (on page 23)
- "Set Up Microsoft SQL" (on page 25)

Database Installation Types

- **Create Schema**

  The Create Schema option, available in the GUI installer and command-line deployment, creates tables and indexes in the default schema in an existing database or tablespace provided by the database administrator. Select this method if you have an account in a database with an empty schema (recommended) and privileges to create tables and indexes.

  Note: In this document, power user refers to users with the privilege to create tables and indexes.

- **Create Database / Tablespace**

  The option to create a database or tablespace is available in the GUI installer and command-line deployment. This option automates database arrangement as much as possible, but requires database administrator credentials. The process creates users, the database or tablespace depending on your database type, and continues with the creation of the schema.

  There are some differences in the create database process depending on the database type:

  - **IBM DB2**

    This option requires an existing database, OS user, and database administrator credentials.

This option does not create a new physical database. It creates a tablespace in an existing database to separate repository data. The user is then granted privileges to use the tablespace, create tables, and connect to the database.

- **Microsoft SQL**

  This option requires an existing user with the database creator role.

  This option creates a new physical database with collation inherited from the server settings.

- **Oracle Database**

  This option requires an existing database and database administrator credentials.

  This option does not create a new physical database. It creates a new tablespace to hold Systinet data separately and creates a new database account which uses the new tablespace as its default tablespace.

- **Manual Database Arrangement**

  The database administrator may want to arrange the database manually:

  - In some cases, the database administrator (DBA) cannot share the DBA credentials required for the Create Database option or the power user credentials for the Create Schema option.

  - In some cases, the database administrator may want to amend the default DDL scripts. For example, to create indexes in a separate tablespace.

  In these cases, the database administrator must perform the database related installation operations manually as part of Decoupled Database Installation.

  Typically the database administrator creates a power user account for the Systinet schema and a common user account with minimal privileges to insert, select, update, and delete SQL operations in power user tables.

  The database administrator does not distribute the power user credentials and provides the common user credentials to the Systinet administrator to configure the application server datasource.

Set Up Oracle Database

Configure the Oracle database as follows for use with Systinet:

- If you are upgrading from Systinet 3.x, use a new database. Using the same database as the previous version will lose your data.

- If you are clustering Oracle database (RAC), you must use Oracle Database 10.2.0.4 or higher. Systinet does not support RAC in earlier versions.

- Systinet installation requires a JDBC driver:

Database	DB Version	Driver Packages	Driver Version	Driver Class
Oracle Database	10.2.0.4	ojdbc14.jar, orai18n.jar	10.2.0.4	oracle.jdbc.driver.OracleDriver
	11.1.0.6	ojdbc6.jar, orai18n.jar	11.1.0.6	

Note: It is highly recommended that thin drivers are used as opposed to OCI drivers due to significant performance increase and easier configuration.

- To use Systinet Full Text Search, include the "Oracle Text" extension when installing the Oracle server. The "Oracle Text" extension is applied to Oracle by default.

- HP strongly recommends creating a database that uses the Unicode for Database Character Set (NLS_CHARACTERSET=AL32UTF8). If you use a non-Unicode database, you may encounter problems storing and searching some national characters outside your character set. Changing the character set after installation is only possible by creating a new database.

- HP recommends setting the `cursor_sharing` parameter to `FORCE` to improve performance and economize shared pool usage.

- If exception `'ORA-01425: Escape character must be string of length 1'`, set `cursor_sharing=EXACT` or request a patch from Oracle for bug #9689594 suitable for your system.

- Create accounts based on the database installation type selected for Systinet installation. The access required is defined by the database installation type:

  - For the Create Database option an account is created by the installer.

  - For the Create Schema option, if you want to separate the Systinet data (recommended), create a tablespace in the database. Create a power user to own the schema, with the new tablespace as its default tablespace.

  - For Manual Database Arrangement create a tablespace in the database, create a power user account to own the schema, with the new tablespace as its default tablespace. Optionally, create a common user account with minimal privileges.

Caution: If you are using Oracle DB with a UNIX 64-bit operating system (including Linux), a TNS-12535 error may occur during installation. This error occurs due to a problem with the random pool. Fix the problem by adding `/sbin/rngd -r /dev/urandom -o /dev/random -t 55` to `/etc/rc.d/rc.local`.

Tip: HP recommends the following free Oracle (performance) troubleshooting tool: AWR (Automatic Workload Repository) reports. These reports must be generated by the database administrator.

If required, see the following sections for additional Oracle setup details:

Set Up an Oracle Power User

In order to use the Create Schema option during installation or for Manual Database Arrangement, the database administrator should create a *power user* with appropriate privileges to the database.

To Set Up a Power User in Oracle:

1. HP recommends creating a new tablespace to hold Systinet data.

2. Create an account that can create schema items, with the new tablespace as its default

tablespace.

3. Grant privileges to the account to connect to the database and create tables, indexes, and sequences.

4. Optionally, grant the account the privilege to execute **"CTXSYS"."CTX_DDL"**.

   This privilege is a precondition for using the Systinet full-text search feature on the database.

Set Up an Oracle Common User

In cases where the database administrator restricts access to the database to just select, insert, update, and delete operations, Systinet requires a user with these privileges.

Note: The Systinet schema must exist before you create the common user.

To Set Up a Common User in Oracle:

1. Save the following SQL statements to the `script.sql` file:

```
set pagesize 0;
set pagesize 0;
set line 200;
set verify off
set feedback off
spool ./grant.sql
SELECT 'GRANT INSERT, UPDATE, DELETE, SELECT ON ' || table_name ||
' TO &2;' FROM user_tables;
SELECT 'GRANT SELECT ON ' || sequence_name || ' TO &2;' FROM user_
sequences;
spool off
spool ./synonyms.sql
SELECT 'CREATE SYNONYM ' || table_name || ' FOR &1' || '.' ||
table_name || ';' FROM user_tables;
SELECT 'CREATE SYNONYM ' || sequence_name || ' FOR &1' || '.' ||
sequence_name || ';' FROM user_sequences;
spool off
```

These statements generate scripts to set the environment, grant rights and create synonyms.

2. Connect to the database as the *power_user* and execute `script.sql` to produce the scripts `grant.sql` and `synonyms.sql`. Then execute `grant.sql`.

```
sqlplus power_user/password@SID
-- generate grant and create synonym statements
@script.sql power_user common_user
-- execute grant.sql
@grant.sql
exit
```

3. As the *common_user*, execute `synonyms.sql`.

```
sqlplus common_user/password@SID
-- execute synonym.sql
@synonyms.sql
exit
```

Set Up Oracle for WebSphere

Configure the Oracle Database to support WebSphere with XA transactions over Oracle datasources.

As user SYS, run the following commands on your Oracle server:

```
grant select on pending_trans$ to public;
grant select on dba_2pc_pending to public;
grant select on dba_pending_transactions to public;
grant execute on dbms_system to <user>;
```

Set Up IBM DB2

You can use Systinet with an IBM DB2 database. The database requires set up and configuration prior to installing Systinet.

To Configure DB2 Database for Use With Systinet:

1. If you are upgrading from HP SOA Systinet 3.x, use a new database. Using the same database as the previous version will lose your data.

2. If you plan to use the Systinet full text search feature, make sure the optional DB2 Net Search Extender is installed.

3. Systinet installation requires a JDBC driver:

Database	DB Version	Driver Packages	Driver Version	Driver Class
IBM DB2	9.1 (FP 5)	db2jcc.jar, db2jcc_license_cu.jar	3.7.73	com.ibm.db2.jcc.DB2Driver
	9.7 (FP 2)			

   Caution: For version 9.7, use the drivers supplied with 9.1. Drivers from 9.7 cause exceptions such as "The database returned no natively generated identity value."

4. If one does not exist, create a database that uses the UTF-8 Code Set.

   If it does not exist, you should create two tablespaces with a 32kB page-size:

   "**Regular**" - this is where user data is stored and you use this tablespace during installation.

   "**System temporary**" - Do not use this name in the installation wizard.

   Create a bufferpool "HPSYSBP" (32kB page-size) and a _system temporary_ tablespace "HPSYSTS" (32kB page-size) that uses the "HPSYSBP" bufferpool.

   Create a _regular_ tablespace "HPSYSDATATS" (32kB page-size) that also uses the "HPSYSBP" bufferpool.

   Check the *Enable self tuning* option and use the "HPSYSDATATS" tablespace when installing SOA.

5. To ensure the successful import or export of large data images HP recommends increasing the log file size (*LOGFILSIZ*) parameter to 2048 or higher and the number of primary log files

(*LOGPRIMARY*) parameter to 15 or higher.

To ensure that there is sufficient memory HP recommends increasing the application heap size (*APPLHEAPSZ*) parameter to 1024 or higher.

6. Increase value of the `stmtheap` property to 16400 or more to avoid following exception:

   com.ibm.db2.jcc.b.SqlException: DB2 SQL error: SQLCODE: -101, SQLSTATE: 54001, SQLERRMC: null

7. Create an OS user account to hold the Systinet data.

8. Create accounts based on the database installation type:

   - For the Create Database option no additional manually created accounts are required.

   - For the Create Schema option, create a power user.

   - For Manual Database Arrangement, create a power user account to own the schema, create the schema manually, and create a common user account with minimal privileges.

9. If it does not already exist, create a *user temporary tablespace*. Grant use of the tablespace to the database (common) user.

If required, see the following sections for additional DB2 setup details:

- "Set Up a DB2 Power User" (on page 24)

- "Set Up a DB2 Common User" (on page 24)

- "Troubleshooting DB2" (on page 25)

Set Up a DB2 Power User

To use the Create Schema option during installation or Manual Database Arrangement, the database administrator should create a *power user* with appropriate privileges to the database.

To Set Up a Power User in DB2:

1. Create a tablespace using the 32k page-sized bufferpool to hold Systinet data.

2. Grant CONNECT, CREATETAB, and IMPLICIT_SCHEMA privileges to the user account.

3. Grant use of the tablespace to the OS user account.

Set Up a DB2 Common User

In cases where the database administrator restricts access to the database to just select, insert, update, and delete operations, Systinet requires a user with these privileges.

Note: The Systinet schema must exist prior to creating the common user.

To Set Up a Common User on DB2:

1. Create an OS account for the common user.

2. Grant the common user connection privileges:

```
GRANT CONNECT ON DATABASE TO common_user
```

3. Open the DB2 Command Editor and connect to the database using *power user* credentials.

4. Generate a list of commands granting privileges to database tables to the common user with the following command:

```
SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON TABLE ' || TABNAME
|| '
       TO common_user;' FROM syscat.tables
       WHERE LOWER(tabschema) = LOWER('power_user')
```

5. After the results display, click **Fetch More Rows** at least twice until all rows are displayed.

6. Select all the resulting commands and copy them to the clipboard.

7. In the Commands window, paste the clipboard contents.

8. Execute the commands.

9. Generate a list of commands to create aliases for the tables with the following command:

```
SELECT 'CREATE ALIAS ' || TABNAME || ' FOR power_user.'
     || TABNAME || ';' FROM syscat.tables
     WHERE LOWER(tabschema) = LOWER('power_user')
```

10. After the results display, click **Fetch More Rows** at least twice until all rows are displayed.

11. Select all resulting commands and copy them to the clipboard.

12. Open a new instance of DB2 Command Editor and connect to the database using the *common user* credentials.

13. In the common user Commands window, paste the clipboard contents.

14. Execute the commands.

Troubleshooting DB2

If an error with `SQLCODE -670` ("The row length of the table exceeded a limit of <length> bytes. (Table space <tablespace-name>.)") occurs during the schema creation process, your tablespace uses a bufferpool with an insufficient page size.

To resolve this error, use tablespace (and bufferpool) with 32kB long page. If you already have 32kB page size use one of following methods:

- In the SDM model: Change the SDM model extension to not include so many long properties - remove useless properties and/or decrease the size of the datatype.

- In the database: Use decoupled installation (Manual Database Arrangement), where the DBA manually creates the database schema. The DBA can reduce column sizes if applicable. Varchar columns that contain user specified data (such columns are typed as NVARCHAR in Oracle/MS SQL schemas) are sized to contain strings of the specified length using 3-byte characters in UTF-8 encoding. The size of such varchar columns in bytes is three times greater than the size of the property in characters. If you ensure (or at least expect) that only 1-byte characters are stored, you can decrease the size of such fields by a factor of 3. Alternatively, you can decrease the size of the most space consuming properties/columns such as descriptions, etc.

Set Up Microsoft SQL

You can use Systinet with a Microsoft SQL database. The database requires set up and

configuration prior to installing Systinet.

1. If you are upgrading from Systinet 3.x, use a new database. Using the same database as the previous version will lose your data.

2. Use SQL Server Configuration Manager to enable the TCP/IP protocol and use a static port (for example 1433).

3. Systinet installation requires a JDBC driver:

Database	DB Version	Driver Packages	Driver Version	Driver Class
Microsoft SQL Server	2005 SP2 (9.00.3042)	sqljdbc.jar	1.2	com.microsoft.sqlserver.jdbc. SQLServerDriver
	2008 SP1 (10.0.2531.0)	sqljdbc4.jar	3.0	

4. Systinet requires XA transactions support. For details about setting up XA transaction support, go to the following location:

http://msdn2.microsoft.com/en-us/library/aa342335.aspx

5. If you want to use the full-text search feature in Systinet, make sure that the Full-Text Search engine is installed together with the database engine during the installation of MSSQL Server.

6. Create a login in the database server to hold Systinet tables in the database. The login must have the *database creator* role.

   The login must be able to access the master database for XA related stored procedures:

   - Create a user in the master database for the login.

   - Assign the SqlJDBCXAUser role to the account.

7. Create users based on the database installation type selected for the HP Systinet installation:

   - For the Create Database option the installer uses the login to automatically arrange the database.

     The created database inherits collation from the MSSQL server default collation. Systinet requires case-sensitive collation. Use a server with case-sensitive collation or manage database collation manually using the Create Schema option.

   - For the Create Schema option, if you want to separate the Systinet data (recommended), use the login to create a database. The database must have case-sensitive collation.

     Note: You can create the database on behalf of another account or use an existing account with an existing database, but you must then grant create table privileges to the new account or the existing account.

     The installer uses the login to create the schema in this new database.

   - For Manual Database Arrangement, use the power user login to create the database with case-sensitive collation. Then create the schema manually, and optionally create a common user account with minimal privileges.

Note: If you intend to use user accounts and group names in HP Systinet that contain non-Latin characters, you must specify an appropriate collation on the database that supports such non-Latin characters.

Note: To prevent some possible deadlocks, HP recommends executing the following statement:
ALTER DATABASE [database_name] SET READ_COMMITTED_SNAPSHOT ON;

To setup/install Systinet with integrated security:

1. (Prerequisite) Copy the `sqljdbc_auth.dll` file to a directory on the Windows system path (%PATH%) on the computer where the JDBC driver is installed.

   If you are running a 32-bit Java Virtual Machine (JVM), use the `sqljdbc_auth.dll` file in the x86 folder, even if the operating system is the x64 version. For details, see
   http://msdn.microsoft.com/en-us/library/ms378428
   [(v=sql.105).aspx#Connectingintegrated](v=sql.105).aspx#Connectingintegrated).

   Note: In Systinet 4.x, the native library directory of JRE used by Systinet (and the application server) should be used for the `sqljdbc_auth.dll` file and the JDBC driver. This means that the `sqljdbc_auth.dll` file should be put in `JAVA_HOME/jre/bin`, and the driver JAR (`sqljdbc4.jar`) should be put in `JAVA_HOME/jre/lib/ext`, respectively.

2. Set up the database and user account manually and select **Create schema** during the installation.

3. Supply a database name with the `;integratedSecurity=true` suffix in the **Database Setup** step.

   Note: There is no need to specify the JDBC driver jar, it is already part of your JDK/JRE when step 1 is done properly; you can leave the field empty.

4. You may be warned by the installer about a failed **XA transaction detection**. Ignore this message and use Systinet self-test to check the XA transaction setup.

   If the validation of the installer shows an error message such as `"This driver is not configured for integrated authentication."`, this means that the DLL in step 1 was not found. Check and make sure that the DLL and JAR files in step 1 have been configured as described.

If required, see the following sections for additional MSSQL setup details:

-

Set Up an MSSQL Common User

In cases where the database administrator restricts access to the database to just select, insert, update, and delete operations, Systinet requires a user with these privileges.

To Set Up a Common User in MSSQL:

1. Open Microsoft SQL Server Management Studio or the sqlcmd command-line editor.

2. Create a common user login in the server and user in the database created for Systinet (systinetdb).

   For example, execute the following statements:

```
USE [master]
GO
CREATE LOGIN [common_user] WITH PASSWORD=N'...', DEFAULT_DATABASE=
[master],
CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF
GO
USE [systinetdb]
GO
CREATE USER [common_user] FOR LOGIN [common_user]
GO
```

3. Grant rights to the common user to read and write to Systinet tables.

   For example, execute the following statements:

```
USE [systinetdb]
GO
EXEC sp_addrolemember N'db_datawriter',N'common_user'
GO
USE [systinetdb]
GO
EXEC sp_addrolemember N'db_datareader', N'common_user'
GO
```

4. The login must be able to access the master database for XA related stored procedures.

   Create a user in the master database for the login and add the user to the SqlJDBCXAUser role.

   For example, execute the following statements:

```
USE [master]
GO
CREATE USER [common_user] FOR LOGIN [common_user]
GO
USE [master]
GO
EXEC sp_addrolemember N'SqlJDBCXAUser', N'common_user'
GO
```

Chapter 4

Setting Up Application Servers

HP Systinet is deployed to J2EE application servers. Each different application server must be set up prior to HP Systinet installation.

"Deploy Systinet Self-Test" (on page 29) describes the use and deployment of an environment verification tool for use during installation and deployment.

The set up of each application server is explained in the following sections:

- "Setting Up JBoss" (on page 31)
- "Setting Up WebLogic" (on page 44)
- "Setting Up WebSphere" (on page 55)

Deploy Systinet Self-Test

For production deployments, you may want to verify significant milestones of the installation and deployment.

Self-Test is a tool that checks various aspects of deployment. It can be used during the setup of particular resources on an application server such as data sources, JNDI, and JMS which are required for the successful deployment of Systinet.

The package is prepared as a standalone application for deployment to application servers.

To Deploy Self-Test as a Standalone Application:

1. Extract the Systinet installer archive with the following command:

   java -jar hp-systinet-4.10.jar -x SYSTINET_HOME

   The Self-Test application package is SYSTINET_HOME/deploy/self-test-standalone.war.

2. Deploy the WAR file using the functionality of your application server or copy the WAR file to your JBoss deploy directory.

Caution: If you set password encryption after deploying the Self-Tester during installation or with the setup tool, you must redeploy the WAR.

To execute the stand-alone self-tester and access its output, start the Self-Test application in your application server and then access the following URL:

`http://hostname:port/self-test-standalone`

Note: `hostname:port` should match your application server.

The self-tester performs the following checks:

Self-Tests

Self-Test	Description
Product configuration checks	Checks product configuration, versions, and libraries.
Product runtime checks	Checks logging configuration, and outputs product base URLs.
Application server checks	Checks application server and JVM settings.
JNDI checks	Checks required JNDI resources.
Datasource checks	Checks the data source connection.
JMS checks	Checks the sending of JMS messages to required JMS destinations.
LDAP checks	Checks LDAP connectivity, if configured during installation or setup.
Performance	Basic HP Systinet performance checks.

You can view the self-test results in the server output console or with your browser.

In the default configuration, the server console output includes only information about the groups of checks that are run and any errors that occur. The full self-test output is stored in the application server log folder, `systinet_self_test.log`.

The web output is more informative and readable, showing all the checks run and the results.

Access the standalone self-test output at the following URL:

`http://`*hostname:port*`/self-test-standalone`

If errors occur, the self-tester provides details about the errors and suggests how to solve the underlying problems.

After installation, Self-Test is also available from the Administration menu in the Tools tab as part of the HP Systinet EAR and opens URL: `http://`*hostname:port/context*`/self-test`.

Self-test also enables you to test HTTP/HTTPS connections to simulate access to external resources in the same way as a deployed HP Systinet. Access this feature at the following URL:

`http://hostname:port/context/self-test/self-http-test`

During application setup and deployment, HP recommends running self-test at the following milestones:

- Before starting application server setup. At this point only the Application server checks should pass.

- After setting up JDBC resources. At this point the Datasource checks should pass if the application server is configured correctly.

- After setting up JMS resources. At this point the JMS checks should pass if the application server is configured correctly.

- After creating mail sessions. At this point the JNDI checks should pass if the application server is configured correctly.

- After deploying the HP Systinet EAR file and starting HP Systinet. At this point all checks should pass if the application server and HP Systinetare configured correctly.

Note: Freely available tools such as jmap, jstack, and jconsole may also be useful for the diagnosis of any performance issues. In case of performance issues, use:

jstack -l <application server java process id> > thread_dump.txt

jmap -dump:format=b,file=heap_dump.bin <application server java process id>

Setting Up JBoss

Deployment to JBoss requires less set up than installation to other J2EE servers. For Development deployments, Systinet installation automates deployment to JBoss. Datasources and JMS are set up on the host JBoss servers and the Systinet EAR file is deployed. The installer also creates a script for setting up the server environment and launching JBoss in simple deployment scenarios.

Caution: If you use JBoss with Windows, install it with a path that contains less than 20 characters. This limitation is caused by JBoss expanding the application in the local disk and the Windows 255 character limit on path names.

Warning: If you use JBoss with HP-UX, there is a known JVM bug that results in a ClassCircularityError in HP-UX when Systinet starts. Avoid this error by setting the `shared.as.jboss.preloading.classes.at.startup` property during installation. See "Using the GUI Installer" or "Deploying Systinet". For details of the issue, see http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4699981 and http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4670071.

Warning: If you use JBoss 5.0.1 EAP with Solaris, there is a known issue where deployment of Systinet may not finish. To avoid this issue, consider deployment to JBoss 4.2.2 or 4.3.0 instead.

You may need to modify the JBoss application server for it to host Systinet in Production environments.

If required, these modifications are covered in the following sections where JBOSS_HOME refers to the application server installation directory, for example `JBOSS/jboss50`.

The set up of JBoss for production environments prior to Systinet installation is described in the following sections:

There are additional steps to complete deployment to JBoss after installation. For details, see .

Prepare Load Balancing for JBoss Clusters

The following instructions are for the use of the mod_jk module in Apache 2.2 but you can use any passive-cookie load balancer which is supported by JBoss. For more information about mod_jk, see the Apache documentation. You can download mod_jk from the Apache site. There is also a version you can copy and paste in the following example:

```
Pasteable mod_jk.conf

# Load mod_jk module
# Specify the filename of the mod_jk lib
LoadModule jk_module modules/mod_jk-apache-2.2.3.so

# Where to find workers.properties
JkWorkersFile conf/workers.properties

# Where to put jk logs
JkLogFile logs/mod_jk.log

# Set the jk log level [debug/error/info]
JkLogLevel info

# Select the log format
JkLogStampFormat  "[%a %b %d %H:%M:%S %Y]"

# JkOptions indicates to send SSK KEY SIZE
JkOptions +ForwardKeySize +ForwardURIEscaped -ForwardDirectories

# JkRequestLogFormat
JkRequestLogFormat "%w %V %T"

# Mount your applications
JkMount /* loadbalancer

# You can use external file for mount points.
# It will be checked for updates each 60 seconds.
# The format of the file is: /url=worker
# /examples/*=loadbalancer
JkMountFile conf/uriworkermap.properties

# Add shared memory.
# This directive is present with 1.2.10 and
# later versions of mod_jk, and is needed for
# for load balancing to work properly
JkShmFile logs/jk.shm

# Add jkstatus for managing runtime data
<Location /jkstatus/>    JkMount status
    Order deny,allow
    Deny from all
```

```
     Allow from 127.0.0.1
</Location>
```

To Set Up `mod_jk` Load Balancing:

1. Install an Apache server, or configure an existing Apache server, to use the ports and host name which will be used for Systinet. Also configure SSL if it is required for deployment.

2. Copy `mod_jk.conf` to `APACHE/conf`.

3. In the Apache Tomcat `/conf` directory, edit `httpd.conf`. Add the line `Include conf/mod_jk.conf` to the end of the file. Make other changes to `httpd.conf` as described in that file's comments and in the Apache documentation.

4. Modify contexts in the file `APACHE\conf\uriworkermap.properties`, if necessary.

5. Modify workers settings in the file `APACHE\conf\workers.properties`. Change `worker.`*`nodeName`*`.port`, `worker.`*`nodeName`*`.host`, `worker.loadbalancer.balance_workers` and the number of workers. Names of nodes (*`nodeName`*) must match names of corresponding JBoss configurations. "Modified workers.properties" is a modified `workers.properties` file.

6. Run the Apache server with the configured load balancer.

Modified workers.properties

```
# Define list of workers that will be used
# for mapping requests
worker.list=loadbalancer,status

# Define Node1
# modify the host as your host IP or DNS name.
worker.node1.port=8009
worker.node1.host=server1
worker.node1.type=ajp13
worker.node1.lbfactor=1

# Define Node2
# modify the host as your host IP or DNS name.
worker.node2.port=8009
worker.node2.host=server2
worker.node2.type=ajp13
worker.node2.lbfactor=1

# Load-balancing behaviour
worker.loadbalancer.type=lb
worker.loadbalancer.balance_workers=node1,node2
worker.loadbalancer.sticky_session=1

# Status worker for managing load balancer
worker.status.type=status
```

Prepare the JBoss Cluster

1. Prepare a temporary configuration for Systinet installation.

   Copy the `JBOSS_HOME/server/all` configuration. Name the copy `nodeX`.

2. Prepare the first cluster node.

   Copy the `JBOSS_HOME/server/all` configuration. Name the copy `node1`.

Configure JMS for JBoss

JBoss uses JMS preconfigured for HSQLDB, which is sufficient for lightweight use in evaluation deployments. However, it has difficulty with large numbers of requests. For production deployments the JMS service should be configured to use a supported database.

Note: Systinet uses XA transactions. The application server transaction manager should be configured to have a minimum of 5 minutes for XA transaction timeout. For details, refer to your application server documentation.

To Set Up JBoss JMS to Use DB2 DS in Non-Clustered Deployments:

1. Copy the DB2 JDBC drivers `db2jcc.jar` and `db2jcc_license_cu.jar` to `JBOSS_HOME/server/default/lib`.

2. Delete the file `JBOSS_HOME/server/default/deploy/hsqldb-ds.xml` .

3. Copy `JBOSS_HOME/docs/examples/jca/db2-ds.xml` to `JBOSS_HOME/server/default/deploy`.

4. In the new copy of `db2-ds.xml`, edit the `connection-url`, `user-name`, and `password` elements to match your local environment.

5. Change the value of the `driver-class` element to `com.ibm.db2.jcc.DB2Driver`.

6. Change the value of the `jndi-name` element from `DB2DS` to `DefaultDS`.

7. Add a `max-pool-size` element at the same level as `password`, `user-name`, and `driver-class`. Set the value of `max-pool-size` to the maximum number of concurrent working users plus the number of concurrent task executions.

   If you do not have an estimate of these numbers, set the `max-pool-size` to 100.

Excerpt from db2-ds.xml

```
<datasources>
  <local-tx-datasource><jndi-name>DefaultDS</jndi-name>
    <connection-url>jdbc:db2://dbserver:50000/database</connection-url>
    <driver-class>com.ibm.db2.jcc.DB2Driver</driver-class>
    <user-name>soa_account</user-name>
    <password>soa_password</password>
    <min-pool-size>5</min-pool-size>
    <max-pool-size>15</max-pool-size>
    <metadata>
      <type-mapping>DB2</type-mapping>
    </metadata>
```

```
     </local-tx-datasource>
</datasources>
```

8. Save `db2-ds.xml`.

9. Delete the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/default/deploy/messaging/hsqldb-persistence-service.xml`

   - JBoss 4.3.0 EAP:

     `JBOSS_HOME/server/default/deploy/jboss-messaging.sar/hsqldb-persistence-service.xml`

   - JBoss 4.2.2 GA:

     `JBOSS_HOME/server/default/deploy/jms/hsqldb-jdbc2-service.xml`

10. Copy the following persistence file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     Copy `JBOSS_HOME/docs/examples/jms/db2-persistence-service.xml` to `JBOSS_HOME/server/default/deploy/messaging`.

   - JBoss 4.3.0 EAP:

     Copy `JBOSS_HOME/docs/examples/jms/db2-persistence-service.xml` to `JBOSS_HOME/server/default/deploy/jboss-messaging.sar`.

   - JBoss 4.2.2 GA:

     Copy `JBOSS_HOME/docs/examples/jms/db2-jdbc2-service.xml` to `JBOSS_HOME/server/default/deploy/jms`.

11. In the new copy of the persistence file, replace the string `DB2DS` with `DefaultDS`.

12. Open the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/default/deploy/messaging/jms-ds.xml`

   - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

     `JBOSS_HOME/server/default/deploy/jms/jms-ds.xml`

   Set the `max-pool-size` element to the maximum number of parallel served execution requests.

13. Open the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/default/deploy/jbossweb.sar/server.xml`

   - JBoss 4.3.0 EAP and JBoss 4.2.2:

     `JBOSS_HOME/server/default/deploy/jboss-web.deployer/server.xml`

   Set the `maxThreads` attribute to the maximum number of parallel served users.

To Set Up JBoss JMS to Use DB2 DS in Clustered Deployments:

1. Copy the DB2 JDBC drivers `db2jcc.jar` and `db2jcc_license_cu.jar` to `JBOSS_HOME/server/node1/lib`.

    Note: `node1` in the path refers to a copy of the `all` configuration folder.

2. Delete the file `JBOSS_HOME/server/default/node1/hsqldb-ds.xml` .

3. Copy `JBOSS_HOME/docs/examples/jca/db2-ds.xml` to `JBOSS_HOME/server/node1/deploy`.

4. In the new copy of `db2-ds.xml`, edit the `connection-url`, `user-name`, and `password` elements to match your local environment.

5. Change the value of the `driver-class` element to `com.ibm.db2.jcc.DB2Driver`.

6. Change the value of the `jndi-name` element from `DB2DS` to `DefaultDS`.

7. Add a `max-pool-size` element at the same level as `password`, `user-name`, and `driver-class`. Set the value of `max-pool-size` to the maximum number of concurrent working users plus the number of concurrent task executions.

    If you do not have an estimate of these numbers, set the `max-pool-size` to 100.

8. Save `db2-ds.xml`.

9. Delete the file `JBOSS_HOME/server/node1/deploy-hasingleton/jms/hsqldb-jdbc2-service.xml`.

10. Copy the following persistence file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      Copy `JBOSS_HOME/docs/examples/jms/db2-persistence-service.xml` to `JBOSS_HOME/server/node1/deploy-hasingleton/messaging`.

    - JBoss 4.3.0 EAP:

      Copy `JBOSS_HOME/docs/examples/jms/db2-persistence-service.xml` to `JBOSS_HOME/server/node1/deploy-hasingleton/jboss-messaging.sar`.

    - JBoss 4.2.2 GA:

      Copy `JBOSS_HOME/docs/examples/jms/db2-jdbc2-service.xml` to `JBOSS_HOME/server/node1/deploy-hasingleton/jms`.

11. In the new copy of of the persistence file, replace the string `DB2DS` with `DefaultDS`.

12. Save the new persistence file.

13. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/node1/deploy/messaging/jms-ds.xml`

    - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

      `JBOSS_HOME/server/node1/deploy/jms/hajndi-jms-ds.xml`

Set the `max-pool-size` element to the maximum number of parallel served execution requests.

14. Open the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/node1/deploy/jbossweb.sar/server.xml`

   - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

     `JBOSS_HOME/server/node1/deploy/jboss-web.deployer/server.xml`

   Set the `maxThreads` attribute to the maximum number of parallel served users.

To Set Up JBoss JMS to Use MSSQL DS in Non-Clustered Deployments:

1. Copy the MSSQL JDBC driver to `JBOSS_HOME/server/default/lib`.

2. Delete the file `JBOSS_HOME/server/default/deploy/hsqldb-ds.xml` .

3. Copy `JBOSS_HOME/docs/examples/jca/mssql-xa-ds.xml` to `JBOSS_HOME/server/default/deploy`.

4. In the new copy of `mssql-xa-ds.xml`, edit the `ServerName`, `DatabaseName`, `User`, and `Password` elements to match your local environment.

5. Change the value of the `jndi-name` element from `MSSQLDS` to `DefaultDS`.

6. Add a `max-pool-size` element at the same level as `password`, `user-name`, and `driver-class`. Set the value of `max-pool-size` to the maximum number of concurrent working users plus the number of concurrent task executions.

   If you do not have an estimate of these numbers, set the `max-pool-size` to 100.

7. Add a new element, `<xa-datasource-property name="ResponseBuffering">full</xa-datasource-property>` at the same level as the other `xa-datasource-property` elements,

8. Save `mssql-xa-ds.xml`.

9. Delete the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/default/deploy/messaging/hsqldb-persistence-service.xml`

   - JBoss 4.3.0 EAP:

     `JBOSS_HOME/server/default/deploy/jboss-messaging.sar/hsqldb-persistence-service.xml`

   - JBoss 4.2.2 GA:

     `JBOSS_HOME/server/default/deploy/jms/hsqldb-jdbc2-service.xml`

10. Copy the following file, depending on your JBoss version:

- JBoss 5.0 EAP and JBoss 5.1 GA:

  Copy `JBOSS_HOME/docs/examples/jms/mssql-persistence-service.xml` to
  `JBOSS_HOME/server/default/deploy/messaging`.

- JBoss 4.3.0 EAP:

  Copy `JBOSS_HOME/docs/examples/jms/mssql-persistence-service.xml` to
  `JBOSS_HOME/server/default/deploy/jboss-messaging.sar`.

- JBoss 4.2.2 GA:

  Copy `JBOSS_HOME/docs/examples/jms/mssql-jdbc2-service.xml` to `JBOSS_HOME/server/default/deploy/jms`.

11. In the new copy of `mssql-jdbc2-service.xml`, replace the string `MSSQLDS` with
    `DefaultDS`.

12. Open the following file depending on your version of JBoss:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/default/deploy/messaging/jms-ds.xml`

    - JBoss 4.3.0 EAP:

      `JBOSS_HOME/server/default/deploy/jms-ds.xml`

    - JBoss 4.2.2 GA:

      `JBOSS_HOME/server/default/deploy/jms/jms-ds.xml`

    Set the `max-pool-size` element to the maximum number of parallel served execution
    requests.

13. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/default/deploy/jbossweb.sar/server.xml`

    - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

      `JBOSS_HOME/server/default/deploy/jboss-web.deployer/server.xml`

    Set the `maxThreads` attribute to the maximum number of parallel served users.

To Set Up JBoss JMS to Use MSSQL DS in Clustered Deployments:

1. Copy the MSSQL JDBC driver to `JBOSS_HOME/server/`*node1*`/lib`.

   Note: *node1* in the path refers to a copy of the `all`configuration folder.

2. Delete the file `JBOSS_HOME/server/`*node1*`/deploy/hsqldb-ds.xml` .

3. Copy `JBOSS_HOME/docs/examples/jca/mssql-xa-ds.xml` to `JBOSS_HOME/server/`*node1*`/deploy`.

4. In the new copy of `mssql-xa-ds.xml`, edit the `ServerName`, `DatabaseName`, `User`, and
   `Password` elements to match your local environment.

5. For Change the value of the `jndi-name` element from `MSSQLDS` to `DefaultDS`.

6. Add a `max-pool-size` element at the same level as `password`, `user-name`, and `driver-class`. Set the value of `max-pool-size` to the maximum number of concurrent working users plus the number of concurrent task executions.

   If you do not have an estimate of these numbers, set the `max-pool-size` to 100.

7. Add a new element, `<xa-datasource-property name="ResponseBuffering">full</xa-datasource-property>` at the same level as the other `xa-datasource-property` elements,

8. Save `mssql-xa-ds.xml`.

9. Delete the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/default/deploy/messaging/hsqldb-persistence-service.xml`

   - JBoss 4.3.0 EAP:

     `JBOSS_HOME/server/default/deploy/jboss-messaging.sar/hsqldb-persistence-service.xml`

   - JBoss 4.2.2 GA:

     `JBOSS_HOME/server/default/deploy/jms/hsqldb-jdbc2-service.xml`

10. Copy the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      Copy `JBOSS_HOME/docs/examples/jms/mssql-persistence-service.xml` to `JBOSS_HOME/server/`*node1*`/deploy/deploy-hasingleton/messaging`.

    - JBoss 4.3.0 EAP:

      Copy `JBOSS_HOME/docs/examples/jms/mssql-persistence-service.xml` to `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/jboss-messaging.sar`.

    - JBoss 4.2.2 GA:

      Copy `JBOSS_HOME/docs/examples/jms/mssql-jdbc2-service.xml` to `JBOSS_HOME/server/`*node1*`/deploy/jms`.

11. In the new copy of `mssql-jdbc2-service.xml`, replace the string `MSSQLDS` with `DefaultDS`.

12. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/default/`*node1*`/deploy/messaging/jms-ds.xml`

    - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

      `JBOSS_HOME/server/`*node1*`/deploy/jms/hajndi-jms-ds.xml`

    Set the `max-pool-size` element to the maximum number of parallel served execution requests.

13. Open the following file depending on your JBoss version:

- JBoss 5.0 EAP and JBoss 5.1 GA:

  `JBOSS_HOME/server/`*node1*`/deploy/jbossweb.sar/server.xml`

- JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

  `JBOSS_HOME/server/`*node1*`/deploy/jboss-web.deployer/server.xml`

Set the `maxThreads` attribute to the maximum number of parallel served users.

To Set Up JBoss JMS to Use Oracle DS in Non-Clustered Deployments:

1. Copy the Oracle JDBC driver to `JBOSS_HOME/server/default/lib`.

2. Delete the file `JBOSS_HOME/server/default/deploy/hsqldb-ds.xml`

3. Copy `JBOSS_HOME/docs/examples/jca/oracle-ds.xml` to `JBOSS_HOME/server/default/deploy`.

4. In the new copy of `oracle-ds.xml`, edit the `connection-url`, `user-name`, and `password` elements to match your local environment.

5. Change the value of the `jndi-name` element from `OracleDS` to `DefaultDS`.

6. Add a `max-pool-size` element at the same level as `password`, `user-name`, and `driver-class`. Set the value of `max-pool-size` to the maximum number of concurrent working users plus the number of concurrent task executions.

   If you do not have an estimate of these numbers, set the `max-pool-size` to 100.

7. Save `oracle-ds.xml`.

8. Delete the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     `JBOSS_HOME/server/default/deploy/messaging/hsqldb-persistence-service.xml`

   - JBoss 4.3.0 EAP:

     `JBOSS_HOME/server/default/deploy/jboss-messaging.sar/hsqldb-persistence-service.xml`

   - JBoss 4.2.2 GA:

     `JBOSS_HOME/server/default/deploy/jms/hsqldb-jdbc2-service.xml`

9. Copy the following file depending on your JBoss version:

   - JBoss 5.0 EAP and JBoss 5.1 GA:

     Copy `JBOSS_HOME/docs/examples/jms/oracle-persistence-service.xml` to `JBOSS_HOME/server/default/deploy/messaging`.

   - For JBoss 5.1 GA, comment out the following element:

     ```
     <!--depends optional-attribute-
     name="Ch-
     annelFactoryName">jboss.jgroups:service=ChannelFactory</depends--
     >
     ```

- JBoss 4.3.0 EAP:

  Copy `JBOSS_HOME/docs/examples/jms/oracle-persistence-service.xml` to `JBOSS_HOME/server/default/deploy/jboss-messaging.sar`.

- JBoss 4.2.2 GA:

  Copy `JBOSS_HOME/docs/examples/jms/oracle-jdbc2-service.xml` to `JBOSS_HOME/server/default/deploy`.

10. In the new copy of the Oracle service file, replace the string `OracleDS` with `DefaultDS`.

11. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP, JBoss 5.1 GA, and JBoss 4.3.0 EAP:

      `JBOSS_HOME/server/default/deploy/jms-ds.xml`

    - JBoss 4.2.2 GA:

      `JBOSS_HOME/server/default/deploy/jms/jms-ds.xml`

    Set the `max-pool-size` element to the maximum number of parallel served execution requests.

12. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/default/deploy/jbossweb.sar/server.xml`

    - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

      `JBOSS_HOME/server/default/deploy/jboss-web.deployer/server.xml`

    Set the `maxThreads` attribute to the maximum number of parallel served users.

13. For JBoss 5.0 EAP, 5.1 GA, and 4.3.0 GA, ensure that a copy of `JBOSS_HOME/server/all/lib/jgroups.jar` exists in `JBOSS_HOME/server/default/lib`.

To Set Up JBoss JMS to Use Oracle DS in Clustered Deployments:

1. Copy the Oracle JDBC driver to `JBOSS_HOME/server/node1/lib`.

   Note: *node1* in the path refers to a copy of the `all` configuration folder.

2. Delete the file `JBOSS_HOME/server/node1/deploy/hsqldb-ds.xml` .

3. Copy `JBOSS_HOME/docs/examples/jca/oracle-ds.xml` to `JBOSS_HOME/server/node1/deploy`.

4. In the new copy of `oracle-ds.xml`, edit the `connection-url`, `user-name`, and `password` elements to match your local environment.

5. Change the value of the `jndi-name` element from `OracleDS` to `DefaultDS`.

6. Add a `max-pool-size` element at the same level as `password`, `user-name`, and `driver-class`. Set the value of `max-pool-size` to the maximum number of concurrent working users plus the number of concurrent task executions.

   If you do not have an estimate of these numbers, set the `max-pool-size` to 100.

7. Save `oracle-ds.xml`.

8. Delete the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/messaging/hsqldb-jdbc2-service.xml`

    - JBoss 4.3.0 EAP:

      `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/jboss-messaging.sar/hsqldb-persistence-service.xml`

    - JBoss 4.2.2 GA:

      `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/jms/hsqldb-jdbc2-service.xml`

9. Copy the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      Copy `JBOSS_HOME/docs/examples/jms/oracle-persistence-service.xml`to `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/messaging`.

    - JBoss 4.3.0 EAP:

      Copy `JBOSS_HOME/docs/examples/jms/oracle-persistence-service.xml` to `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/jboss-messaging.sar`.

    - JBoss 4.2.2 GA:

      Copy `JBOSS_HOME/docs/examples/jms/oracle-jdbc2-service.xml` to `JBOSS_HOME/server/`*node1*`/deploy-hasingleton/jms`.

10. In the new copy of the Oracle service file, replace the string `OracleDS` with `DefaultDS`.

11. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/`*node1*`/deploy/messaging/jms-ds.xml`

    - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

      `JBOSS_HOME/server/`*node1*`/deploy/jms/hajndi-jms-ds.xml`

    Set the `max-pool-size` element to the maximum number of parallel served execution requests.

12. Open the following file depending on your JBoss version:

    - JBoss 5.0 EAP and JBoss 5.1 GA:

      `JBOSS_HOME/server/`*node1*`/deploy/jbossweb.sar/server.xml`

    - JBoss 4.3.0 EAP and JBoss 4.2.2 GA:

      `JBOSS_HOME/server/`*node1*`/deploy/jboss-web.deployer/server.xml`

    Set the `maxThreads` attribute to the maximum number of parallel served users.

13. For JBoss 5.0 EAP, 5.1 GA, and 4.3.0 GA, ensure that a copy of `JBOSS_`

`HOME/server/all/lib/jgroups.jar` exists in `JBOSS_HOME/server/CONFIG_ NAME/lib`.

Modify the JBoss Run Script

When you launch Systinet with the `SYSTINET_HOME/bin/serverstart` script, it calls `env-jboss` to set JBoss environment variables before calling the JBoss run script. No further set up is necessary for most evaluation or development scenarios. However, `serverstart` is not appropriate for all production environments and it may be appropriate to execute the JBoss `run` script directly.

Note: If you execute the JBoss run script directly, use the `-server` JDK option.

The following procedures describe how to alter the JBoss `run` script for use in production deployments:

If JBoss is installed on UNIX, set the java.awt.headless property to "true".

To Set java.awt.headless:

1. Open the `JBOSS_HOME/bin/run` script in an editor.

2. Insert this line where JAVA_OPTS is set:

   `-Djava.awt.headless=true`

3. Save and exit the script.

Increase the maximum memory limit on the JBoss server to optimize Systinet performance.

Caution: This procedure is intended for cases where using `serverstart` is inappropriate. If you need to change the memory allocation settings and use `serverstart` you should remove the memory allocation line from the `run` script and apply the changes to `SYSTINET_ HOME/bin/env-jboss` instead.

To Change the Memory Settings:

1. Open the `run` script in the `bin` directory of the JBoss server.

2. Find the following lines:

```
rem JVM memory allocation pool parameters. Modify as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -Xms128m...
```

3. Do one of the following:

   - For 32-bit JVM, edit the lines as follows:

```
rem JVM memory allocation pool parameters. Modify as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -Xms1536m -Xmx1536m
    -XX:MaxPermSize=256m -XX:NewRatio=8
```

   - For 64-bit JVM, edit the lines as follows:

```
rem JVM memory allocation pool parameters. Modify as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -Xms4096m -Xmx4096m
    -XX:MaxPermSize=256m
```

4. Save and exit the script.

Note: Memory sizing should take performance requirements into consideration for the deployed system. These settings are only a recommendation.

Note: Heap size recommendations depend on the number of concurrent users. Based on HP measurements on a 64-bit server using JDK 1.6.0_16 (Java version: 1.6.0_16,Sun Microsystems Inc.Java VM: Java HotSpot(TM) 64-Bit Server VM 14.2-b01,Sun Microsystems Inc.)

-Xmx:

- 50 users: 1700m

- 100 users: 2200m

- 150 users: 3000m

- 300 users: 4000m

Other recommended JVM options:

- Memory saving: `-XX:+UseParallelOldGC -XX:+UseCompressedOops`

- In case of occasional memory and performance issues even with the recommended heap size: `-XX:SoftRefLRUPolicyMSPerMB=0`

- For debugging: `-XX:+PrintCommandLineFlags`

Set the JBoss Datasource Maximum Pool Size

The default JBoss datasource Maximum Pool Size is not adequate for a production environment. For example, the default MaxPoolSize based on default Oracle configuration is only 15. The Maximum Pool Size should be at least 1/4 the number of parallel requests that you require to be handled simultaneously.

To Increase the Maximum Pool Size:

1. Open `JBOSS_HOME/server/CONFIG_HOME/deploy/hp-soa-systinet-xa-ds.xml` in an editor. (CONFIG_HOME refers to the JBoss configuration to which you will deploy Systinet. For non-clustered deployments, this is usually `default` and for clustered deployments, this is usually `all`.)

2. Edit the element `max-pool-size`. Its value should be at least 1/4 of the number of simultaneous parallel requests.

3. Save your changes and exit.

Setting Up WebLogic

Set up a separate WebLogic domain to host Systinet. You must configure the domain itself and JDBC and JMS properties for the managed servers and/or clusters in the domain. You need to know the number and location of cluster servers or managed servers before you start.

Note: In this document, WL_HOME refers to the WebLogic server installation directory.

The set up of WebLogic prior to Systinet installation is described in the following sections:

- "Create a WebLogic Domain" (on page 45)

- "Set Up WebLogic Managed Servers" (on page 46)

- "Create Resources in WebLogic" (on page 48)

- "Create a WebLogic Mail Session" (on page 49)

- "Create JDBC Resources in WebLogic" (on page 49)

- "Create JMS Resources in WebLogic" (on page 52)

- "Set Up the WebLogic Security Realm" (on page 55)

There are additional steps to complete deployment to WebLogic after installation. For details, see "Deploy the EAR to WebLogic" (on page 125).

Create a WebLogic Domain

You must host HP Systinet in a separate WebLogic domain.

To Create a WebLogic Domain Using the WebLogic Configuration Wizard:

1. Launch the WebLogic Configuration wizard with the following command:

   WL_HOME/common/bin/config

   Tip: In Windows you can launch the wizard from the **Start** menu.

2. Select **Create a New WebLogic Domain**, and click **Next**.

3. In WebLogic 11g (10.3.1), set the domain name and location and click **Next**.

4. You can use the default settings for the domain source and then click **Next**.

   The Admin Username page opens.

5. Set the WebLogic administrator username and password, and click **Next**.

   The Configure Server Start Mode and JDK page opens.

6. You can select either **Development** or **Production** mode.

7. Select your JDK and then click **Next**.

8. In WebLogic 10g (10.3), select **Yes** and click **Next**.

9. In WebLogic 10g, you can use the default Administrator Server settings. Click **Next**.

10. In WebLogic 11g (10.3.1), do any of the following:

    - Select **Managed Servers, Clusters, and Machines** to set up your servers, clusters, and machines for Systinet deployment.

    - Select **Administration Server** to specify an admin server.

    Click **Next**.

11. Create the managed servers required by your deployment. You require at least one managed server. Do not install Systinet to the administration server. Give the servers arbitrary names, such as `hpsoa1`. You can use a proxy for clusters. Make sure the server ports do not conflict with the administration server.

12. Create any clusters required for your deployment and then click **Next**.

13. If you use clusters, assign managed servers to them and then click **Next**.

14. *Optional:* Create an HTTP proxy for your clusters, and then click **Next**.

15. Create a machine in your domain and then click **Next**.

16. Assign all managed servers, both clustered and standalone, to the machine. You do not have to assign the administration server to the machine. Click **Next**.

17. In WebLogic 11g (10.3.1), review the domain and click **Create**.

18. In WebLogic 10g (10.3), review the new domain and click **Next**.

19. In WebLogic 10g (10.3), set the domain name and location and click **Create**.

Note: In this document, the domain is referred to as *hpsoa_domain*. The location is referred to as `DOMAIN_HOME`.

Set Up WebLogic Managed Servers

Each managed server hosting Systinet requires some configuration.

Note: The **Lock and Edit** and **Activate Changes** steps do not apply to WebLogic 10g (10.3) in Development mode as any changes made are directly applied. If you are using WebLogic 10g (10.3) in development mode, skip these steps.

To Set Up a Managed Server:

1. On each machine hosting the administration server, a managed server, or a cluster, start the WebLogic Node Manager with the following command:

   WL_HOME/server/bin/startNodeManager

   Caution: WebLogic 10g (10.3) node manager uses system variables *PATH* and *CLASSPATH* in the server start command. The node manager does not handle these variables if they contain spaces. To avoid this problem, do one of the following:

   - On Windows, replace the conflicting parts of the paths with DOS-like 8.3 file names and restart node manager.

   - Edit `WL_HOME/common/nodemanager/nodemanager.properties`, and add the parameter `StartScriptEnabled=true`, and then restart node manager.

2. Start the WebLogic server for your domain with the following command:

   DOMAIN_HOME/startWebLogic

3. In your browser, open the WebLogic Administration Console:

   `http://localhost:7001/console`

4. Log in with the administrator credentials created in "Create a Domain for Systinet".

5. In the web console in the Change Center section, click **Lock & Edit**.

6. In the Domain Structure section, expand **Services** and select **JTA**.

   The Domain Settings page opens.

7. HP recommends setting **Timeout Seconds** to 300 and clicking **Save**.

8. In the Change Center section, click **Activate Changes**.

9. In the Domain Structure section, expand **Environment** and select **Servers**.

   The Summary of Servers page opens.

10. In the Change Center section, click **Lock & Edit**.

11. For each managed server set the start-up parameters, Step 12 to Step 15.

12. In the Summary of Servers page, click the new server name.

   The Settings page opens.

13. Select the **Configuration: Server Start** tab.

14. Set the class path to the following:

   ■ For WebLogic 10g (10.3): `DB_DRIVER_PATHS;JAVA_HOME/lib/tools.jar;WL_HOME/server/lib/weblogic_sp.jar; WL_HOME/server/lib/weblogic.jar;BEA_HOME/modules/features/weblogic.server.modules_10.3.0.0.jar; BEA_HOME/modules/features/com.bea.cie.common-plugin.launch_2.1.0.0.jar`

   ■ For WebLogic 11g (10.3.1): `DB_DRIVER_PATHS;JAVA_HOME/lib/tools.jar;WL_HOME/server/lib/weblogic_sp.jar; WL_HOME/server/lib/weblogic.jar;BEA_HOME/modules/features/weblogic.server.modules_10.3.1.0.jar; BEA_HOME/modules/features/com.bea.cie.common-plugin.launch_2.3.0.0.jar`

   Note: DB_DRIVER_PATHS must contain the paths to all JARs for the drivers required by the database supported by Systinet.. JAVA_HOME is the location of the JDK that WebLogic uses and BEA_HOME is set during WebLogic installation. On UNIX systems, use colons instead of semi-colons as the file separator. For Oracle Database, the classpath must include the file location for orai18n.jar

15. Add the following to Arguments:

   ■ For Sun or HP 32-bit JDKs:

      -Xms1536m -Xmx1536m -XX:MaxPermSize=512m

   ■ For Sun or HP 64-bit JDKs:

      -Xms4096m -Xmx4096m -XX:MaxPermSize=512m

   Note: Memory sizing should take performance requirements into consideration for the deployed system. These settings are only a recommendation.

   Note: Heap size recommendations depend on the number of concurrent users. Based on HP measurements on a 64-bit server using JDK 1.6.0_16 (Java version: 1.6.0_16,Sun Microsystems Inc.Java VM: Java HotSpot(TM) 64-Bit Server VM 14.2-b01,Sun Microsystems Inc.)

   -Xmx:

- 50 users: 1700m

- 100 users: 2200m

- 150 users: 3000m

- 300 users: 4000m

Other recommended JVM options:

- Memory saving: `-XX:+UseParallelOldGC -XX:+UseCompressedOops`

- In case of occasional memory and performance issues even with the recommended heap size: `-XX:SoftRefLRUPolicyMSPerMB=0`

- For debugging: `-XX:+PrintCommandLineFlags`

  Caution: If you use a UNIX operating system, also add the following property: Generic JVM Arguments `-Djava.awt.headless=true`

16. Click **Save**.

17. Click **Activate Changes**.

The managed server is now available to start. HP recommends setting up resources, as described in the following section, before starting the managed server. The managed server must be running if you start Systinet from the Deployments page of the WebLogic Administration console.

Warning: If you start servers from the command line or a script, the Java arguments you add in the Administration Console are not applied. Start the managed server with commands based on these scripts:

startMyNode.bat **for Windows:**

```
set DOMAIN_HOME=c:\your\weblogic\domain\home
set JAVA_OPTIONS="-Djava.awt.headless=true"
set USER_MEM_ARGS="-Xms1024m -Xmx1024m -XX:MaxPermSize=512m"
%DOMAIN_HOME%/bin/startManagedWebLogic [nodename]
```

startMyNode.sh **for Linux:**

```
export DOMAIN_HOME=/your/weblogic/domain/home
export JAVA_OPTIONS="-Djava.awt.headless=true"
export USER_MEM_ARGS="-Xms1024m -Xmx1024m -XX:MaxPermSize=512m"
.   $DOMAIN_HOME/bin/startManagedWebLogic.sh [nodename]
http://hostname:7001
```

Create Resources in WebLogic

Systinet requires a number of resources to be set up in WebLogic.

Use the Administration Console to create them.

Note: The **Lock and Edit** and **Activate Changes** steps do not apply to WebLogic 10g (10.3) in Development mode as any changes made are directly applied. If you are using WebLogic 10g (10.3) in development mode, skip these steps.

To Use the Administration Console to Create Resources:

1. In your browser, open the WebLogic Administration Console:

   `http://localhost:7001/console`

2. Log in as the WebLogic administrator.

3. Use the Administration Console to create mail, JDBC, and JMS resources, as described in the following sections.

You can verify your resources set up in your browser:

`http://localhost:7001/console/consolejndi.portal`

Create a WebLogic Mail Session

Systinet requires a mail session for automated notifications.

To Create an Systinet Mail Session:

1. In the Domain Structure section, expand **Services** and select **Mail Sessions**.

   The Summary of Mail Sessions page opens.

2. Click **Lock & Edit**.

3. Click **New**.

   The Create a New Mail Session page opens.

4. Enter a name, and then click **OK**.

5. In the Summary of Mail Sessions page, click the new mail session name.

6. Enter the JNDI Name, `/Mail`, enter JavaMail Properties according to your environment mail settings, for example,
   `mail.tran-`
   `sport.protocol=smtp;mail.user=builder;mail.smtp.host=mail.com,` and then click **Next**.

   Note: JNDI names must be exact.

7. In the Settings page, select the **Targets** tab.

8. Target all servers and clusters hosting HP Systinet, and click **Save**.

9. Click **Activate Changes**.

Create JDBC Resources in WebLogic

Systinet requires two JDBC datasources, an XA-enabled datasource and a non-XA-enabled datasource. These datasources handle all traffic between the Systinet on WebLogic and the database server. Each WebLogic managed server and/or cluster server requires a persistent store on the database, which uses the non-XA-enabled datasource for communication.

Use the WebLogic Administration Console to create JDBC datasources. The Administration Server must be running.

Note: Systinet uses XA transactions. The application server transaction manager should be configured to have a minimum of 5 minutes for XA transaction timeout. For details, see your application server documentation.

To Create an XA-Enabled JDBC Datasource:

1. Open the Summary of JDBC Datasources page (**Services→JDBC→Data Sources**).

2. Click **Lock and Edit**.

3. Click **New**.

4. Give the datasource a unique, arbitrary descriptive name, such as `HP SOA Systinet DS`.

5. Give the datasource the JNDI name `hpsoasystinetDS`.

   Note: JNDI names must be exact.

6. From the Database drop-down list, select the same database type that you use for Systinet.

7. From the Database Driver drop-down list, select an XA-supporting JDBC database driver using the default driver class for your database type.

   Note: If you are using Oracle, select the Oracle "thin" XA driver.

8. Click **Next** to open the Transaction Options page. and click **Next** again to open the Connection Properties page.

9. In the Connection Properties page, use the same database parameters you use for Systinet. Proceed to Target Selection by clicking **Next**.

10. In Select Targets, select all servers or clusters hosting Systinet.

11. Click **Finish** to return to the Summary of JDBC Datasources page.

    The datasource you created appears in the table of datasources.

12. Click **Activate Changes**.

13. Click **Lock and Edit**.

14. Click the name of the XA datasource in the table of datasources to open its details page in the Configuration: General tab.

15. Open the **Configuration: Connection Pool** tab.

    Increase the maximum capacity of the connection pool. The Maximum Capacity should be at least 1/4 the number of parallel requests that you require to be handled simultaneously. If you do not have an estimate of this number, set the maximum capacity to 100.

16. Increase the Initial Capacity to the number of expected concurrent users.

17. Click **Save**.

18. To enable failover, in the Connection Pool tab, expand the **Advanced** section.

    Select **Test Connections on Reserve**.

19. Open the Configuration:Transactions tab ensure that **Use XA Datasource Interface** is selected.

20. Click **Save**.

21. Navigate out of the datasource details page, for example to the Summary of JDBC Datasources page, and click **Activate Changes**.

    Note: If you do not navigate out of the datasource details page before you save changes to the datasource, you cause a `JDBCSystemResourceMBean cannot be null`

exception. This exception is harmless, because the changes to the datasource are activated anyway, but avoidable.

Note: If the exception "Could not get JDBC Connection; nested exception is java.sql.SQLException: Internal error: Cannot obtain XAConnection weblogic.common.resourcepool.ResourceDisabledException: Pool hpsoasystinetDS is disabled, cannot allocate resources to applications..." occurs in the in log file, you can do any of the following:

- Increase the count of connections in the datasource.

- Increase the timeout for acquiring a connection.

- Increase the value of Connection Reserve Timeout (Data Sources→hpsoasystinetDS→Connection Pool→Advanced). (Default is 10 seconds).

- Setting 0 (infinite waiting for connection) is not recommended because of a risk of deadlocks.

To Create a Non-XA-Enabled JDBC Datasource:

1. Open the JDBC datasources page (**Services**→**JDBC**→**Data Sources**).

2. Click **Lock and Edit**.

3. Click **New**.

4. Give the datasource a unique, arbitrary descriptive name such as `HP SOA Systinet JMS DS`.

5. Give the datasource the JNDI name `jms-hpsoasystinetDS`.

   Note: JNDI names must be exact.

6. From the Database drop-down list, select the same database type that you use for Systinet.

7. From the Database Driver drop-down list, select a non-XA-supporting JDBC database driver for the database type.

   Note: If you are using Oracle, select the Oracle "thin" non-XA driver.

   Click **Next** to open the Transaction Options page.

8. Select **Supports Global Transactions** and click **Next** to open the Connection Properties page.

9. In the Connection Properties page, use the same database parameters you use for Systinet. Proceed to Target Selection by clicking **Next**.

10. In Select Targets, select all servers or clusters hosting Systinet.

11. Click **Finish**. The datasource you created appears in the table of datasources.

12. Click **Activate Changes**.

13. Click **Lock and Edit**.

14. To enable failover, click the name of the non-XA datasource in the table of datasources to open its details page in the Configuration:General tab.

15. Open the Configuration:Connection Pool tab and expand the Advanced section.

Select **Test Connections on Reserve**.

Click **Save**.

16. Navigate out of the datasource details page, for example to the Summary of JDBC Datasources page, and click **Activate Changes**.

    Note: If you do not navigate out of the datasource details page before you save changes to the datasource, you cause a JDBC `SystemResourceMBean cannot be null` exception. This exception is harmless, because the changes to the datasource are activated anyway, but avoidable.

Create a JDBC persistent store for every migratable cluster server and every standalone server hosting Systinet. These persistent stores use the `jms-hpsoasystinetDS` non-XA datasource.

To Create a JDBC Persistent Store:

1. Navigate to **Services→Persistent Stores**.

2. Click **Lock and Edit**.

3. From the New drop-down menu, select **Create a JDBC Store** to open the Create JDBC Store wizard.

4. Give the persistent store a unique, arbitrary name, such as *SERVER_NAME* Store.

5. From the Target drop-down list, select the standalone managed server or migratable cluster server corresponding to the selected persistent store.

6. In the Datasource drop-down field, select the non-XA-enabled datasource you created.

7. Give the persistent store a unique prefix, so that the stores do not use the same table.

8. Click **Finish** and save your changes.

9. Repeat the procedure for each migratable cluster server and/or standalone managed server.

10. Click **Activate Changes**.

Create JMS Resources in WebLogic

Systinet requires JMS resources to be set up in WebLogic.

Note: You can configure JMS to meet your requirements. This section describes a JMS set up that ensures that JMS resources are accessible by HP Systinet and function correctly.

Create a JMS server for each migratable cluster server and each standalone server.

To Create a JMS Server:

1. Open the JMS Servers page, **Services→Messaging→JMS Servers**.

2. Click **Lock and Edit**

3. Click **New** to open the Create a New JMS Server wizard in the JMS Server Properties page.

4. In the Name field, give the JMS server a unique, arbitrary descriptive name, such as *SERVER_ NAME JMS*, indicating which server is targeted.

5. From the Persistent Store drop-down field, select the persistent store of the managed server or

migratable cluster server to target.

Click **Next** to open the Select Targets page

6. From the Target drop-down field, select the standalone managed server or migratable cluster server corresponding to the persistent store you selected.

   Click **Finish**.

7. Click **Activate Changes**.

Create a JMS Module to contain definitions of JMS connection factories as well as required JMS destinations.

To Create a JMS Module:

1. Open the JMS Modules page, **Services→Messaging→JMS Modules**.

2. Click **Lock and Edit**.

3. Click **New** to open the Create JMS System Module wizard.

4. Give the JMS module a unique, arbitrary descriptive name, such as `HP SOA Systinet JMS Module.`

   You may apply any descriptor file name and location, or leave those fields blank to use the default.

   Click **Next**.

5. Target the standalone server or the cluster hosting Systinet.

6. Select **Would you like to add resources to this JMS system module?**, and click **Finish**.

   The details page for the JMS Module opens in the Configuration tab.

7. Create the connection factories listed in the following table:

JMS Connection Factories for WebLogic

Name	JNDI Name
HP SOA Systinet Connection Factory	/ConnectionFactory
Reporting Sender Connection Factory	jms/ReportingSenderConnectionFactory
Reporting Receiver Connection Factory	jms/ReportingReceiverConnectionFactory

a. Click **New** in the Summary of Resources table to open the Create a New JMS System Module Resource wizard.

b. Select **Connection Factory** and click **Next** to open the Create a New Connection Factory wizard.

c. Give the connection factory a unique, arbitrary descriptive name (for example the ones listed in the table above).

d. Give the connection factory the JNDI name specified in the JNDI Name column.

   Note: JNDI names must be exact.

    e. Use the default targeting, which selects the parent module target.

    f. Click **Finish**.

    g. Edit each connection factory and select **XA Connection Factory Enabled** in the Configuration:Transactions tab.

    h. If the Systinet host is a cluster, open the Configuration: Load Balancing tab and disable server affinity.

    i. Navigate back to the list of JMS Modules and then click **Activate Changes**.

8. If the HP Systinet host is a managed server and not a cluster create a subdeployment.

    a. Click **Lock & Edit**.

    b. Navigate to the HP Systinet JMS Module details page.

    c. Open the Subdeployments tab and create a subdeployment for the JMS module.

    d. Set the subdeployment target as the Systinet host managed server's JMS server.

    e. Create the resources listed in the table below.

       Return to the JMS module details page, and click **New** in the Resources table. Select the resource type and click **Next**. Leave blank all fields not included in the table. After you enter the values for a resource, configure it to use the subdeployment and click **Finish**.

JMS Resources for a WebLogic Managed Server

Resource Type	Name	JNDI Name
Queue	SC scheduleTimerQueue	queue/scheduleTimerQueue
Queue	PM Validations Queue	queue/Validation
Queue	PM Priority Validations Queue	queue/PriorityValidation
Queue	SC TaskProcessorQueue	queue/taskProcessorQueue
Queue	RF Executions Queue	queue/ReportingExecutions
Topic	SC taskStopperTopic	topic/taskStopperTopic

9. If the Systinet host is a cluster create the resources listed in the following table:

JMS Resources for a WebLogic Cluster

Resource Type	Name	JNDI Name
Distributed Queue	SC scheduleTimerQueue	queue/scheduleTimerQueue
Distributed Queue	PM Validations Queue	queue/Validation
Distributed Queue	PM Priority Validations Queue	queue/PriorityValidation
Distributed Queue	SC TaskProcessorQueue	queue/taskProcessorQueue
Distributed Queue	RF Executions Queue	queue/ReportingExecutions
Distributed Topic	SC taskStopperTopic	topic/taskStopperTopic

a. Click **Lock & Edit**.

b. Navigate to the Systinet JMS Module details page.

c. Click **New** in the Resources table.

d. Select the resource type and click **Next**.

e. Input the Name and JNDI Name. Leave blank all fields not included in the table and then click **Next**.

f. After you enter the values for a resource, target your cluster and click **Finish**.

10. Click **Activate Changes**.

Set Up the WebLogic Security Realm

In Systinet authentication is performed by the application server. You must set up the WebLogic Security Realm, otherwise you can only log in to Systinet with the WebLogic administrator credentials.

In the Domain Structure section of the Administration Console navigate to Security Realms. Click **Configure New Security Realms** in the **How do I...** section to open the WebLogic guide to setting up a security realm or changing the default realm.

Create your realm according to your requirements for LDAP and WebLogic user store rights.

Note: When using multiple Providers in your Security Realm, make sure that all providers have their Control Flag set to `SUFFICIENT`.

Any changes require a restart of the administration server and any managed servers.

Setting Up WebSphere

WebSphere requires initial configuration before you can deploy HP Systinet to it:

There are additional steps to complete deployment to WebSphere after installation. For details, see .

Set Up a WebSphere Cluster

Clustered deployment of HP Systinet is very similar to standalone deployment.

In all the following set up procedures, make sure to do the following:

- Whenever you select deployment scope, choose the cluster itself.

- When a restart is necessary, restart the whole cluster, including all servers joined to the cluster.

- When configuring a cluster, configure all servers within the cluster.

- When you deploy HP Systinet, map modules to servers by selecting the cluster and an instance of *IBM HTTP Server*.

The following procedure describes how to set up a proxied load balanced cluster with two servers running on one node.

To Create a Load Balanced Cluster:

1. Install and start *IBM HTTP Server*.

2. Create a new WebSphere cell (deployment manager and application server) profile, by doing the following:

   - Start the WebSphere Profile Management Tool.

   - Select **Cell**, and click **Next**.

   - Select **Advanced profile creation**.

   - Select **Deploy the administrative console** (recommended), and **Deploy the default application**.

   - Enter a unique Deployment Manager Profile Name (DMGR_NAME), Application Server Profile Name (APPSRV_NAME), and select a location for the new profile, and then click **Next**.

   - Enter the Deployment Manager Node Name and the Application Server Node Name.

     Note: These become the nodes containing the clustered servers.

     If necessary, correct the Host Name and Cell Name (CELL_NAME), and then click **Next**.

   - Select **Enable administrative security**, enter the administrator credentials, and then click **Next**.

   - If required, change the port values, and click **Next**.

   - Deselect **Run the deployment manager process as a Windows service**, and click **Next**.

   - Click **Next**, and then **Create**.

   - Deselect **Launch the First Steps Console**, and click **Finish**.

3. Start the deployment manager, application server node, and the application server:

   a. Execute the command:

      ```
      PROFILE_HOME/DMGR_HOME/bin/startManager
      ```

   b. Execute the command:

      ```
      PROFILE_HOME/APPSRV_HOME/bin/startNode
      ```

Note: If you want to run one or more nodes of the cluster on different machines, use the following procedure for each machine.

To apply a cluster to other machines:

a. Install IBM WebSphere®.

b. Start the WebSphere Profile Management Tool.

c. Click **Next**, and select **Custom Profile**.

d. Select **Advanced Profile Creation**.

e. Enter the Profile Name, for example, `HPsoaClusterAppsrv2`, and Profile Directory (PROFILE2_HOME).

f. Select **Make this profile default** and click **Next**.

g. Enter the Node Name (for example, `HpsoaClusterNode2`), and click **Next**.

h. Enter the Deployment Manager Hostname or IP Address, pointing to an existing deployment manager in a cell you want the new node to federate with.

   Set the credentials to administer the new deployment manager, optionally change the deployment manager port, and then click **Next**.

i. If necessary, change the port values, and click **Next**.

j. Start the node with the following command:

   PROFILE2_HOME/bin/startNode

   The new node should appear in the deployment manager admin console nodes listing, **System Administration→Nodes**.

4. To create the cluster:

   a. In your browser, open the WebSphere Administration Console:

      `http://localhost:9060/admin`

      Note: The port may vary depending on your settings.

   b. Select **Servers**, and select **Clusters**.

   c. Click **New**.

   d. Enter a cluster name (CLUSTER_NAME), select **Configure HTTP session memory-to-memory replication**, and then click **Next**.

   e. In the Select Basis for First Cluster Member, select **Create the member by converting an existing application server**, and click **Next**.

   f. Enter a new member name, for example `server2`, and click **Add Member**.

   g. Add servers as required.

      If you require a different node, select it from **Select Node**.

   h. Click **Next**, and **Finish**, and then **Save**.

Create a WebSphere Profile

For non-clustered deployment, create a clean WebSphere profile with the *Cell* environment. This

profile is stored in `WS_HOME/AppServer/profiles/PROFILE_NAME`.

Note: In this document, the path is referred to as `PROFILE_HOME`.

If you are using a web server such as IBM HTTP Server (IHS) as a proxy or load balancer, register it with the Deployment Manager. For details, see the WebSphere Help.

Create a WebSphere Mail Session

Create a mail session using the WebSphere Administration Console.

To Create a Mail Session:

1. Open the WebSphere Administration Console:

    - For Windows: `http://localhost:9060/ibm/console`

    - For Linux: `http://localhost:9062/ibm/console`

2. Select **Resources→Mail→Mail Sessions**.

3. Select your cell in the **Scope** drop-down field and click **New**.

4. Specify the mail session parameters as follows:

    - A unique, arbitrary descriptive name, for example `HP SOA Systinet Mail`.

    - The JNDI name `/Mail`.

    - Connection settings as per company email set up. You must set the `Outgoing Mail` server.

    - SMTP credentials if required.

Create JDBC Resources for WebSphere

Systinet requires an XA-enabled JDBC datasource to communicate with the database. JMS messaging requires a non-XA datasource.

Before creating these two datasources, you must create a JDBC provider for each of them.

Note: Systinet uses XA transactions. The application server transaction manager should be configured to have a minimum of 5 minutes for XA transaction timeout. For details, see your application server documentation.

Open the WebSphere Administration Console (http://localhost:9060/ibm/console) and create JDBC resources, in the order of the following sections:

1. Create a JDBC provider for an XA datasource

2. Create a JDBC provider for a non-XA datasource

3. Create an XA-enabled JDBC data source

4. Create a non-XA-enabled JDBC datasource

To Create a JDBC Provider for an XA Datasource:

1. Select **Resources→JDBC→JDBC Providers**.

2. For **Scope**, select your cell, and click **New**.

3. Select your database type.

4. Under Provider, select the driver for your database type.

   Note: For DB2, if there is more than one driver available, select the DB2 Universal driver.

   Note: For Oracle, if there is more than one driver available, select a "Thin" driver.

5. For the implementation type, select **XA data source**.

   The Name is automatically completed with the driver name, followed by `(XA)`.

6. For the value of the variable `${driver_name_PATH}`, enter the location of the driver.

   Note: DB2 driver files are in `IBM_HOME/SQLLIB/java` by default.

7. Click **Finish**.

To Create a JDBC Provider for a Non-XA Datasource:

- Repeat the procedure "To Create a JDBC Provider for an XA Datasource", with the following exceptions:

   Select the implementation type **Connection pool data source**.

   The automatically generated name should not end in `(XA)`.

Note: If you get the error DSRA3602E, refer to Wsadmin scripting fails with DSRA3602E.

To Create an XA Enabled JDBC Datasource:

1. Select **Resources**→**JDBC**→**Data Sources**.

2. For **Scope**, select your cell, and then click **New**.

3. Give the data source a unique, arbitrary descriptive name, for example, `HP Systinet DS`.

4. Give the datasource the JNDI name `hpsystinetDS`.

   Note: JNDI names must be exact.

5. Click **Next**.

   The Select JDBC Provider page opens.

6. Select **Select an existing JDBC provider**, select the XA JDBC provider you previously created, and then click **Next**.

   The Database Properties page opens.

7. The database properties you enter depend on the type of database you are using:

   For DB2:

   - Enter the database name, such as `platform`. Your database administrator can tell you this name.

   - From the **Driver type** drop-down field, select driver type "4".

   - Enter the server name.

- Enter the port number if it differs from the default `50000`.

- Deselect **Use this datasource for CMP**.

For Oracle:

- Type the full URL of the database you plan to use for HP Systinet, such as `jdbc:oracle:thin:@server:1521:database`

- From the drop-down field, select the data store helper class name for your version of the database.

- Deselect **Use this datasource for CMP**.

8. Click **Next** and leave all fields set as `(none)`.

9. Click **Next** to see the summary and then click **Finish**.

10. Open the newly created data source and create an authentication alias:

   - Click **JAAS - J2C Authentication Data**.

     A list of authentication aliases opens.

   - Click **New**.

   - Give an arbitrary string value for the alias, for example, `HP Systinet Credentials`.

   - For credentials, enter the user name and password for the database you use with HP Systinet.

   - Click **Finish**.

11. Reopen the newly created datasource and apply the new authentication alias:

   - In Component-Managed Authentication Alias, select the previously created authentication alias.

   - Under Authentication Alias for XA Recovery, select **Use Component-Manager Authentication Alias**.

   - Under Container-Managed Authentication, for the Mapping Configuration Alias, select **DefaultPrincipalMapping**.

   - Click **OK**.

12. Reopen the datasource and increase its connection pool size:

   - Under Additional Properties, click **Connection pool properties**.

     The Connection Pool page opens.

   - For Maximum Connections, type a number equal to at least 1/4 of the number of parallel requests that you require to be handled simultaneously. If you do not have an estimate of this number, set the maximum connections to 100.

   - For Minimum Connections, type a number equal to the number of expected concurrent users.

   - Click **OK**.

13. Click **Test connection** to make sure that your datasource configuration is correct.

Note: If you get the error "Connection not available, Timed out waiting for 180000" in the log file, you can do any of the following:

- Increase the Maximum connections property in **Resources→JDBC→Datasources→HP Systinet DS for Oracle→Connection pool properties** (or specify 0 for no connection count limit)

- Increase the value Connection Timeout property in **Resources→JDBC→Datasources→HP Systinet DS on Oracle→Connection pool properties** (default is 180 seconds). Setting 0 (infinite waiting for connection) is not recommended because of a risk of deadlocks.

To Create a Non-XA Enabled JDBC Datasource:

- Repeat the procedure "To Create an XA-Enabled JDBC Datasource", with the following exceptions:

  - Give the non-XA datasource the JNDI name, `jms-hpsystinetDS`.

    Note: JNDI names must be exact.

  - Select the non-XA JDBC provider.

  - Use the same authentication alias you created for the XA-enabled datasource.

After creating JDBC resources, restart the WebSphere Deployment Manager.

Create a WebSphere Messaging Bus

In WebSphere, JMS communication and the persistent storage of that communication are handled via a bus.

To Create a Messaging Bus:

1. Open the WebSphere Administration Console:

   `http://localhost:9060/ibm/console`

2. Select **Service Integration→Buses**.

   The Buses page opens.

3. Click **New**.

   The Create a New Messaging Engine Bus wizard opens.

4. Give the bus a unique, arbitrary descriptive name, for example, `SOABus`.

5. Deselect **Bus Security**, as it is not required, and click **Next**.

6. Click **Finish**.

   The Buses page reopens.

7. Click the name of the bus you created to open its details page.

8. Click **Bus members**.

   The Bus members page opens.

9. Click **Add**.

   The Add a New Bus Member wizard opens.

10. Select a standalone server or cluster that will host Systinet, and click **Next**.

    The Select Type of Message Store page opens.

11. Select **Data store** for the type of message store, and click **Next**.

12. Enter the message store properties for the bus.

    Note: You can use the existing `jms-hpsoasystinetDS` data source but you might prefer to use a different data source for performance reasons.

    If you use an existing data source, for the Schema Name, type the database user name, set the Authentication Alias to `HP SOA Systinet Credentials`, select **Create Tables**, and then click **Next**.

13. Review your selected options and click **Finish**.

    The Bus Members page reopens.

14. Repeat Step 9 to Step 13 for every standalone server and cluster that will host Systinet.

15. Return to the bus details page.

    The Configuration tab is open by default.

16. Under Destination Resources, click **Destinations**.

    A table of destinations opens.

17. Add the following destinations by clicking **New**:

Destination type	Identifier
Queue	scheduleTimerQueue
Queue	ReportingExecutions
Queue	Validation
Queue	Priority Validation
Queue	taskProcessorQueue
Topic Space	taskStopperTopic

Set Up JMS in WebSphere

Systinet requires JMS messaging resources that you must set up in the WebSphere Administration Console.

Note: You can configure JMS to meet your requirements. This section describes a JMS set up that ensures that JMS resources are accessible by Systinet and function correctly.

To set up JMS:

1. Open the WebSphere Administration Console:

   `http://localhost:9060/ibm/console`

2. Select **Resources→JMS**.

3. Add the resources listed in the JMS Resources table.

JMS Resources

Resource Type	Name	JNDI Name
Queue Connection Factory	RF Connection Factory (Send)	jms/ReportingSenderConnectionFactory
Queue Connection Factory	RF Connection Factory (Rec)	jms/ReportingReceiverConnectionFactory
Queue Connection Factory	SOA Queue Connection Factory	jms/SOAQueueConnectionFactory
Topic Connection Factory	SOA Topic Connection Factory	jms/SOATopicConnectionFactory
Queue	SC scheduleTimer Queue	queue/scheduleTimerQueue
Queue	PM Validations Queue	queue/Validation
Queue	PM Priority Validations Queue	queue/PriorityValidation
Queue	SC TaskProcessorQueue	queue/taskProcessorQueue
Queue	RF Executions Queue	queue/ReportingExecutions
Topic	SC taskStopperTopic	topic/taskStopperTopic

For each resource:

a. Under JMS, click the resource type.

b. Select the scope created in during "Creating a WebSphere Profile", and click **New**.

c. Select Default Messaging Provider, and click **OK**.

d. Use the parameters from the JMS Resources table.

e. Use the bus you created during "Create a WebSphere Messaging Bus".

f. Where a Queue Name, or Topic Space is required, select the relevant queue or topic that you created in Step 17 of "Create a WebSphere Messaging Bus".

g. Click **OK**.

4. Modify the connection pool for the SOA Queue and the SOA Topic connection factories, by doing the following:

   ▪ Select the connection factory to modify.

   ▪ Under Additional Properties, click **Connection Pool Properties**.

- Change Maximum Connections to `100`.

- Click **OK**.

5. Select **Resources→Asynchronous Beans**, and select **Work Managers**.

6. Select the scope you created during "Create a WebSphere Profile", and click **New** to create the following work managers:

   - **SC Work Manager**

     Set JNDI Name `/wm/platform`, change Maximum Number of threads to `100`, and select **Growable**.

     Caution: The leading forward slash is required for the JNDI name in this case.

   - **RF Work Manager**

     Set JNDI Name `wm/reporting`.

7. Set the specifications listed in the JMS Activation Specifications table:

JMS Activation Specifications

Name	JNDI Name	Destination JNDI Name
RF Activation	jms/RFActivation	queue/ReportingExecutions
PM Activation	jms/PMActivation	queue/Validation
PM Priority Activation	jms/PMPriorityActivation	queue/PriorityValidation
PL Scheduler Timer Queue Activation	jms/PLSchedulerTimerQueueActivation	queue/scheduleTimerQueue
PL Task Runner Queue Activation	jms/PLTaskRunnerQueueActivation	queue/taskProcessorQueue
PL Task Stopper Topic Activation	jms/PLTaskStopperTopicActivation	topic/taskStopperTopic

For each specification:

a. Under JMS, click **Activation Specifications**.

b. Select the scope created during "Create a WebSphere Profile", and then click **New**.

c. Select **Default Messaging Provider**, and then click **Next**.

d. Use the parameters from the JMS Activation Specifications table.

e. Use the appropriate Destination Type `Queue` or `Topic` for each resource.

f. Use the bus you created during "Create a WebSphere Messaging Bus".

g. Click **OK**.

8. Expand **Service Integration**, and select **Buses**.

9. Select the bus you created during "Create a WebSphere Messaging Bus".

10. In the Topology section, click **Messaging Engines**.

11. Copy the name of the messaging engine to the clipboard.

12. Select **Resources→JMS**, and select **Activation Specifications**.

13. "Maximum Concurrent Endpoints" must be decreased to 3 on "PM Activation" in JMS - Activation specifications.

    "Maximum Concurrent Endpoints" must be decreased to 2 on "PM Priority Activation" in JMS - Activation specifications.

14. Select **PL Task Stopper Topic Activation**.

15. In the Subscription Durability section, add the following parameters:

    - Leave Subscription Durability as non-durable.

    - Enter a subscription name, for example, `PL Task Stopper Subscription Name`.

    - Enter a client identifier, for example, `PL Task Subscription ID`.

    - Paste the messaging engine name as the Durable Subscription Home.

16. Click **OK**.

Configure WebSphere Container Settings

To configure WAS:

1. Click **Servers→ Application servers→server_name** .

2. Under **Container Settings**, expand **Web Container Settings** and click **Web container transport chains**.

3. Click **WCInboundDefaultSecure →HTTP Inbound channel (HTTP_4)**

4. Under **Transport Channels**, click **HTTP Inbound Channel (HTTP_4)**.

5. Under **Additional properties**, click **Custom Properties→New** .

6. Enter property `CookiesConfigureNoCache`, value `false`

7. Click **Apply** or **OK**.

8. Click **Save** to save your configuration changes, then restart the server.

Set WebSphere Startup Parameters

Systinet requires several parameters to be set in order to function correctly.

Use the WebSphere Administration Console to set these startup parameters.

To Set the Startup Parameters:

1. In your browser, open the WebSphere Administration Console:

   `http://localhost:9060/ibm/console`

2. Expand **Servers**, expand **Server Types**, and select **WebSphere Application Servers**.

3. Select the server.

4. In the Server Infrastructure section, expand **Java and Process Management**, and select **Process Definition**.

5. In the Additional Properties section, select **Java Virtual Machine**.

6. Set the following properties:

   - Initial Heap Size `1000`

   - Maximum Heap Size `1536` for 32-bit JDKs, `4096` for 64-bit JDKs.

   - Generic JVM Arguments `-XX:MaxPermSize=256m`

   Note: Memory sizing should take performance requirements into consideration for the deployed system. These settings are only a recommendation.

   Note: Heap size recommendations depend on the number of concurrent users. Based on HP measurements on a 64-bit server using JDK 1.6.0_16 (Java version: 1.6.0_16,Sun Microsystems Inc.Java VM: Java HotSpot(TM) 64-Bit Server VM 14.2-b01,Sun Microsystems Inc.)

   -Xmx:

   - 50 users: 1700m

   - 100 users: 2200m

   - 150 users: 3000m

   - 300 users: 4000m

   Other recommended JVM options:

   - Memory saving: `-XX:+UseParallelOldGC -XX:+UseCompressedOops`

   - In case of occasional memory and performance issues even with the recommended heap size: `-XX:SoftRefLRUPolicyMSPerMB=0`

   - For debugging: `-XX:+PrintCommandLineFlags`

   Caution: If you use a UNIX operating system, also add the following property: Generic JVM Arguments `-Djava.awt.headless=true`

   Tip: To enable non-Latin characters in HTTP parameters on behalf of Systinet set the following Generic JVM Arguments:

   - `-Dclient.encoding.override=UTF-8`

   - `-Ddefault.client.encoding=UTF-8`

7. Click **OK**.

Note: You must restart the server for these changes to take effect.

Finish WebSphere Cluster Setup

1. To add a web server node to the cluster:

a. In your browser, open the WebSphere Administration Console:

   `http://localhost:9060/admin`

   Note: The port may vary depending on your settings.

b. Select **Servers→Web Servers**, and click **New**.

c. Enter a Server Name, for example, `IHS_NAME`, and click **Next** twice.

d. Enter the Web Server Location, which should be the installation directory for *IBM HTTP Server* (IHS_HOME), and the a Plug-in Installation Location, usually, `IHS_HOME/Plugins`.

e. Click **Next**, and **Finish**, and then **Save**.

2. For debug purposes, add an alias to the default virtual host to enable direct access to applications on all clustered servers, by doing the following:

   a. In your browser, open the WebSphere Administration Console:

      `http://localhost:9060/admin`

      Note: The port may vary depending on your settings.

   b. Select **Environment**, and select **Virtual Hosts**.

   c. Click **default_host**, and then click **Host Aliases**.

   d. Click **New**.

   e. Enter the value for the second clustered server port, usually **9081**, click **OK**, and then click **Save**.

      Repeat this step for as many servers as you require, in addition to adding their ports.

3. Regenerate the routing information for the web server.

   Select **Servers→Web Servers**, and select `IHS_NAME`, and then select **Generate Plug-in** and **Propagate Plug-in**.

Setting Security Custom Properties

To add a security custom property:

Set `com.ibm.ws.security.addHttpOnlyAttributeToCookies` to the value `true`.

How to set a custom property on IBM WebSphere Application Server Version 7 or Version 8:

1. In the administrative console, click **Servers** and under Servers click **Server Types** and under Server Types click **WebSphere application servers**.

2. Click on the server to which the custom property is to be applied.

3. Under **Configuration** and **Container settings** click **Web Container Settings** and under Web Container Settings click **Web container**.

4. Under **Configuration** and **Additional Properties** click **Custom Properties**.

5. In the Custom Properties page, click **New**.

6. In the settings page, enter the name of the custom property to be added in the **Name** field and the value to be set for the custom property in the **Value** field. Note that some properties are case sensitive.

7. Click **Apply** or **OK**.

8. Click **Save** in the **Messages** box that appears.

9. Restart the server for the custom property to take effect.

Chapter 5

Preparing LDAP and SiteMinder

Depending on your deployment you may want to integrate with LDAP or SiteMinder.

The set up of each, prior to Systinet installation, is explained in the following sections:

Prepare LDAP Integration

Automatic Service Discovery

The automatic discovery of LDAP servers means you do not have to hardwire the URL and port of the LDAP server. Instead you can use `ldap:///o=JNDITutorial,dc=example,dc=com` as a URL, and the real URL is deduced from the distinguished name `o=JNDITutorial, dc=example,dc=com`.

Automatic discovery of the LDAP service using the URL's distinguished name is supported only in Java 2 SDK, versions 1.4.1 and later, so make sure that your Java version supports this.

LDAP Service Properties

Systinet integration with LDAP uses a JNDI interface to connect to LDAP servers.

For more information, about the JNDI API, see http://java.sun.com/products/jndi/tutorial/ldap/connect/create.html and http://java.sun.com/j2se/1.5.0/docs/guide/jndi/jndi-dns.html#URL .

The following JNDI properties must be known to the server:

Property Name	Property Description	API Link
Naming Provider URL	URL of the LDAP service.	http://java.sun.com/j2se/1.5.0/docs/a-pi/javax/naming/Context.html#PROVIDER_URL
Initial Naming Factory	Java class for the initial naming factory.	http://java.sun.com/j2se/1.5.0/docs/a-pi/javax/naming/Context.html#INITIAL_CONTEXT_FACTORY
Security Prin-	The name of	http://java.sun.com/j2se/1.5.0/docs/a-pi/javax/naming/Context.html#SECURITY_PRINCIPAL

Prop- erty Name	Property Descrip- tion	API Link
cipal	the security principal for read access to the directory service.	
Pass- word	Pass- word of security principal.	http://java.sun.com/j2se/1.5.0/docs/a- pi/javax/naming/Context.html#SECURITY_CREDENTIALS
Secu- rity Pro- tocol	Name of the security protocol. Default is "simple."	http://java.sun.com/j2se/1.5.0/docs/a- pi/javax/naming/Context.html#SECURITY_PROTOCOL

Set Up SiteMinder Endpoint Authentication

In Siteminder, configure Systinet endpoint authentication.

By default, Systinet performs the following authentication on Systinet endpoints:

- **FORM authentication**:

  - /web/service/catalog/*

  - /web/policy-manager/*

  - /web/shared/*

  - /web/artifactIconList.htm

- **HTTP basic authentication**:

  - /systinet/platform/restBasic/*

  - /platform/restSecure/*

  - /policymgr/restSecure/*

  - /reporting/restSecure/*

  - /remote/navigator/*

  - /remote/upload/*

- **Unauthenticated URL patterns:**

- /systinet/platform/rest/*

- /platform/rest/*

- /policymgr/rest/*

- /reporting/rest/*

- /web/design/*

- /remote/dql/*

Note: All endpoints are preceded by `http(s):/host:port/context` as set during installation.

Chapter 6

Using the GUI Installer

Using the GUI Installer is the easiest way to install HP Systinet. However, it may not be suitable for all the configuration options required by production environments.

Before using the GUI Installer, make sure that you have a correctly set up environment.

For hardware and software requirements, as well as supported platforms, see "Prerequisites and Supported Platforms" (on page 12).

For an evaluation environment, you need valid credentials to a configured database. For details, see "Preparing Databases" (on page 19).

JBoss does not require any additional configuration for evaluation purposes. If you are using the GUI installation for a production environment with JBoss or for a different application server, see "Setting Up Application Servers" (on page 29).

GUI installation consists of the following steps:

1. "Start GUI Installation" (on page 74)

2. "GUI Installation - Welcome" (on page 76)

3. "GUI Installation - License" (on page 77)

4. "GUI Installation - Installation Folder" (on page 78)

5. "GUI Installation - Scenario Selection" (on page 79)

6. "GUI Installation - License Information" (on page 80)

7. "GUI Installation - Updates" (on page 81)

8. "GUI Installation - Custom Extensions" (on page 82)

9. "GUI Installation - Password Encryption" (on page 83)

10. "GUI Installation - Database Selection" (on page 84)

11. "GUI Installation - Database Setup" (on page 85)

12. "Database Parameters" (on page 86)

  - "GUI Installation - DB2 Create Tablespace" (on page 87)

  - "GUI Installation - DB2 Create Schema" (on page 89)

  - "GUI Installation - MSSQL Create Database" (on page 91)

  - "GUI Installation - MSSQL Create Schema" (on page 93)

  - "GUI Installation - Oracle Create Tablespace" (on page 95)

  - "GUI Installation - Oracle Create Schema" (on page 97)

13. "GUI Installation - JDBC Drivers" (on page 99)

In the cases of Decoupled Database or JDKless Deployment, there are additional required steps after GUI installation is complete. For details, see "Completing GUI Installation" (on page 115).

Start GUI Installation

1. Make sure the application server is not running.

2. Do one of the following:

   ▪ Execute the file `hp-systinet-4.10.jar`, located on the installation CD or in your distribution directory.

   ▪ Execute the following command:

     java -jar hp-systinet-4.10.jar

   ▪ For manual database deployment, execute the following command:

     java -jar hp-systinet-4.10.jar -a

   ▪ For deployment not using the JDK, generate the installation configuration file:

     java -jar hp-systinet-4.10.jar -s deployment.properties

     Caution: For JBoss with HP-UX, execute the following command instead:

     java -jar hp-systinet-4.10.jar -Dshared.as.jboss.preloading.classes.at.startup=true

     Caution: Installation with some DB2 JDBC drivers does not manage explicit SQL commit commands in auto-commit mode. If commit errors occur during installation with DB2, execute the following command instead:

     java -jar hp-systinet-4.10.jar -Dshared.installer.db.exclude.commits=true

   The GUI Installation wizard opens displaying the Welcome page.

Continue to .

The install command has the following additional options:

- **-h, --help**

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

- **-x, --extract** *PATH*

  Extract the installation archive to the specified location.

- **-i, --install-to** *SYSTINET_HOME*

  Install HP Systinet in console mode to the specified location. Normally used in conjunction with **-u**.

- **-s, --save-config** *FILE*

  Execute the GUI Installation, but save the configuration to the specified file instead of installing HP Systinet.

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

  Run the installation in decoupled database mode.

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

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

- **--passphrase *PASSPHRASE***

If you want to use password encryption, specify the passphrase to use for encryption.

- **-d, --debug**

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

GUI Installation - Welcome

In the Welcome page, review the hardware and software requirements.
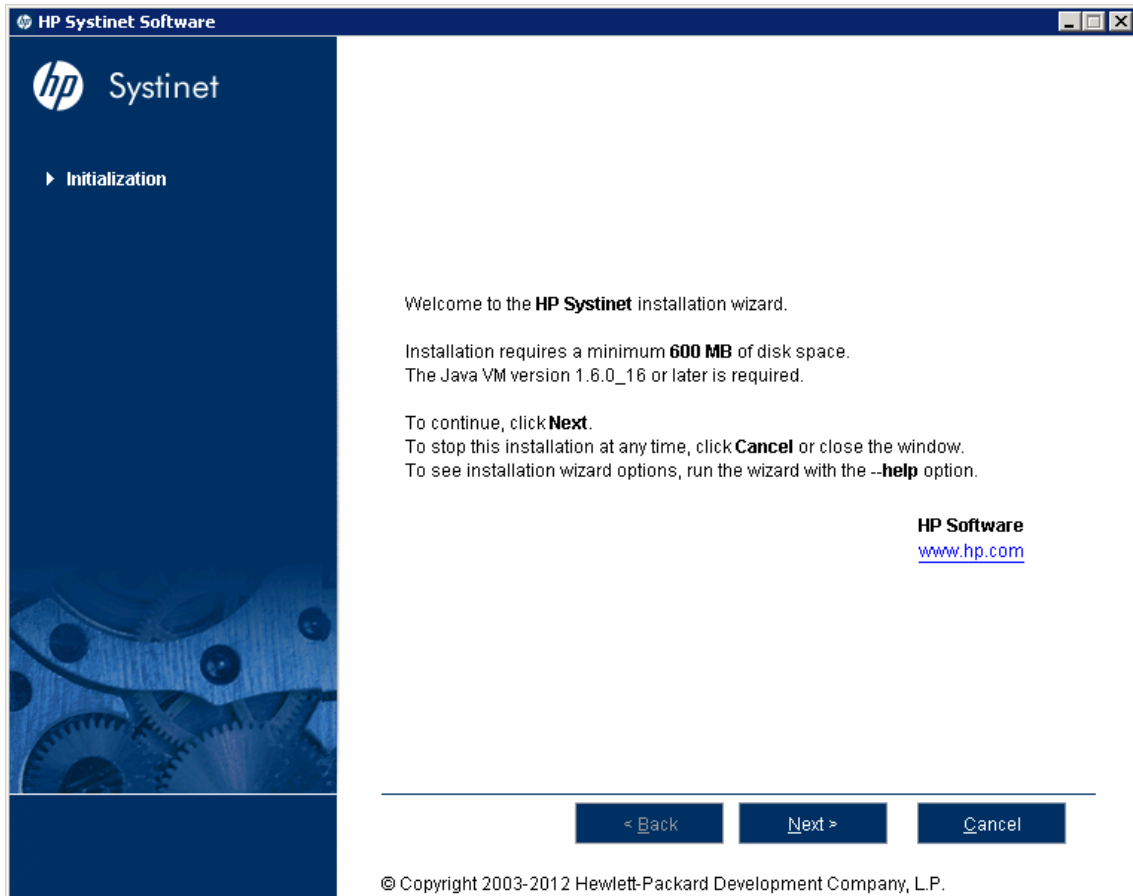
Click **Next** to open the License page.

Continue to .

GUI Installation - License

In the License page, review the license. The License page shows the license in English, German, Spanish, and French.
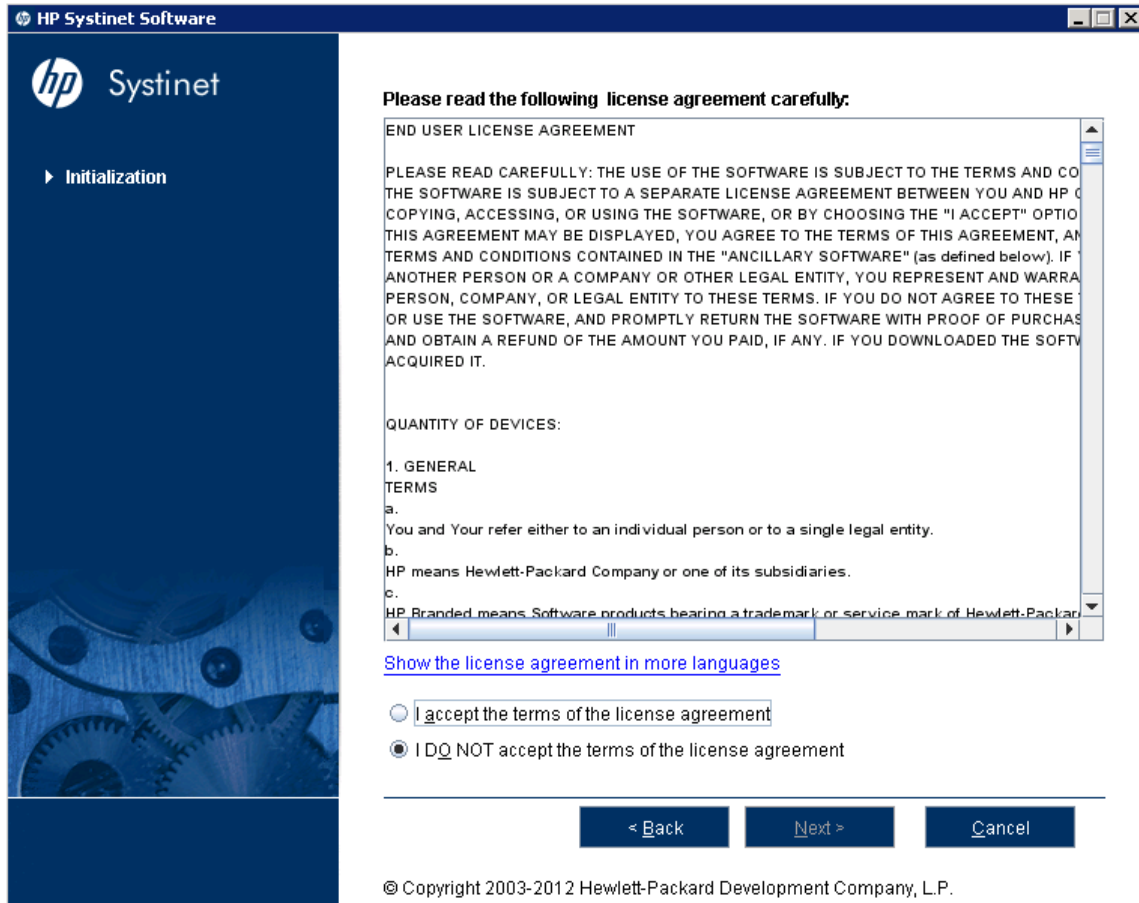
Click **Show the license agreement in more languages** to open a PDF which also contains the license agreement in Japanese, Korean, Chinese, and Taiwanese.

Select **I Accept the Terms of the License Agreement**, and then click **Next** to open the Installation Folder page.

Continue to .

GUI Installation - Installation Folder

In the Installation Folder page, input or click **Browse** to select the location you want to use as your Systinet installation folder.
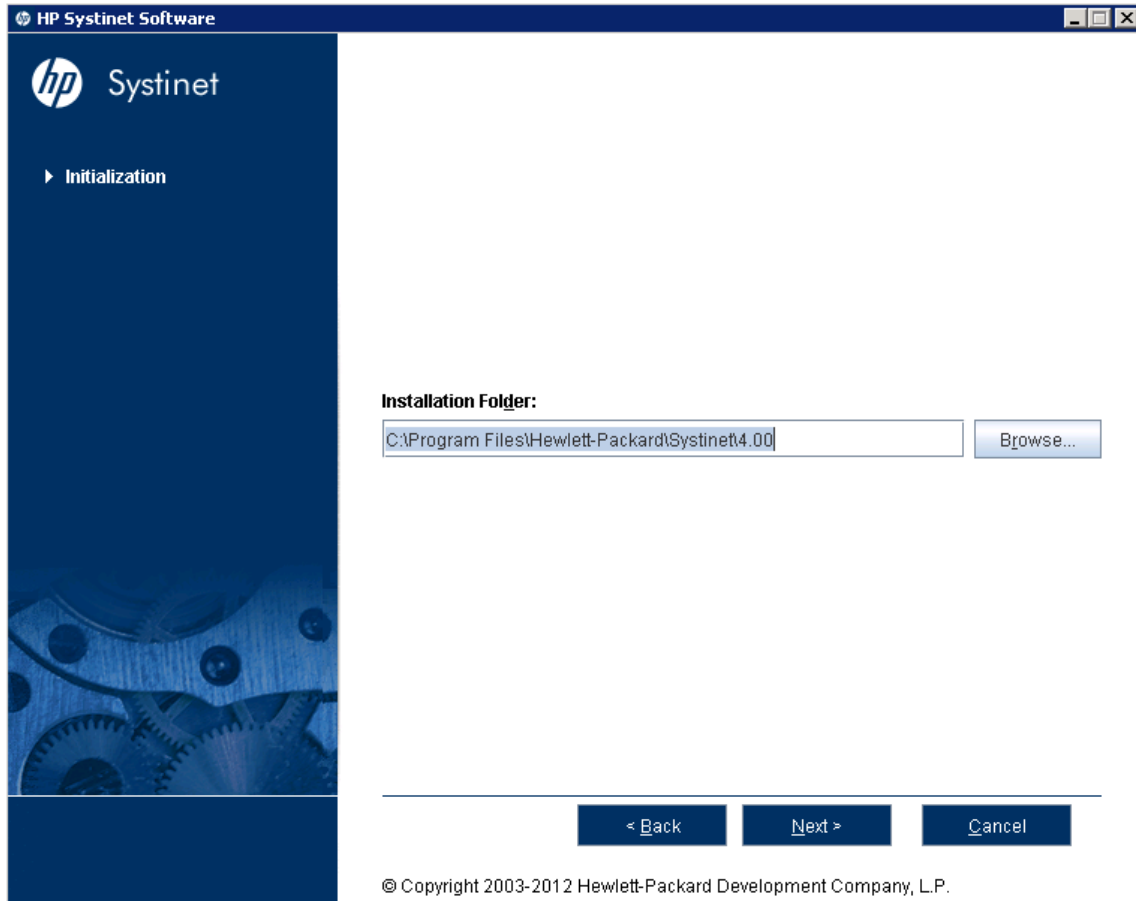
Caution: If you are upgrading from HP SOA Systinet 3.x, install to a new installation directory.

Click **Next** to unpack the distribution files to the chosen location and open the Scenario Selection page.

Note: In this document, the installation location is referred to as SYSTINET_HOME.

Caution: The location name cannot contain more than 80 characters.

Continue to .

GUI Installation - Scenario Selection

In the Scenario Selection page, select **Default**.
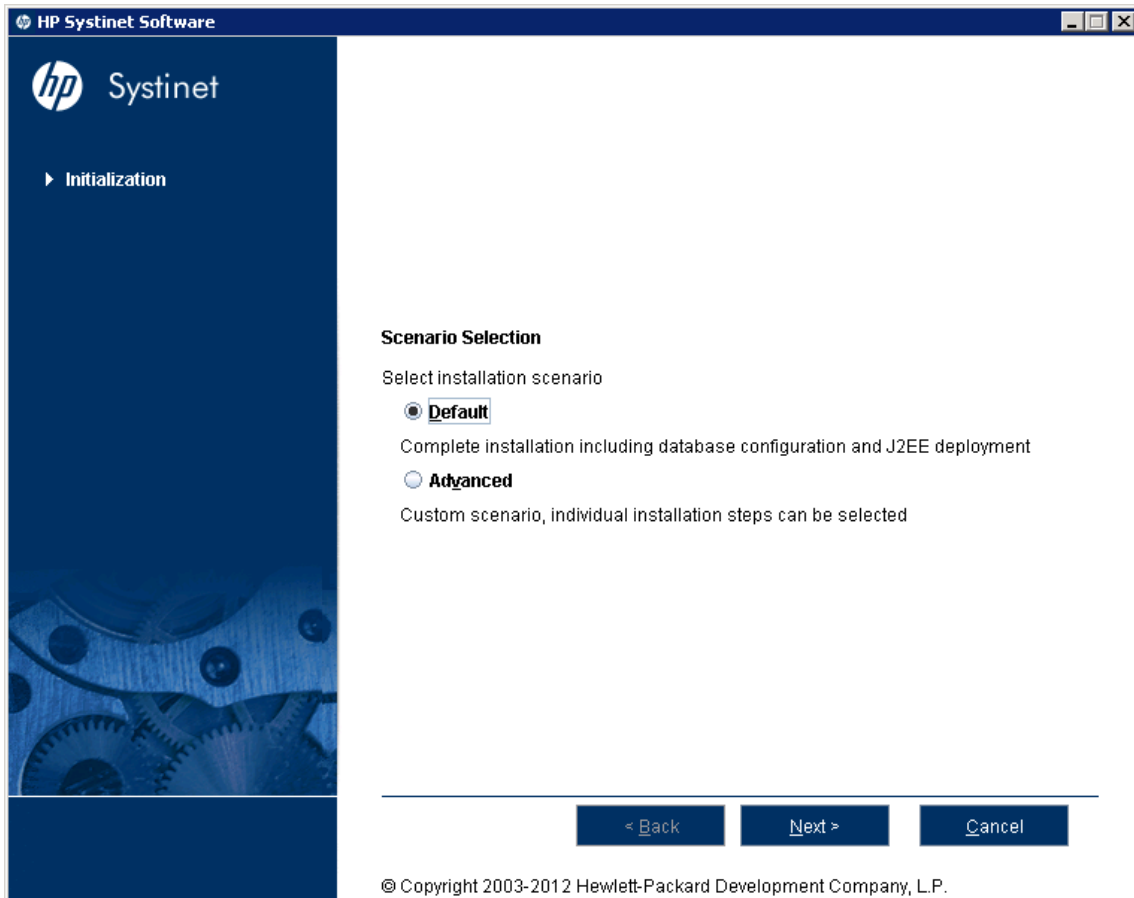
Note: The **Advanced** scenarios enable you to perform parts of the installation separately. These functions are duplicated by the Setup Tool and are discussed as administration functions. For details, see "Setup Tool" in the *Administrator Guide*.
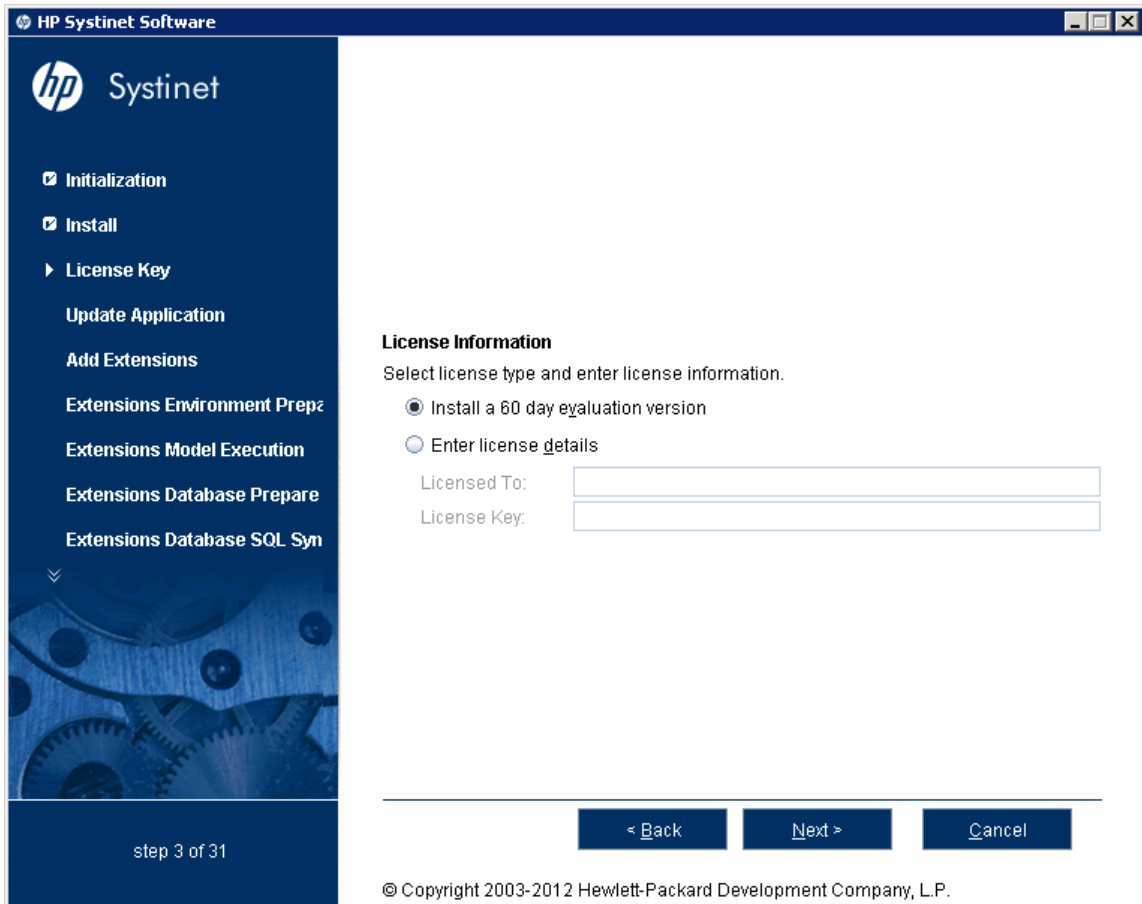
Click **Next** to validate the installation and open the License Information page.

Continue to .

GUI Installation - License Information

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

- Select **Install a 60 day evaluation license**.

- Select **Enter license details** and type the license details provided by your sales representative.

Click **Next** to open the Updates page.

Note: The administrator can change the license at a later date. For details, see "License Management" and "Managing the License" in the *Administrator Guide*.

Continue to .

GUI Installation - Updates

In the Updates page, use **Add** and **Remove** to select updates to apply during installation.
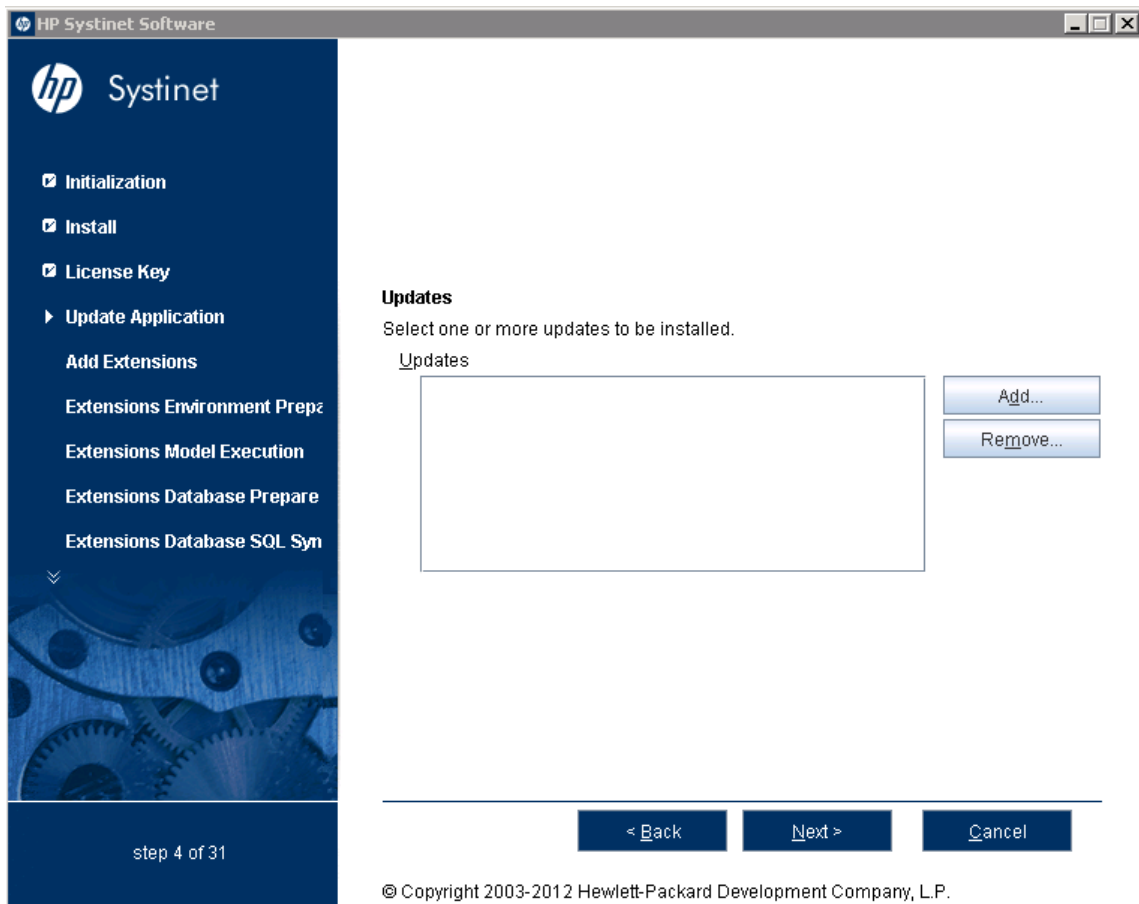
Click **Next** to verify any selected updates and open the Custom Extensions page.

Continue to "GUI Installation - Custom Extensions" (on page 82).

GUI Installation - Custom Extensions

In the Custom Extensions page, use **Add** and **Remove** to select extensions to apply during installation.
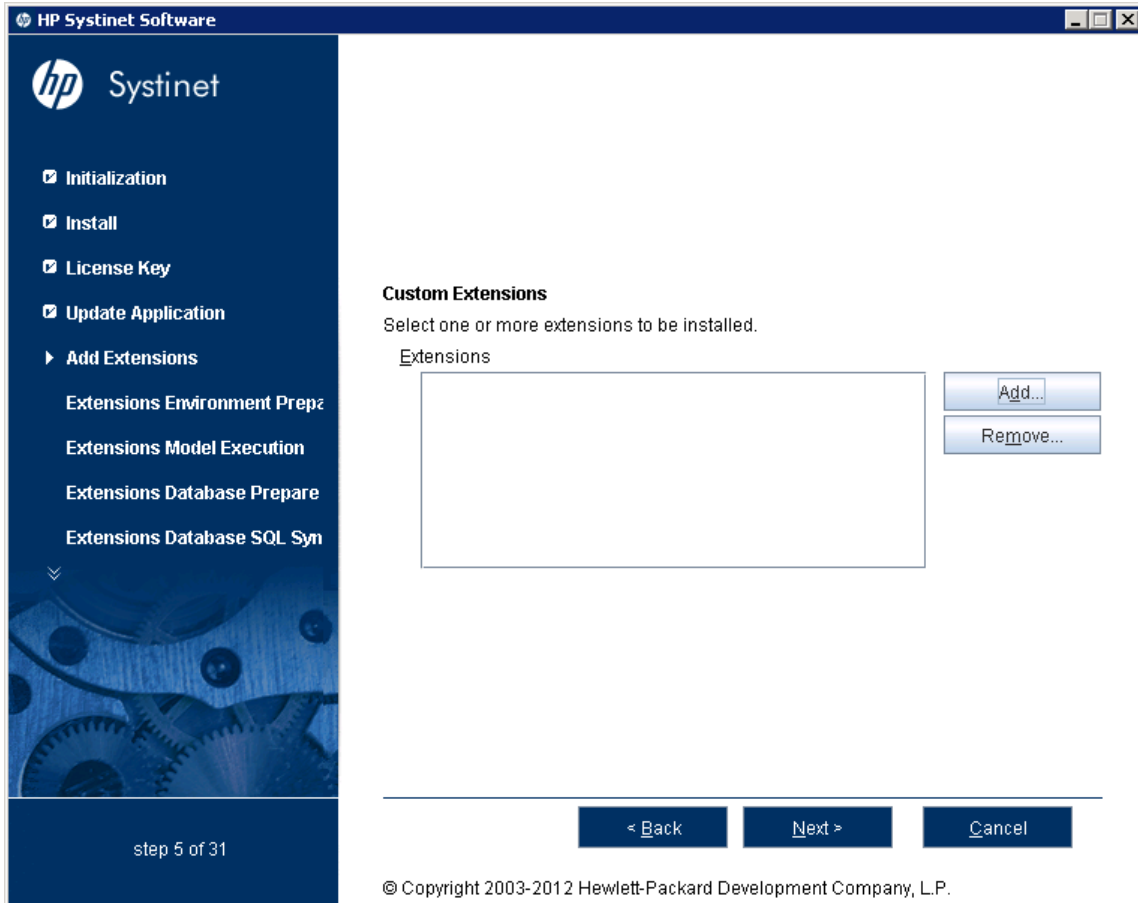
Click **Next** to validate any selected extensions and open the Password Encryption page.

Continue to "GUI Installation - Password Encryption" (on page 83).

GUI Installation - Password Encryption

In the Password Encryption page select whether Systinet protects credentials for access to other systems with strong encryption.

1. Do one of the following:

   - For production or sensitive installations, select **Enable**, type the Master Passphrase and Confirm Passphrase.

   - For demo installations, select **Disable**, and then click **Next**.

2. Click **Next** to validate the encryption and open the Database Selection page.

3. Click **Next** to validate the encryption and open the Repository Import page.

Note: After installation with encryption, all passwords stored in the configuration file are in an encrypted form unreadable without the provided passphrase. For executions of the Setup Tool and some other command line tools you may need to enter passphrase or provide it using the **--passphrase** command line option.

Continue to .

GUI Installation - Database Selection

In the Database Selection Page, select the database type to use.
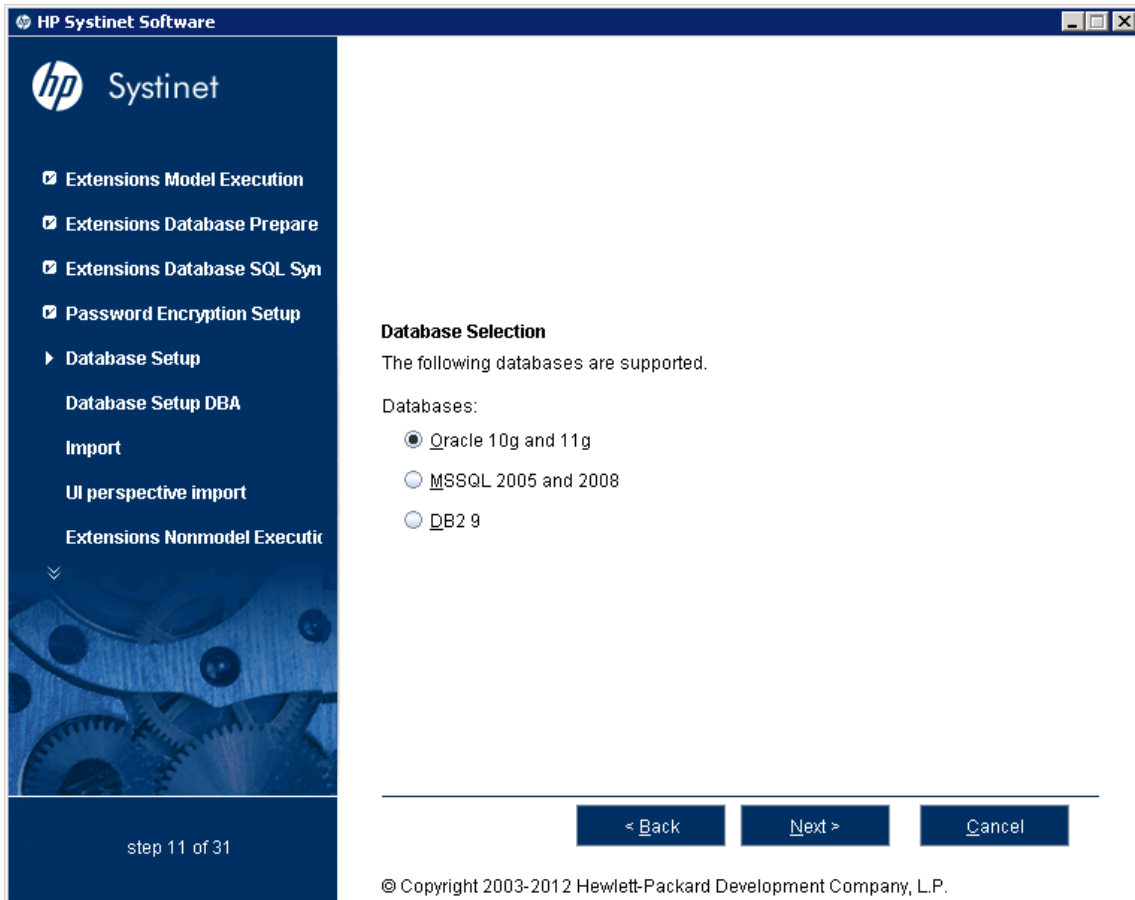
Select your database type and click **Next** to open the Database Setup Operations page.

Continue to "GUI Installation - Database Setup" (on page 85).

GUI Installation - Database Setup

In the Database Setup Operations page, select your database installation type.
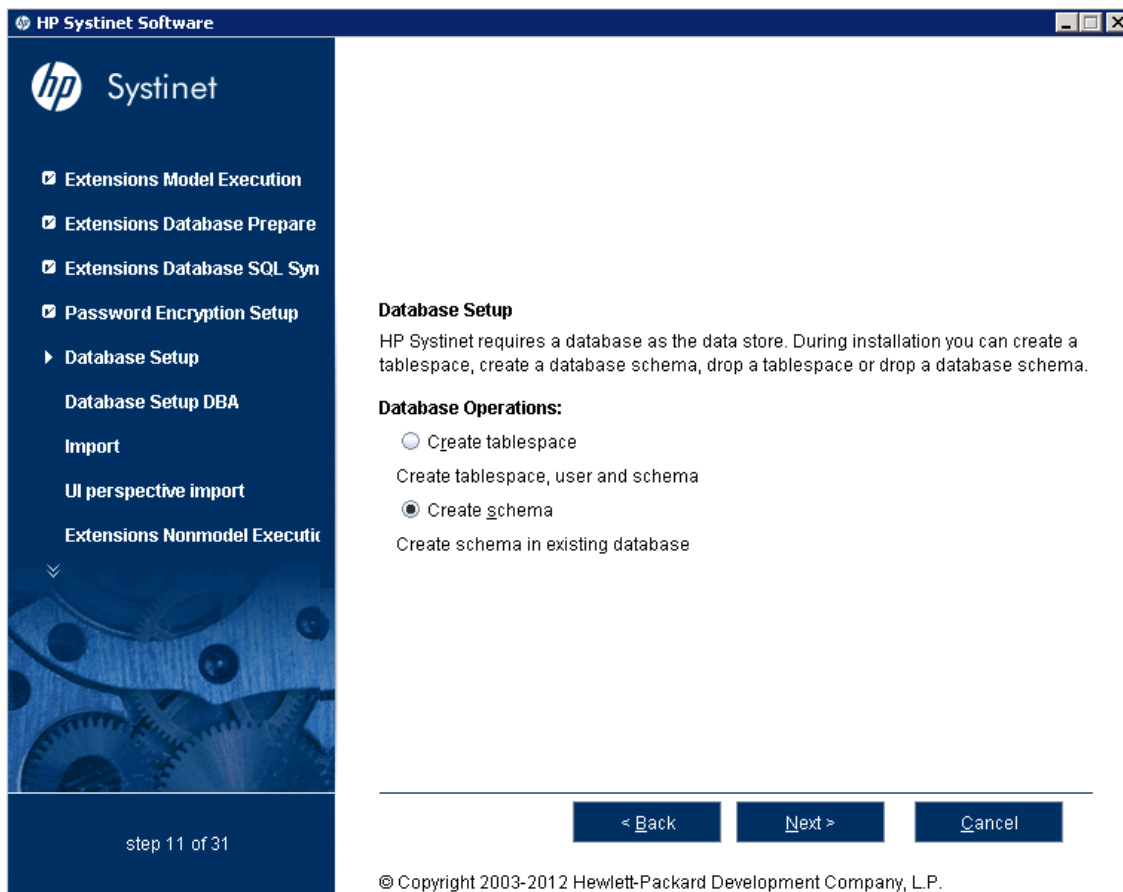
Click your required database setup type and click **Next** to open a Database Options page specific to the database and database installation type.

Continue to the appropriate DB Options page:

Database Parameters

The required database parameters vary depending on your database type and setup type.

For details, see the appropriate section:

GUI Installation - DB2 Create Tablespace

To create a new tablespace in DB2, set the following parameters:

DB2 Create Tablespace Parameters

| Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	In the database connection string `jdbc:db2://dbhost42:50000/platform`, the hostname is `dbhost42`.
Database Server Port	Connection port for the database.	In the database connection string `jdbc:db2://dbhost42:50000/platform`, the port number is `50000`.
Existing Database Name	Name of the database.	In the database connection string `jdbc:db2://dbhost42:50000/platform`, the database name is `platform`.
Database Administrator Name	User name and password of the administrator of the database.	—
Database Administrator Password		
New Database Tablespace	Name of the tablespace to create	The tablespace name must not conflict with existing objects in the database.
Tablespace Datafile	Path to the tablespace datafile that is stored on the database host machine.	
Existing Database User Name	Name and password of an existing database user.	—
Database User Password		
Buffer Pool /with 32k page size/	Buffer pool to use for the tablespace.	

Click **Next** to open the JDBC Drivers page.
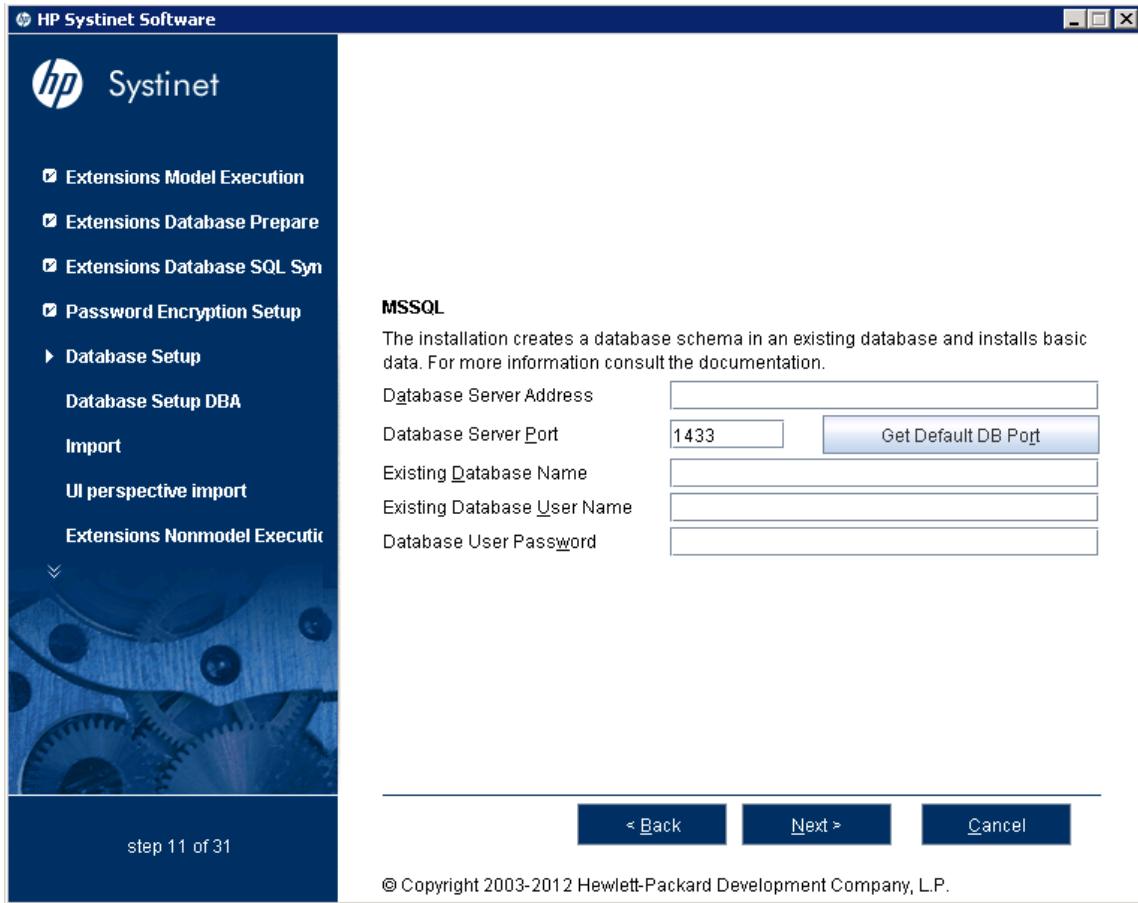
Continue to "GUI Installation - JDBC Drivers" (on page 99).

GUI Installation - DB2 Create Schema

To create a new schema in DB2, set the following parameters:

DB2 Create Schema Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:db2://dbhost42:50000/platform`, the hostname is `dbhost42`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:db2://dbhost42:50000/platform`, the port number is `50000`.
Existing Database Name	Name of the database.	For example, in the database connection string `jdbc:db2://dbhost42:50000/platform`, the database name is `platform`.
Existing Database User Name	User name and password of an existing database user.	—
Database User Password		
Database Tablespace	Existing tablespace to use for the new schema.	

Click **Next** to open the JDBC Drivers page.

Continue to "GUI Installation - JDBC Drivers" (on page 99).

GUI Installation - MSSQL Create Database

To create a new database in MSSQL, set the following parameters:

MSSQL Create Database Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform`, the hostname is `sqlhost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform`, the port number is `1433`.
New Database Name	Name of the database.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform`, the database name is `platform`.
Existing Database User Name Database User Password	For the Create Database option the user must have the database creator role. When using `integratedSecurity`, just fill non-blank text (dummy).	—
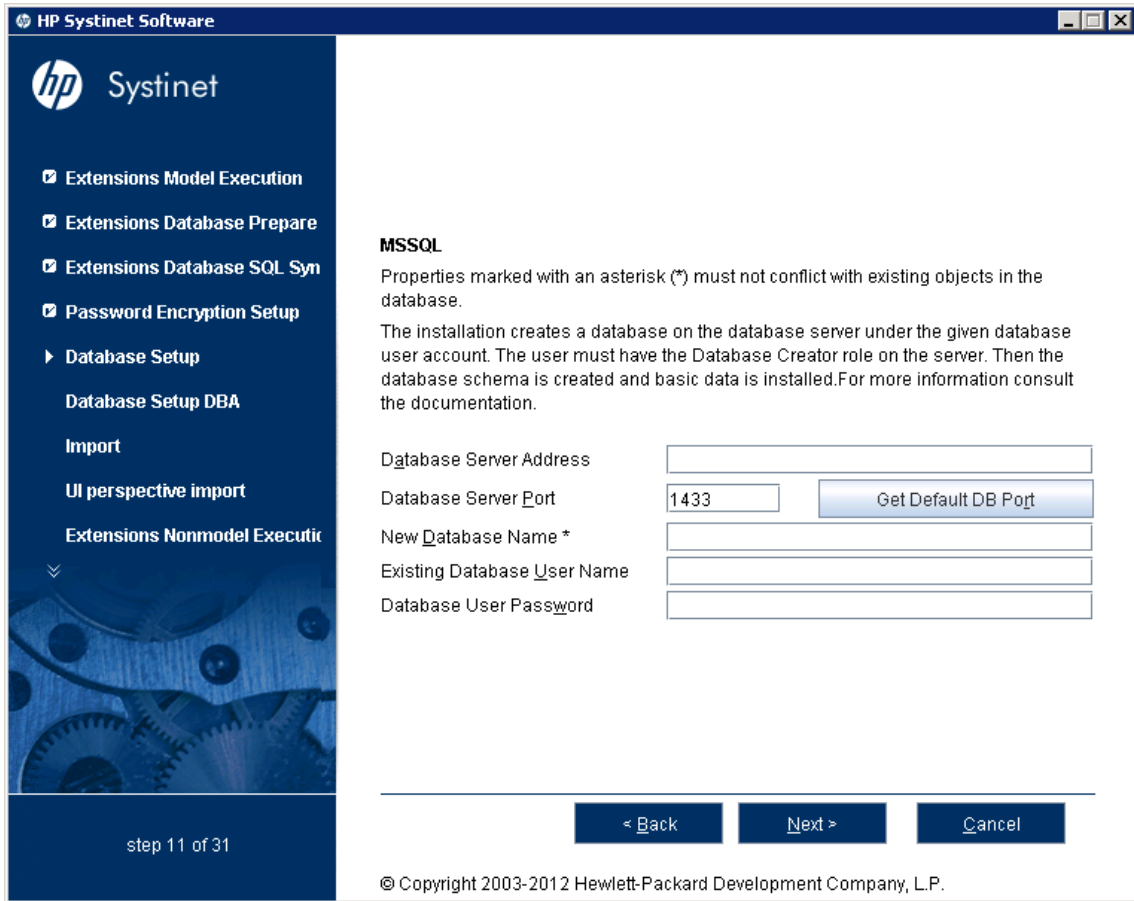
Click **Next** to open the JDBC Drivers page.

Continue to .

GUI Installation - MSSQL Create Schema

To create a new schema in MSSQL, set the following parameters:

MSSQL Create Schema Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform`, the hostname is `sqlhost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform`, the port number is `1433`.
Existing Database Name	Name of the database.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform`, the database name is `platform`.
Existing Database User Name	For the Create Schema option the user must have schema creation rights.When using `integratedSecurity`, just fill non-blank text (dummy).	—
Database User Password		

Click **Next** to open the JDBC Drivers page.

Continue to .

GUI Installation - Oracle Create Tablespace

To create a new tablespace in Oracle, set the following parameters:

Oracle Create Tablespace Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform`, the hostname is `orahost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform`, the port number is `1521`.
Existing Database Name	Name of the database.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform`, the database name is `platform`.
Full Connection String	Full connection string to the database.	Select this as option as an alternative to inputting the individual connection parameters.
Database Administrator Name	User name and password of the administrator of the database.	—
Database Administrator Password		
New Database Tablespace	Name of the tablespace to create.	The tablespace name must not conflict with existing objects in the database.
Tablespace Datafile	Path to the tablespace datafile that is stored on the database host machine.	The new database tablespace must not conflict with existing objects in the database.
New Database User Name	Name and password of a new database user.	The user name must not conflict with existing objects in the database.
Database User Password		
Confirm Password		

Click **Next** to open the JDBC Drivers page.

Continue to .

GUI Installation - Oracle Create Schema

To create a new schema in Oracle, set the following parameters:

Oracle Create Schema Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform`, the hostname is `orahost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform`, the port number is `1521`.
Existing Database Name	Name of the database.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform`, the database name is `platform`.
Full Connection String	Full connection string to the database.	Select this as option an alternative to inputting the individual connection parameters.
Existing Database User Name	User name and password to connect to the database.	—
Database User Password		

Click **Next** to open the JDBC Drivers page.

Continue to .

GUI Installation - JDBC Drivers

In the JDBC Drivers page, input or click **Browse** to select the drivers to use.
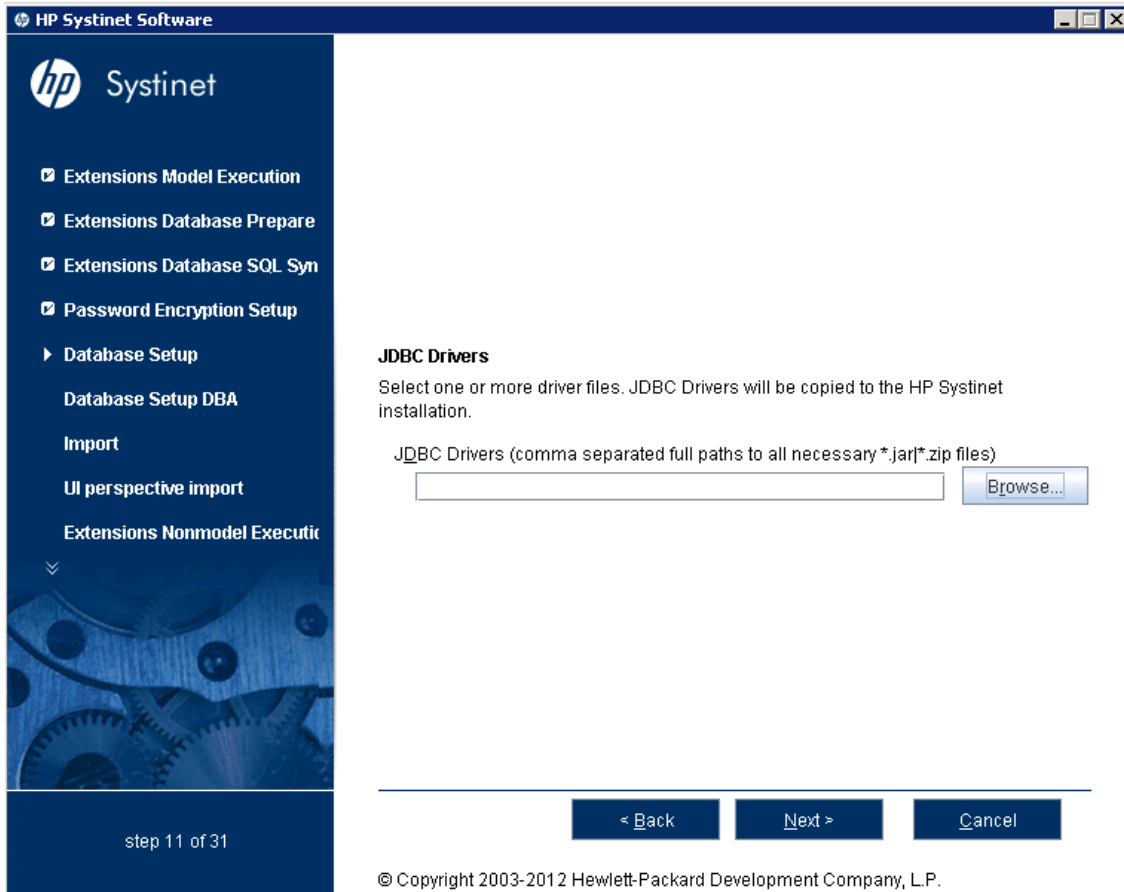
Note: Separate multiple driver names with commas.

Supported Oracle Drivers

Database	DB Version	Driver Packages	Driver Version	Driver Class
Oracle Database	10.2.0.4	ojdbc14.jar, orai18n.jar	10.2.0.4	oracle.jdbc.driver.OracleDriver
	11.1.0.6	ojdbc6.jar, orai18n.jar	11.1.0.6	

Note: It is highly recommended that thin drivers are used as opposed to OCI drivers due to significant performance increase and easier configuration.

Supported DB2 Drivers

Database	DB Version	Driver Packages	Driver Version	Driver Class
IBM DB2	9.1 (FP 5)	db2jcc.jar, db2jcc_license_cu.jar	3.2	com.ibm.db2.jcc.DB2Driver
	9.7 (FP 2)			

Caution: For version 9.7, use the drivers supplied with 9.1. Drivers from 9.7 cause exceptions such as "The database returned no natively generated identity value."

Supported MSSQL Drivers

Database	DB Version	Driver Packages	Driver Version	Driver Class
Microsoft SQL Server	2005 SP2 (9.00.3042)	sqljdbc.jar	1.2	com.microsoft.sqlserver.jdbc. SQLServerDriver
	2008 SP1 (10.0.2531.0)	sqljdbc4.jar	3.0	

Click **Next** to validate the database parameters, the configuration tables, and the driver, and open the Repository Import page.

Continue to .

GUI Installation - Repository Import

In the Repository Import page, select the initial data you want to upload to Systinet.
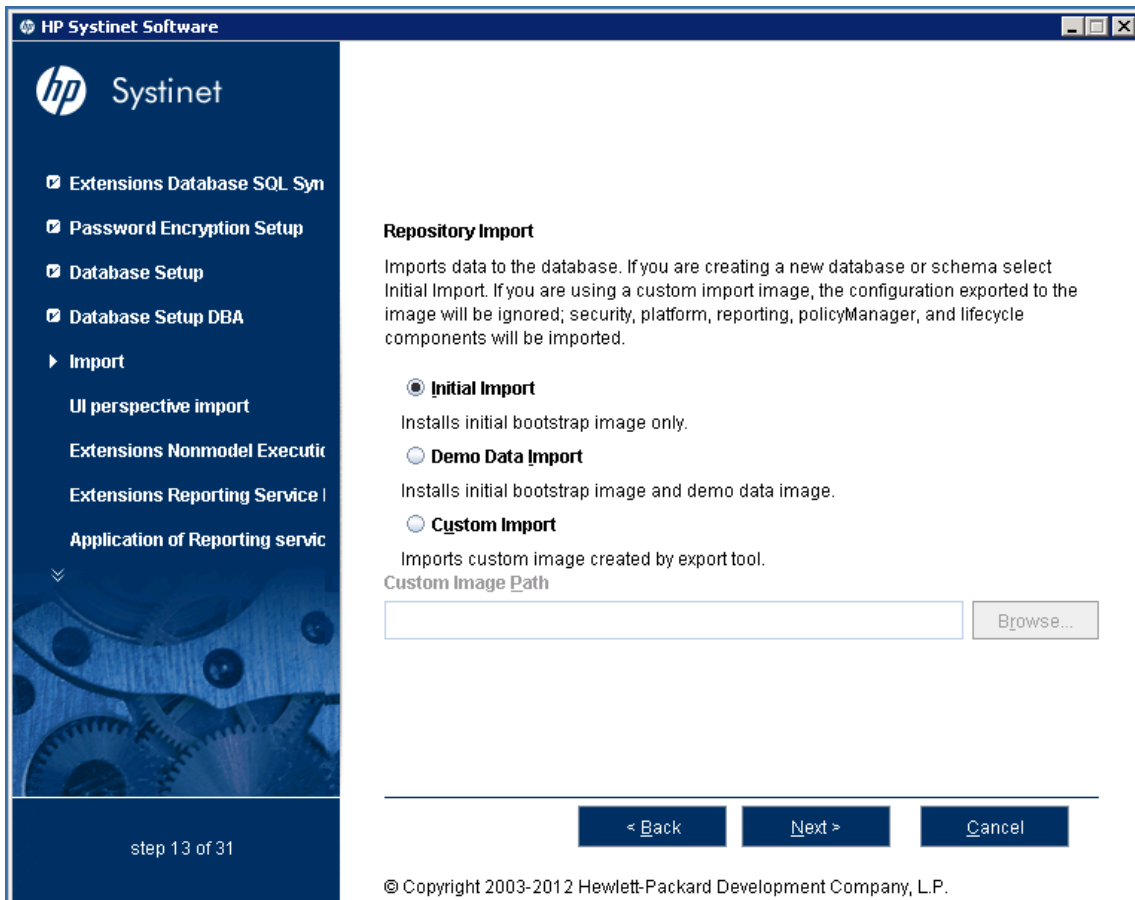
1. Do one of the following:

   - Select **Initial Import** to import a bootstrap image only.

   - Select **Demo Data Import** to import the included demo data set.

     The demo data contains a demo domain containing a large number of artifacts and some users. The user details for JBoss are contained in the `user.properties` file and may be changed later.

     Note: The compliance status of artifacts included in the demo data does not reflect their initial status as the import does not contain any policy validation data. Regenerate the validation data manually or allow the automatic validation task to regenerate it.
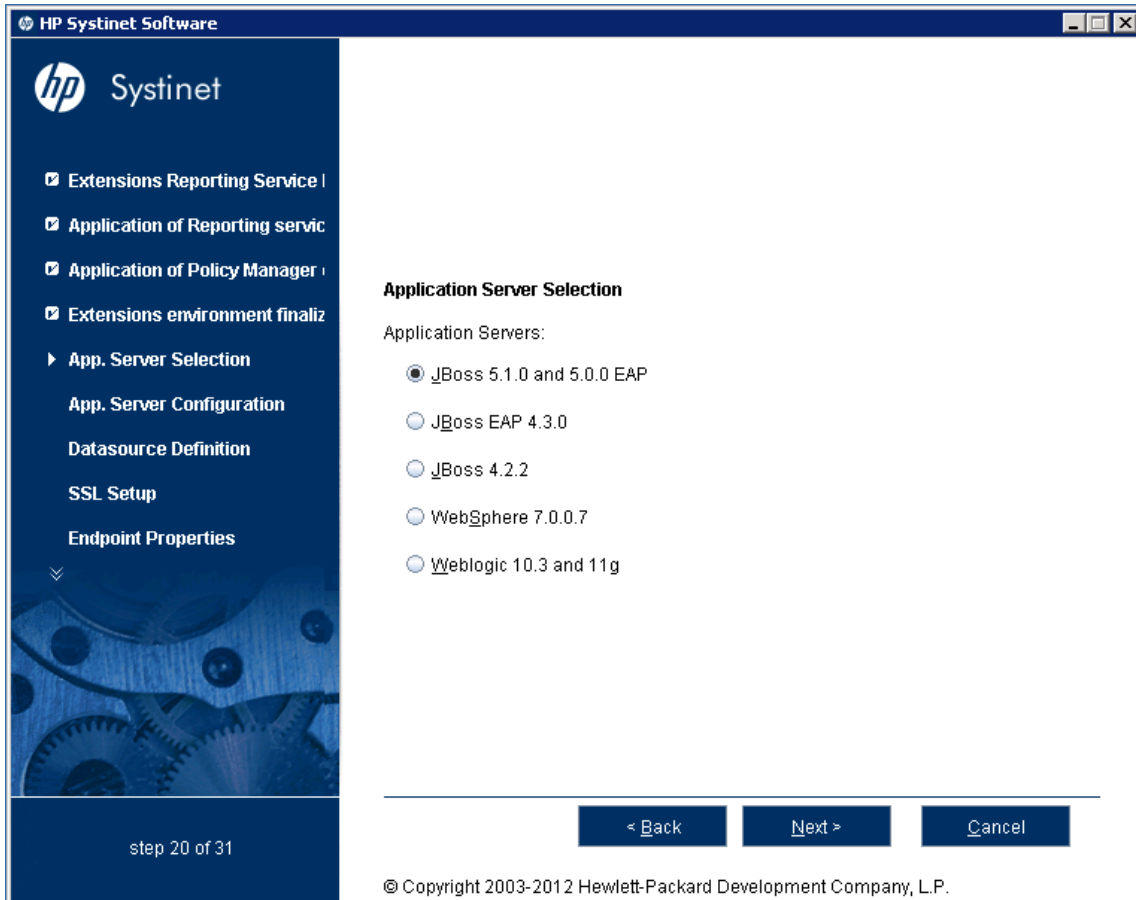
   - Select **Custom Import**, and input or **Browse** to select a custom image.

2. Click **Next** to validate the data image and open the Application Server Selection page.

GUI Installation - Application Server Selection

In the Application Server Selection page, select the application server to use.

Note: For evaluation purposes, HP recommends JBoss. Other application servers require additional set up and configuration.

Select your application server type and click **Next**.

If you selected JBoss, continue to "GUI Installation - JBoss Deployment Properties" (on page 103).

If you selected a different application server, continue to "GUI Installation - Endpoint Properties" (on page 104).

GUI Installation - JBoss Deployment Properties

In the JBoss Deployment Properties page, input or click **Browse** to select the JBoss application server installation folder and set the JBoss Configuration directory.
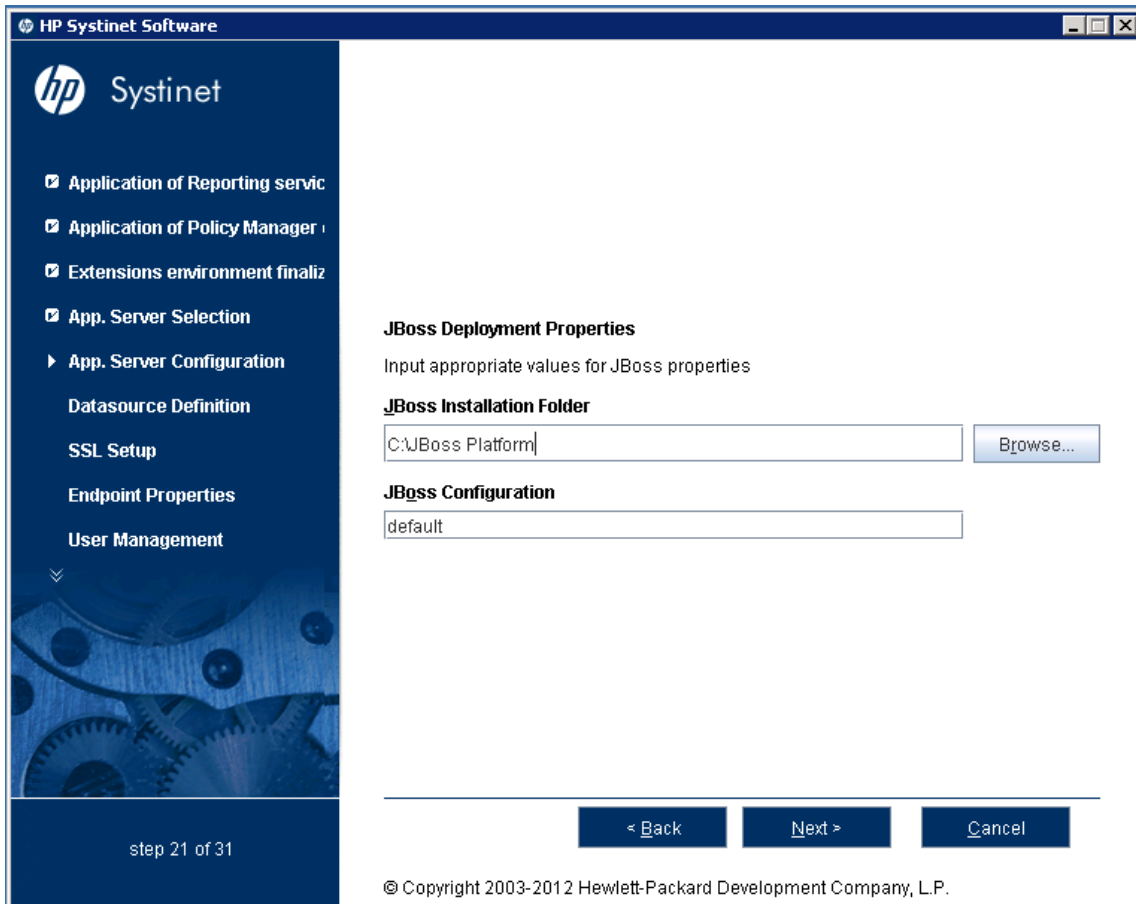
- For development and evaluation purposes, use the `default` configuration.

- For production deployments, use the appropriate configuration for your requirements, for more details, see "Server Configurations" in the JBoss Installation Guide.

- For a JBoss cluster use the `nodeX` configuration.

Click **Next** to verify the data source and JBoss settings, and open the Endpoint Properties page.

GUI Installation - Endpoint Properties

In the Endpoint Properties page, specify the endpoint properties.

For integration with SiteMinder, set the endpoint to the proxy server integrated with SiteMinder.

For a JBoss cluster, specify the load balancing server hostname and ports.

Click **Next** to open the User Management Integration page.

Caution: If you change the port numbers from their default values, you must also change the application server configuration to use these ports.

Continue to .

GUI Installation - User Management Integration

In the User Management Integration page. select if you want to integrate with LDAP or store accounts in your database.
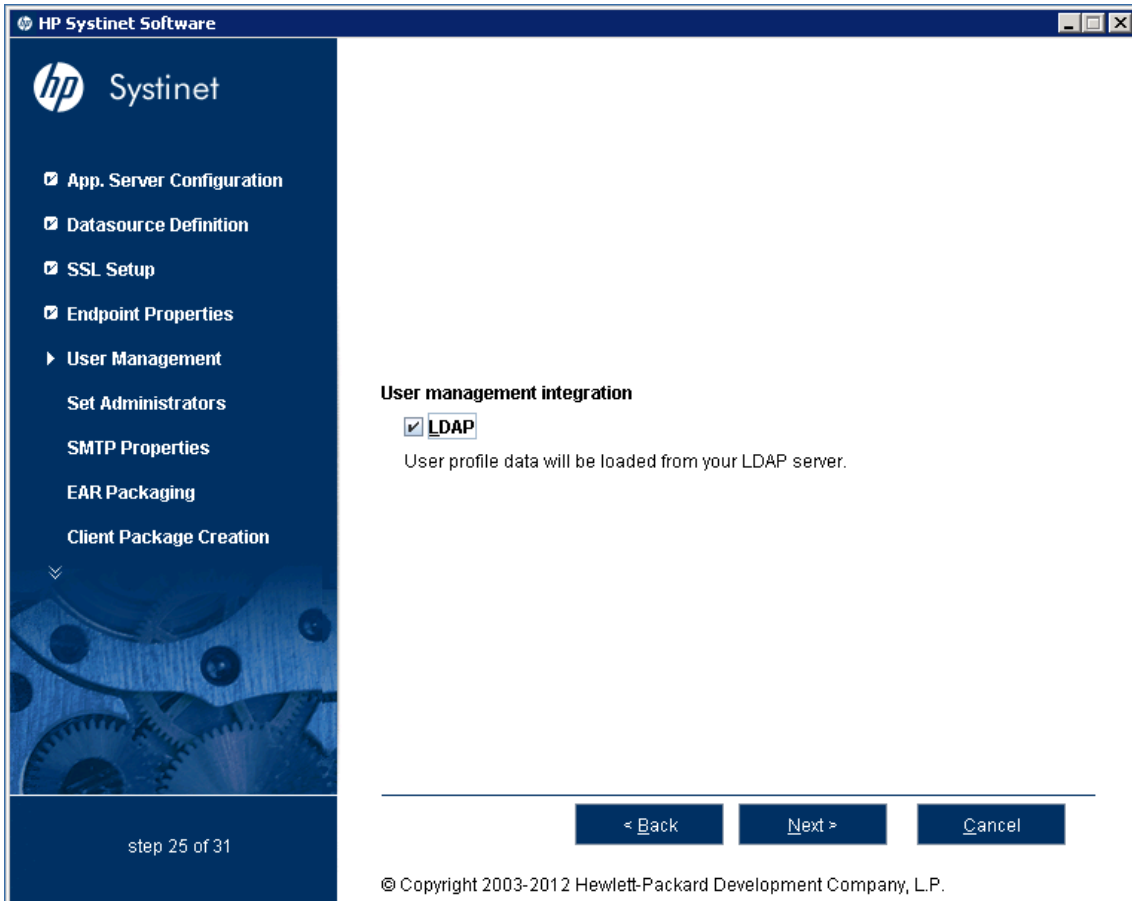
If you selected LDAP, click **Next** to continue to "GUI Installation - LDAP Service Properties" (on page 106).

If you did not select LDAP, click **Next** to continue to "GUI Installation - System Email Configuration" (on page 111).

GUI Installation - LDAP Service Properties

In the LDAP Service page, set the LDAP connection parameters, credentials, and case sensitivity.

Note: HP Systinet logins are case-insensitive by default. If want the login name to be case-sensitive you must set the `shared.um.account.caseInsensitiveLoginName` property to `false`. For details, see "How to Manage System Settings" in the *Administration Guide*. You must also ensure that the application server uses matching case-sensitive or -insensitive authentication.

Click **Next** to open the LDAP Search Rules page.

GUI Installation - LDAP Search Rules

In the LDAP Search Rules page enter the following parameters:

LDAP Search Rules Properties

Property	Description
Search Filter	The notation of the search filter conforms to the LDAP search notation. You can specify the LDAP node property that matches the user account or group.
Search Base	LDAP is searched from this base according to the Search Scope settings.
Search Scope	• One-level Scope: Only direct sub-nodes of the search base (entries one level below the search base) are searched. The base entry is not included in the scope. • Subtree Scope: The search base and all its sub-nodes are searched.
Results Limit	Number of items returned when searching LDAP. If more results are returned by an LDAP search the remainder are disregarded and not shown.

Click **Next** to open the LDAP User Properties Mapping page.

GUI Installation - LDAP User Properties Mapping

In the User Property Mapping page, use **Add** and **Remove** to set the property mappings.
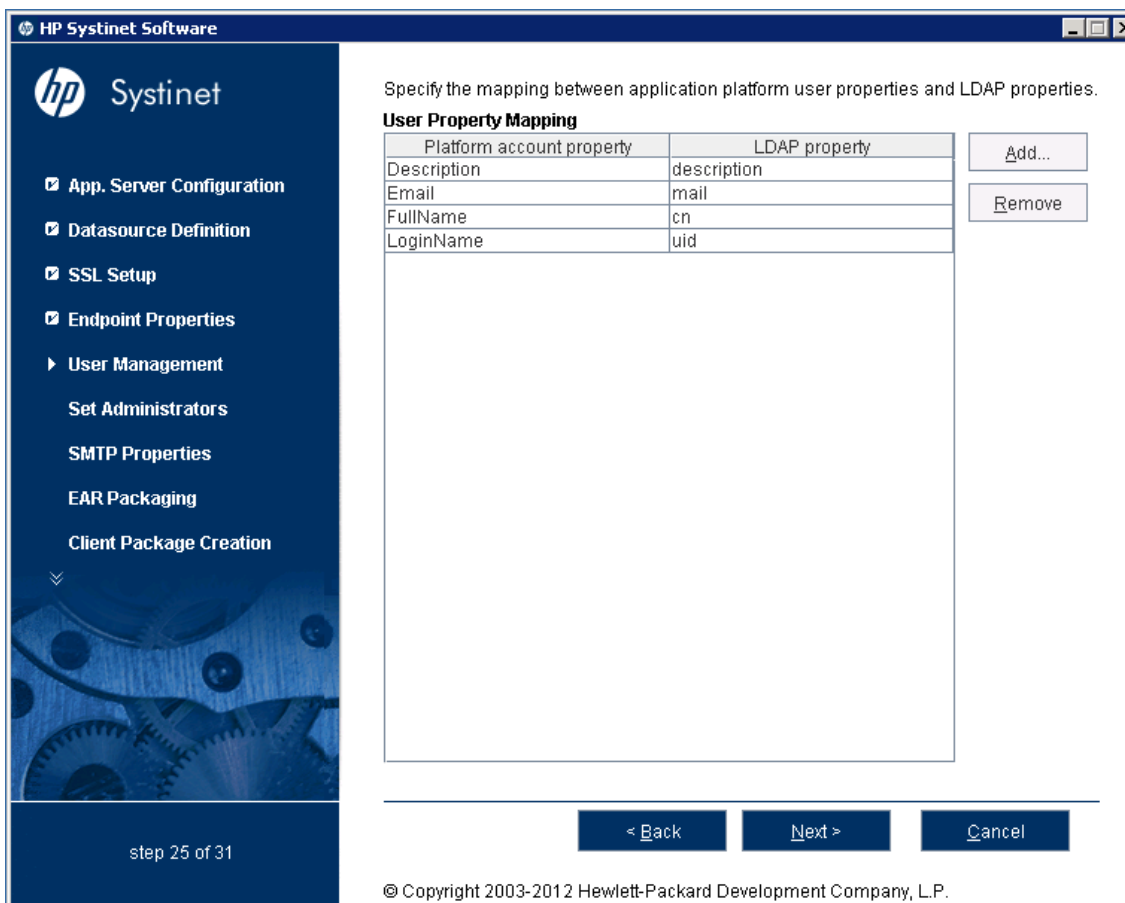
You must map the following mandatory user account properties from an LDAP server:

```
java.lang.String loginName
java.lang.String fullName
```

You can map the following optional user account properties from an LDAP server:

```
java.lang.String Email
java.lang.String Description
java.lang.String LanguageCode
java.lang.String Phone
java.lang.String AlternatePhone
java.lang.String Address
java.lang.String City
java.lang.String Country
```

Caution: Ensure that your mappings are correct and that these properties exist on your LDAP server. The incorrect mapping of any properties, even optional ones, can have a severe performance impact for sign-in for some LDAP services.

Click **Next** to open the LDAP Group Search Rules page.

GUI Installation - LDAP Group Search Rules

In the Group Properties page, enter the following parameters:

LDAP Search Rules Properties

Property	Description
Search Filter	The notation of the search filter conforms to the LDAP search notation. You can specify the LDAP node property that matches the user account or group.
Search Base	LDAP is searched from this base according to the Search Scope settings.
Search Scope	- One-level Scope: Only direct sub-nodes of the search base (entries one level below the search base) are searched. The base entry is not included in the scope. - Subtree Scope: The search base and all its sub-nodes are searched.
Results Limit	Number of items returned when searching LDAP. If more results are returned by an LDAP search the remainder are disregarded and not shown.

Click **Next** to open the Group Property Mapping page.

Continue to "GUI Installation - LDAP Group Properties Mapping" (on page 110).

GUI Installation - LDAP Group Properties Mapping

In the Group Property Mapping page, use **Add** and **Remove** to set the property mappings.
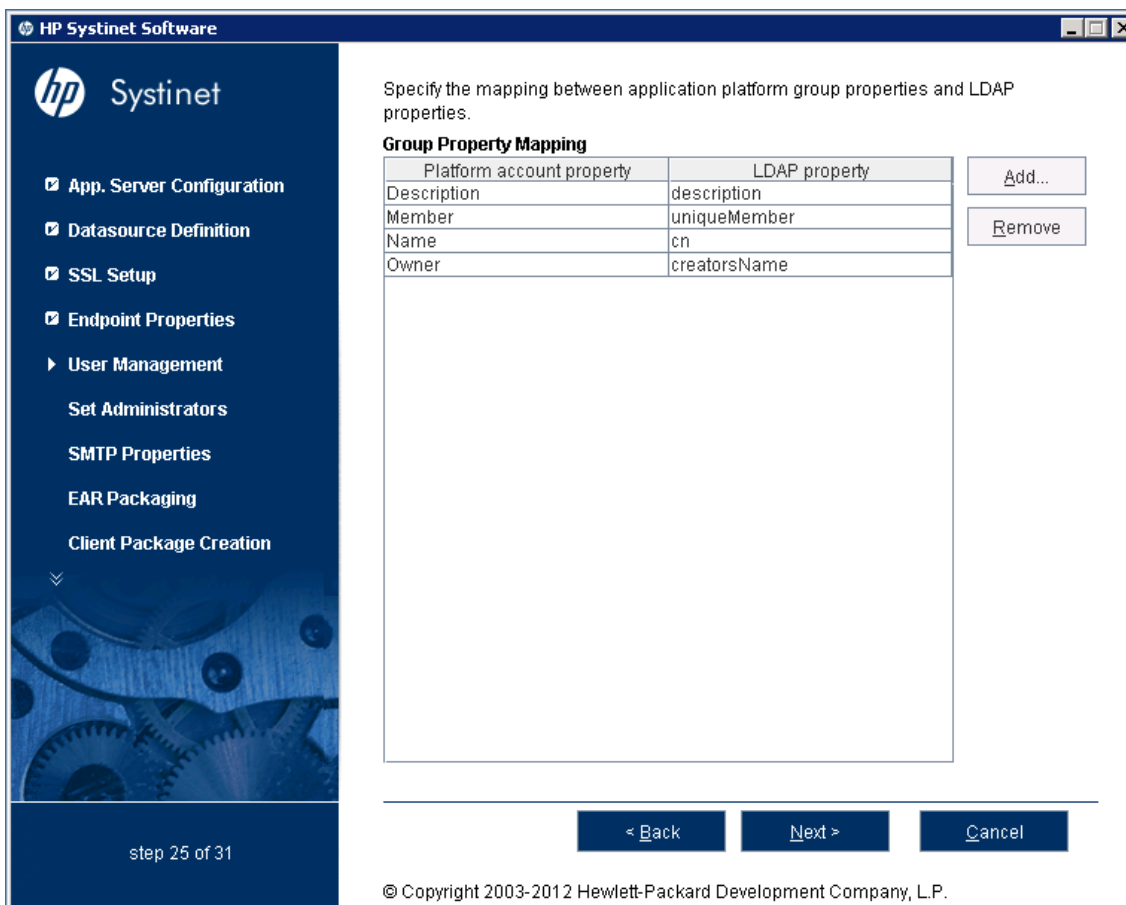
The following mandatory group properties must be mapped from an LDAP server:

```
java.lang.String name
java.lang.String member
```

The following optional group properties can be mapped from an LDAP server:

```
java.lang.string Owner
java.lang.String Description
```

Caution: Ensure that your mappings are correct and that these properties exist on your LDAP server. The incorrect mapping of any properties, even optional ones, can have a severe performance impact for sign-in for some LDAP services.

Click **Next** to open the System Email Configuration page.

Continue to .

GUI Installation - System Email Configuration

Enter the system mail account to be used as the source of automatic notification mails and system messages.
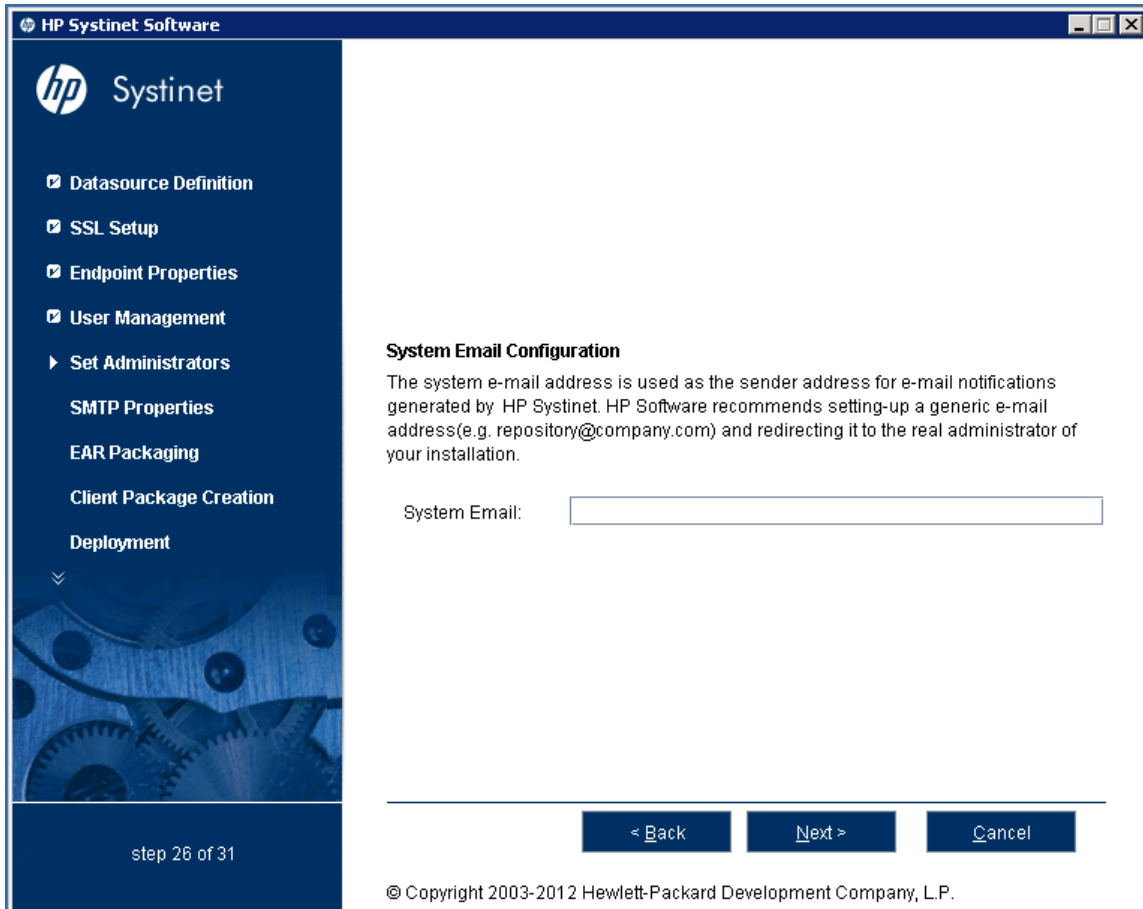
Click **Next** to open the Administrator Account Configuration page.

Continue to .

GUI Installation - Administrator Account Configuration

In the Administrator Account Configuration page, set the administrator credentials.
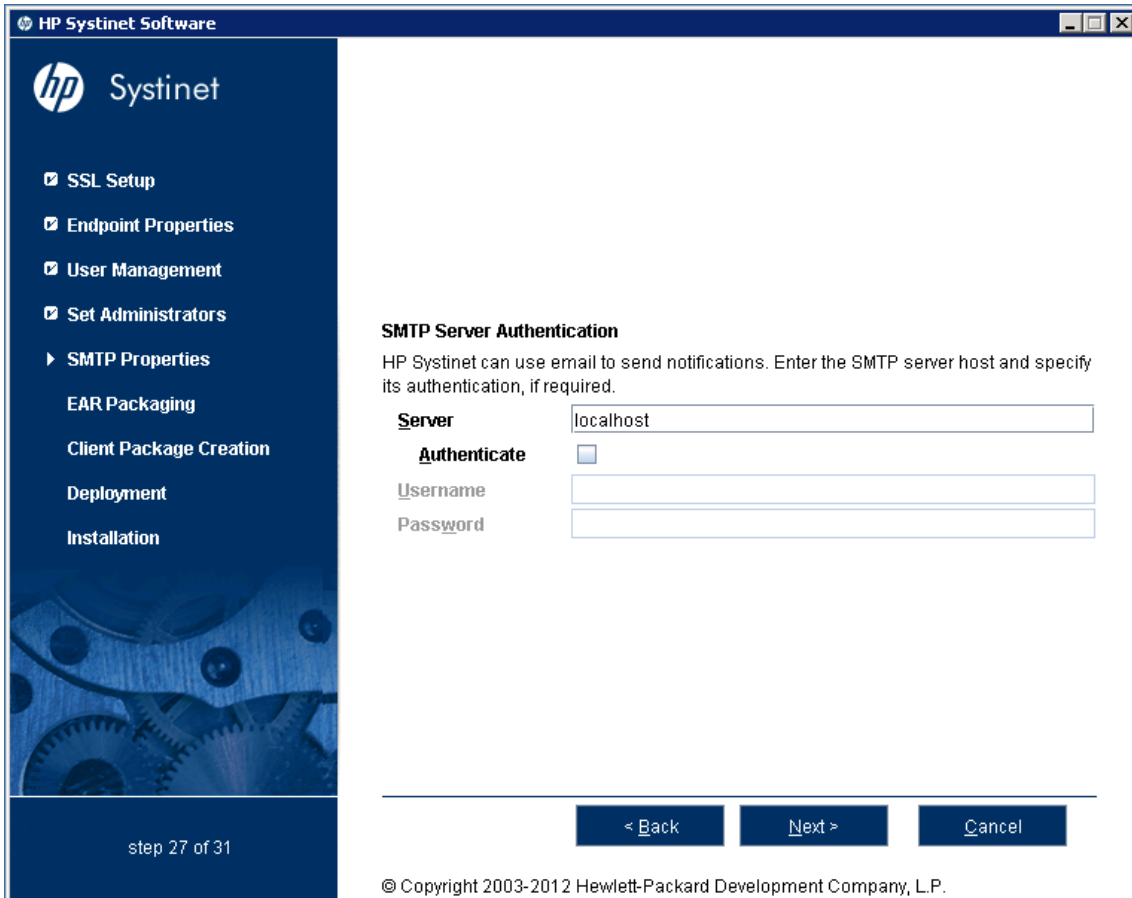
Click **Next** to open the SMTP Server Authentication page.

Note: The administrator login name must be valid for the selected application server instance. The user with the specified name becomes an Systinet administrator. For JBoss the specified administrator account is automatically created.

Continue to "GUI Installation - SMTP Server Authentication" (on page 113).

GUI Installation - SMTP Server Authentication

If you want mail notifications, set the mail server host.

To authenticate, select **Authenticate** and enter the SMTP server credentials.

Click **Next** to create the client package and open the Confirmation page.

Continue to .

GUI Installation - Confirmation

In the Confirmation page, click **Next** to start the installation process and open the Installation Progress page.

Continue to .

GUI Installation - Installation Progress

In the Installation Progress page, track each step of the installation.

For manual database deployment the installation stops after creating the database scripts.

When the installation is complete, click **Next** to open the Installation Finished page, and click **Finish** to exit the Installation Wizard.

Completing GUI Installation

For Decoupled Database deployment and JDKless Deployment, you must perform additional steps before installation is complete.

For details, see the following sections:

- "Decoupled Database Script Execution" (on page 115)
- "Finish Decoupled Database Installation" (on page 115)
- "Create an Archive for JDKless Deployment" (on page 115)

Decoupled Database Script Execution

Provide the scripts created by the installer to the database administrator.

The installer creates the scripts in `SYSTINET_HOME/sql`.

- If you are creating a new database/tablespace use the database administrator account to execute `createdb.sql`.
- To create the schema use the power user account to execute `all.sql`.

Note: The schema creation scripts contain drop instructions which can, by design, fail and their failure must be ignored. If you are overwriting an existing Systinet database, make sure that the SQL tool ignores these failures.

Note: For Oracle Database, `all.sql` executes a series of separate scripts to create the schema.

Finish Decoupled Database Installation

Execute the following command to finish the installation:

SYSTINET_HOME/bin/setup -c

Note: Add **--passphrase** *PASSPHRASE* if you set password encryption.

Create an Archive for JDKless Deployment

Prepare an archive of the Build deployment to apply to the Target environment.

1. Enter the full hostname (including domain) and port numbers for the Target environment in the `deployment.properties` file.

2. Delete the HP Systinet extraction folder and execute the installation command:

   java -jar hp-systinet-4.10.jar -u deployment.properties -i /opt/hp/systinet/4.10

3. Archive the clean deployment:

   tar -cjf hp-systinet-4.10-clean.tar.bz2 /opt/hp/systinet

   Note: If possible, use `tar.gz` or `tar.bz2` to preserve executable flags.

Chapter 7

Deploying Systinet

After installation, deployment environments may require additional configuration.

For details, see the following sections:

Set Up Authentication

By default, Systinet requires authentication for selected web resources. The configuration of these requirements conforms to the J2EE specification, as part of the deployment descriptors contained in the Systinet EAR file.

"Authentication Methods" describes the default authentication method with the URL patterns, relative to the deployment context of the EAR file (the default is `soa`).

Authentication Methods

Authentication Method	URL Patterns
Form Authentication (required by the web UI)	web/service-catalog/* (Service Catalog UI)
	web/policy-manager/* (Policy Manager UI)
	web/shared/* (shared UI)
Basic Authentication (HTTP) (required by parts of the REST interface and self-tester)	systinet/platform/restBasic/* (see "Proprietary REST Interface" in the *Developer Guide*)
	platform/restSecure/* (see "Atom-Based REST Interface" in the *Developer Guide*)

Authentication Method	URL Patterns
	policymgr/restSecure/* (Policy Manager REST interface)
	reporting/restSecure/* (Reporting REST interface)
	self-test/secure-snoop
No authentication	web/resources/* (static UI resources such as images)
	systinet/platform/rest/* (see "Proprietary REST Interface" in the *Developer Guide*)
	platform/rest/* (see "Atom-Based REST Interface" in the *Developer Guide*)
	policymgr/rest/* (Policy Manager REST interface)
	reporting/rest/* (Reporting REST interface)
	self-test (excluding secure-snoop page)

The Systinet EAR contains various WAR files. Some of the presented web pages may include links between resources contained in different WAR files. The security context (knowledge of the authenticated user) may be lost when following such links, so you may be prompted to sign in again.

Application servers provide a single-sign-on (SSO) solution for this situation:

- **JBoss**

  SSO is set up during Systinet installation.

  For details, see http://www.jboss.org/wiki/Wiki.jsp?page=SingleSignOn .

  Caution: If you setup 2-Way SSL with JBoss you must delete `WEB/INF/context.xml` in the `web-ui-war.war` file.

- **WebLogic**

  SSO is already set up in the deployment descriptor in the deployed EAR file.

- **WebSphere**

  The SSO option is switched on when you enable administrative security.

Set Up Role Mapping

Systinet requires one J2EE role, `authenticated`. By default, this role is mapped to any authenticated user for all application servers. If required, you can change the mapping of this role to grant or deny access for selected users that pass authentication.

For details, see the relevant security documentation for your application server.

Systinet also contains an `administrator` role, which enables privileged access to all Systinet resources independently of ACLs, as well as access to Systinet administration tasks.

This role is managed by Systinet and not by the application server. The initial administrator name is set during installation of Systinet. Any administrator can use the Systinet UI to assign the administrator role to additional users or user groups.

Set Up SiteMinder Integration

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

To Integrate Siteminder Using the Setup Tool:

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

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

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

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

5. Do one of the following:

   - Select **Use Cookies** to accept authentication cookies.

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

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

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

   The Setup Tool updates your deployment and configuration.

8. After setup completes, click **Next** and click **Finish** to exit the Setup Tool

9. Redeploy the Systinet EAR file as described in the appropriate sections for each application server.

Deploying Systinet to JBoss

After installation, JBoss may require additional configuration, particularly for production environments.

For details, see the following sections:

- "Configure JBoss Port Numbers" (on page 119)

- "Enable SSO in JBoss Clusters" (on page 119)

- "Set Up the JBoss User Store" (on page 119)

- "Create JBoss Cluster Nodes" (on page 122)

- "Modify JBoss Logging" (on page 123)

- "Enable Non-Latin HTTP Parameters in JBoss" (on page 125)

- "Redeploy the EAR File to JBoss" (on page 125)

> **Caution**: `hp-soa-systinet.ear` contains the encryption key used to encrypt passwords for the database. It should be protected with system file permissions.

> **Caution**: The credentials used to connect to the data source are stored in the JBoss deployment folder with the name `hpsoasystinet-xa-ds.xml`. This file contains the username and password in plain text and should be protected with file system permissions.

Configure JBoss Port Numbers

By default, Systinet uses ports 8080 and 8443. If you select a different set of ports during installation, you must configure JBoss after installation to use these ports. If you are using port numbers that are higher than the default, the easiest way is to edit the JBoss configuration files:

To Edit JBoss Port Numbers:

1. Open the `JBOSS_HOME/bin/run` script in an editor.

2. Insert this line where JAVA_OPTS is set:

    `-Djboss.service.binding.set=ports-01`

    This value represents the factors of 100 by which additional port numbers above the default value are enabled. For example, if you use the value `ports-01`, ports 8180, 8280, 8380... are enabled. If you set the value `ports-02`, the additional ports are 8280, 8480, 8680...

3. Save and exit the script.

Enable SSO in JBoss Clusters

Systinet automatically configures SSO when Systinet is deployed to a single JBoss application server. For JBoss clusters, the application server requires you to authenticate again every time you request a URL pointing to a previously unaccessed WAR module. (For example, log in to the UI and access a REST endpoint, JBoss requests authentication again).

To prevent this behavior and enable a single login for applications deployed to JBoss clusters, you must change the configuration:

To Enable SSO in JBoss Clusters:

1. Open `JBOSS_HOME/server/CONFIG_NAME/deploy/jboss-web.deployer/server.xml` with a text editor.

2. Uncomment the following section:

    ```
    <Valve className="org.apache.catalina.authenticator.SingleSignOn"/>
    ```

3. Save `server.xml` and restart the application server.

For more details about SSO in JBoss, see http://www.jboss.org/community/docs/DOC-12280.

Set Up the JBoss User Store

By default, Systinet uses a JBoss user store to authenticate users. The default user store is a plain text file `JBOSS_PROFILE/conf/users.properties`, which contains lines with `USERNAME=PASSWORD`. All users listed in this file can authenticate with Systinet.

Systinet defines a new JBoss security domain that you can customize to set up authentication against various user stores, including LDAP. The definition of this domain is contained in

`SYSTINET_HOME/deploy/jboss/hp-soa-systinet.sar`, which is deployed to JBoss during installation.

To Modify JBoss Authentication:

1. Extract `SYSTINET_HOME/deploy/jboss/hp-soa-systinet.sar` to a directory.

2. In the unzipped directory, open `hp-systinet-login-config.xml` with a text editor.

3. Change the login module definitions as required.

    For details, see the JBoss security documentation.

    "Systinet JBoss Login Configuration File" is an excerpt of the relevant section of this file.

4. Zip the directory back to `hp-soa-systinet.sar`.

5. Redeploy the SAR file to `JBOSS_PROFILE/deploy/hp-soa-systinet.sar` and restart JBoss.

Systinet JBoss Login Configuration File

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE policy PUBLIC "-//JBoss//DTD JBOSS Security Config 3.0//EN"
      "http://www.jboss.org/j2ee/dtd/security_config.dtd">
<policy>
  <application-policy name="hp-systinet">
    <authentication>
      <!-- ================================= -->
      <!-- CLIENT CERT authentication EXAMPLE -->
      <!-- ================================= -->
      <!-- JBOSS's SSL client certificate mapping, uncomment when
using
         CLIENT-CERT login method -->
      <!--
        <login-module
code="org.jboss.security.auth.spi.BaseCertLoginModule"
flag="optional">
          <module-option name="password-
stacking">useFirstPass</module-option>
          <module-option
name="verifier">org.jboss.security.auth.certs.AnyCertVerifier</module-
option>
          <module-option name="securityDomain">java:/jaas/hp-
systinet</module-option>
        </login-module>
      -->
      <!-- ===================================== -->
      <!-- USERNAME/PASSWORD authentication EXAMPLE -->
      <!-- ===================================== -->
      <!-- JBOSS's login module that verifies name and password
against users.properties -->
      <!-- file from the classpath (classpath contains JBOSS's
configuration conf directory -->
      <login-module
```

```
code="org.jboss.security.auth.spi.UsersLoginModule" flag="optional">
       <module-option name="password-stacking">useFirstPass</module-
option>
     </login-module>
     <!--
       JBOSS's login module that verifies name and password against
LDAP.
       To enable LDAP authentication, uncomment the following login-
module element,
       customize the module options according to your environment.
       Finally, remove or comment the previous login module
org.jboss.security.auth.spi.UsersLoginModule.
       -->
     <login-module
code="com.hp.systinet.security.jboss.LdapLoginModule" flag="optional">
       <module-option
name="java.naming.provider.url">ldap://localhost:63284</module-option>
       <module-option
name="java.-
naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</module-
option>
       <module-option
name="java.naming.security.authentication">simple</module-option>
       <module-option name="bindDN">uid=user,ou=people,dc=your,
dc=company</module-option>
       <module-option name="bindCredential">changeit</module-option>
       <module-option name="baseCtxDN">dc=your,dc=company</module-
option>
       <module-option name="baseFilter">(&amp;(uid={0})
(objectClass=person))</module-option>
       <module-option name="searchScope">SUBTREE_SCOPE</module-
option>
       <module-option name="allowEmptyPasswords">false</module-
option>
       <module-option name="password-stacking">useFirstPass</module-
option>
     </login-module>
     <!-- ========================================= -->
     <!-- Mandatory Role Mapping, authenticated users -->
     <!-- will become members of "authenticated" role -->
     <!-- ========================================= -->
     <!-- custom login module is used to assign authenticated role --
>
     <login-module
code="com.hp.systinet.security.jboss.AssignRoleLoginModule"
flag="optional">
       <module-option name="role">authenticated</module-option>
     </login-module>
   </authentication>
 </application-policy>
```

```
</policy>
```

Caution: Any new updates, extensions, or application installations will overwrite any manual changes made to `JBOSS_PROFILE/deploy/hp-soa-systinet.sar`.

Create JBoss Cluster Nodes

1. Copy the `nodeX` datasource, `JBOSS_HOME\server\nodeX\deploy\hp-systinet-xa-ds.xml`. Paste it into `JBOSS_HOME\server\node1\deploy\`

2. Copy the `nodeX` mail configuration, `JBOSS_HOME\server\nodeX\deploy\mail-service.xml`. Paste it into `JBOSS_HOME\server\node1\deploy\`

3. Enable the use of the `mod_jk` load balancer. Set the value of the `UseJK` attribute to `true` in the file `JBOSS_HOME\server\node1\deploy\jbossweb.deployer\META-INF\war-deployers-jboss-beans.xml`

4. Open the file `JBOSS_HOME\server\node1\deploy\jbossweb.sar\server.xml` for editing.

5. Comment out the HTTP connector listening at port 8080.

   This step is optional, but an existing HTTP listener can hide a misconfiguration or a bug.

6. Add the attribute `jvmRoute="${jboss.server.name}"` to the `Engine` element with the name `jboss.web`. (Do not evaluate the attribute value. Place it in the configuration file as is. It will be evaluated by JBoss at runtime.) The `jvmRoute="${jboss.server.name}"` attribute appends a suffix with the node name to outgoing JSESSIONID headers. These suffixes are used by the load balancer to maintain session affinity.

7. Apply the following workaround to disable session replication among clusters:

   a. Open the file `JBOSS_HOME\server\node1\deploy\jboss-web-cluster.sar\META-INF\jboss-service.xml` for editing.

   b. Change the value of `buddyReplicationEnabled` from false to true.

      Change the value of `numBuddies` from 1 to 0.

8. Copy the following files from `JBOSS_HOME\server\nodeX\conf` to `JBOSS_HOME\server\node1\conf`:

   - `roles.properties`

   - `users.properties`

   - `server.cer`

   - `server.keystore`

9. Create additional cluster nodes.

   a. Copy your JBoss installation to a second computer.

   b. Create a `JBOSS_HOME/server/node2` directory on that computer.

   c. Copy the content of directory `JBOSS_HOME\server\node1` to the `node2` directory on

the second computer.

   d. Repeat for node3, node4...nodeN.

10. JBoss 5.0 EAP, 5.1 GA, and 4.3.0 EAP use a messaging service which requires each cluster node to have a unique ID.

For each node, edit `JBOSS_HOME/server/`*NODE*`/deploy/messaging/messaging-service.xml`.

Locate and modify `<attribute name="ServerPeerID">`*N*`</attribute>`.

Replace *N* with a unique integer value for each node.

11. Copy the following files from `JBOSS_HOME\server\nodeX\deploy` to `JBOSS_HOME\server\node1\farm\`. They are distributed to all other cluster nodes when those nodes boot.

- hp-soa-systinet.ear

- hp-soa-systinet.sar

12. Launch `node1` on the first computer. When it successfully starts, launch `node2` node on the second computer. Continue for all other nodes. For each node, it is necessary to specify the URL of the HA-JNDI service in the local JBoss. Base the command-line for starting a node on the following:

```
JBOSS_HOME\bin\run.bat -b 0.0.0.0 -c nodeName
      -Dhpsoa.hajndi.url-jnp://hostname:1100/
      -Djboss.partition.name=DefaultPartition
```

13. Systinet should be running on `http://`*balancerHostname*`:`*port*`/`*context*`/`

Caution: JBoss relies on UDP multicasts by default. Multicast messaging may be blocked by switches or routers between cluster nodes. HP recommends using JBoss JMX console to verify that the nodes actually form a cluster. For details, see http://docs.jboss.org/jbossas/jboss4guide/r4/html/cluster.chapt.html. If the cluster nodes are disconnected, consult the troubleshooting guide at http://www.jboss.org/community/wiki/ClusteringFAQ.

Modify JBoss Logging

By default, HP Systinet logs messages to the hosting application server log files. When HP Systinet is deployed to JBoss, log messages are sent to the following file:

`JBOSS_DEPLOY\log\server.log`

Note: `JBOSS_DEPLOY` is the deployment directory on the JBoss application server where HP Systinet is deployed.

The message threshold level, by default, is *INFO*.

To Modify the Log File Parameters:

1. Stop the HP Systinet server.

2. Save `JBOSS_DEPLOY\conf\jboss-log4j.xml.log` to a recoverable backup location in case you need it later.

3. Open `JBOSS_DEPLOY\conf\jboss-log4j.xml.log` with a text editor.

4. The logging parameter can be one of the following values:

   - DEBUG

   - INFO

   - WARNING

   - ERROR

   Each value includes the messages for more serious values. For example, setting the logging level to `WARNING` would write all warning and error messages to the log.

   To set a logging level, add the following parameter after the `MaxFileSize` parameter:

   ```
   <param name="Threshold" value="LEVEL"/>
   ```

5. You can also set size-based rolling instead of time/date-based rolling.

   Comment out or delete the time/date based rolling appender:

   ```
   <!-- A time/date based rolling appender -->
   <appender name="FILE"
   class="org.jboss.logging.appender.DailyRollingFileAppender">
     <errorHandler
   class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
     <param name="File" value="${jboss.server.log.dir}/server.log"/>
     <param name="Append" value="false"/>
     <!-- Rollover at midnight each day -->
     <param name="DatePattern" value="'.'yyyy-MM-dd"/>
     <!-- Rollover at the top of each hour
     <param name="DatePattern" value="'.'yyyy-MM-dd-HH"/>
     -->
     <layout class="org.apache.log4j.PatternLayout">
       <!-- The default pattern: Date Priority [Category] Message\n --
   >
       <param name="ConversionPattern" value="%d %-5p [%c] %m%n"/>
       <!-- The full pattern: Date MS Priority [Category] (Thread:NDC)
   Message\n
       <param name="ConversionPattern" value="%d %-5r %-5p [%c]
   (%t:%x) %m%n"/>
         -->
     </layout>
   </appender>
   ```

6. To enable size-based rolling, uncomment the size-based rolling appender:

   ```
   <!-- A size based file rolling appender
   <appender name="FILE"
   class="org.jboss.logging.appender.RollingFileAppender">
     <errorHandler
   class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
     <param name="File" value="${jboss.server.log.dir}/server.log"/>
   ```

```
<param name="Append" value="false"/>
<param name="MaxFileSize" value="500KB"/>
<param name="MaxBackupIndex" value="1"/>
<layout class="org.apache.log4j.PatternLayout">
  <param name="ConversionPattern" value="%d %-5p [%c] %m%n"/>
</layout>
</appender>
-->
```

7. In the size-based appender section, set the maximum file size to for example, 100KB, by modifying the `MaxFileSize` parameter:

```
<param name="MaxFileSize" value="100KB"/>
```

8. Save `JBOSS_DEPLOY\conf\jboss-log4j.xml.log`.

9. Start the HP Systinet server.

Enable Non-Latin HTTP Parameters in JBoss

If you deploy the Systinet EAR to JBoss manually then make the following changes to enable non-Latin characters in HTTP parameters.

Note: This process is automated when the installer deploys the EAR file to JBoss.

To Enable Non-Latin Encoding for JBoss:

1. Open `JBOSS_HOME/server/`*CONFIGURATION*`/deploy/jboss-web.deployer/server.xml` with a text editor.

2. In all `connector` elements defined in `server.xml`, set the `URIEncoding attribute` to `UTF-8`.

Redeploy the EAR File to JBoss

You can manually deploy the EAR file to JBoss using the Setup Tool. This is required if you use the Setup Tool to configure Systinet during installation and deployment (for example, for SiteMinder setup).

To Deploy the EAR file to JBoss:

1. Stop the application server.

2. Start the Setup Tool by executing the following command:

   SYSTINET_HOME/bin/setup.bat(sh)

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

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

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

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

Deploy the EAR to WebLogic

The Systinet installer does not deploy the EAR file to WebLogic, you must deploy it using WebLogic functionality.

Note: The **Lock and Edit** and **Activate Changes** steps do not apply to WebLogic 10g (10.3) in Development mode as any changes made are directly applied. If you are using WebLogic 10g (10.3) in development mode, skip these steps.

HP recommends that you precompile JSPs before deployment. Use the following script to create an EAR file with precompiled JSPs:

`SYSTINET_HOME/deploy/`*AS*`/jspc/precompile_jspc` where *AS* is an application server specific folder name.

The script may require some environment variables to be set. If they are not set, the script fails and outputs the name of the required environment variable. The script creates `SYSTINET_HOME/deploy/precompiled.ear` which can be used instead of `SYSTINET_HOME/deploy/hp-soa-systinet.ear` during deployment.

To Deploy the HP Systinet EAR to WebLogic:

1. Start the WebLogic server.

2. In your browser, open the WebLogic Administration Console:

   `http://localhost:7001/console`

3. Log in with the administrator credentials created in "Create a WebLogic Domain for Systinet".

4. In the console, click **Lock & Edit**.

5. In the Domain Structure section, select **Deployments**, and click **Install**.

6. Navigate to `SYSTINET_HOME/deploy/`, select the Systinet EAR file, and then click **Next**.

   Note: Documentation WAR file is created in the `.../deploy/ directory` and must be deployed manually.

7. Select **Install this deployment as an application**, and click **Next**.

8. Select the managed server or cluster you want to host Systinet, and click **Next**.

9. In the Security section, select **DD Only**, and click **Finish**.

10. Click **Activate Changes**.

11. Start the server hosting HP Systinet:

    DOMAIN_HOME/bin/startManagedWebLogic `MY_MANAGED_SERVER`

Start Systinet using the **Start** on the Deployments page.

To verify that the HP Systinet deployment is running, view self-test in a browser window, at `http://`*hostname:port*`/`*context*`/self-test`.

Caution: `hp-soa-systinet.ear` contains the encryption key used to encrypt passwords for the database. It should be protected with system file permissions.

Deploy the EAR to WebSphere

The Systinet installer does not deploy the EAR file to WebSphere, you must deploy it using WebSphere functionality.

To Deploy the HP Systinet EAR to WebSphere:

1. In your browser, open the Administration Console:

   `http://localhost:9060/ibm/console`

2. Expand `Applications`, expand `Application Types`, and select `WebSphere Enterprise Applications`.

3. Click **Install**.

4. Click **Browse**, navigate to `SYSTINET_HOME/deploy/`, and select the Systinet EAR file.

   Note: Documentation WAR file is created in the `.../deploy/ directory` and must be deployed manually.

5. Select **Prompt me only when additional information is required**, and click **Next**.

6. Set the following options:

   ▪ Distribute application

   ▪ Allow dispatching includes to remote resources

   ▪ Allow servicing includes from remote resources

   ▪ If you have not manually precomiled JSPs before deployment, ensure that **Precompile JavaServer Pages** is selected.

7. Map modules to servers by selecting the servers to deploy Systinet.

8. Map modules to servers by selecting a module and virtual host.

9. Proceed to the Summary step, and click **Finish**.

10. Wait for the deployment to finish, and click **Save**.

11. Expand **Applications**, expand **Application Types**, and select **WebSphere Enterprise Applications**.

12. Select `HP Systinet`.

13. In the Detail Properties section, click **Class loading and update detection**.

14. Set the following properties:

    ▪ Polling interval `0`

    ▪ Classes loaded with application class loader first (parent last)

    ▪ Single class loader for application

15. Click **OK**, and save your changes.

16. Expand **Security**, and select **Global Security**.

17. Select **Enable application security**. If the **Enable application security** option is disabled, then select **Enable administrative security** and **Enable application security**.

    Deselect **Use Java 2 security to restrict access to local resources**.

18. In the Authentication section, expand **Web and SIP Security**, and select **General Settings**.

19. Select **Use available authentication data when an unprotected URI is accessed** and click **OK**.

20. In the Configuration page, click **Apply**.

21. You can set users and roles if required.

> **To create a user:**
>
>   a. Expand **Users and Groups**, and select **Manage Users**.
>
>   b. Click **Create**.
>
>   c. Enter the user parameters, and click **Create**.

22. Expand **Applications**, expand **Application Types**, and select **Enterprise Applications**.

23. Select the check-box for `HP Systinet`, and click **Start**.

> **Note**: Systinet starts automatically, whenever the server is started.

Note: The Systinet log can be viewed in the file: `PROFILE_HOME/logs/server_name/SystemOut.log`.

Caution: `hp-soa-systinet.ear` contains the encryption key used to encrypt passwords for the database. It should be protected with system file permissions.

Enable Full-Text Search in DB2

To enable full-text search you must create indexes and schedule their update in DB2. Use the DB2 Net Search Extender. Connect to the database using the same credentials used during installation.

Use the following example.

Create Indexes for FTS and Schedule Synchronization in DB2

```
db2text START

#use sa user in this case
db2text ENABLE DATABASE FOR TEXT CONNECT TO <database> USER sa USING
<password>

db2text CREATE INDEX idx_ry_resource_meta FOR TEXT ON ry_resource(m_
extensions)
  CONNECT TO <database> USER <user> USING <password>

db2text CREATE INDEX idx_ry_resource_data FOR TEXT ON ry_resource
(data)
  CONNECT TO <database> USER <user> USING <password>

#schedule a regular index update each day at midnight
db2text ALTER INDEX idx_ry_resource_meta FOR TEXT UPDATE FREQUENCY D
(*) H(0) M(0)
  CONNECT TO <database> USER <user> USING <password>

db2text ALTER INDEX idx_ry_resource_data FOR TEXT UPDATE FREQUENCY D
(*) H(0) M(0)
  CONNECT TO <database> USER <user> USING <password>
```

Commands to update the index manually can be found in the following example:

Synchronizing Indexes in DB2 Manually

```
db2text UPDATE INDEX idx_ry_resource_meta FOR TEXT
  CONNECT TO <database> USER <user> USING <password>

db2text UPDATE INDEX idx_ry_resource_data FOR TEXT
  CONNECT TO <database> USER <user> USING <password>
```

For more scheduling details, see the *DB2 Net Search Extender* documentation.

Searching Uploaded Documents with DB2

DB2 Net Search Extender uses external *Stellent/Oracle Outside In* technology to obtain text from DOC, PDF, and other text format files before indexing. For details, see the *Net Search Extender Administration* and *User Guides*.

Note: Indexing DOC and PDF files in Systinet with DB2 has not been tested.

Enable Full-Text Search in MSSQL

To enable full text search you must enable the service and create a full text catalog and indexes. Use MSSQL Server Management Studio or the sqlcmd command line tool.

Connect to the database using the same parameters used during Systinet installation.

To Enable Full-Text search on MSSQL:

1. Make sure that the SQL Server Fulltext Search service is running, and that the database is full-text enabled.

   By default, new databases are full-text enabled unless you create them with MSSQL Server Management Studio.

   In this case, select the database in the Object Explorer window, and select **Properties>Files**, and then select **Use full-text indexing**.

2. To create a full-text catalog, execute the following command:

   ```
   sqlcmd -U <user> -P <password> -d <database>
   CREATE FULLTEXT CATALOG ry_resource_ftsc
   go
   ```

   Note: You must have CREATE FULLTEXT CATALOG permission.

   It is possible to reuse an existing catalog, but HP recommends creating a new one for independent management purposes.

   For more details, see http://msdn2.microsoft.com/en-us/library/ms189520.aspx.

3. Do one of the following:

   ▪ To create a full-text index that is synchronized immediately after any data changes, execute the following command:

   ```
   sqlcmd -U <user> -P <password> -d <database>
   CREATE FULLTEXT INDEX ON ry_resource(
     m_extensions TYPE COLUMN m_extensions_fe LANGUAGE 0x0,
     data TYPE COLUMN data_fe LANGUAGE 0x0)
   ```

```
KEY INDEX pk_resource ON ry_resource_ftsc WITH CHANGE_TRACKING
AUTO
go
```

- To create a full-text index that is synchronized manually, execute the following command:

```
sqlcmd -U <user> -P <password> -d <database>
CREATE FULLTEXT INDEX ON ry_resource(
  m_extensions TYPE COLUMN m_extensions_fe LANGUAGE 0x0,
  data TYPE COLUMN data_fe LANGUAGE 0x0)
KEY INDEX pk_resource ON ry_resource_ftsc WITH CHANGE_TRACKING
OFF, NO POPULATION
go
```

For more details, see http://msdn2.microsoft.com/en-us/library/ms187317.aspx.

To synchronize the index manually, execute the following command:

```
sqlcmd -U <user> -P <password> -d <database>
ALTER FULLTEXT INDEX ON ry_resource START FULL POPULATION
go
```

The statement executes asynchronously, so the population may take some time.

To verify the population status, execute the command:

```
SELECT FULLTEXTCATALOGPROPERTY('ry_resource_ftsc','PopulateStatus')
go
```

Index population is complete when the population status is 0.

For more details, see http://msdn.microsoft.com/en-us/library/ms188359.aspx.

Searching Uploaded Documents with MSSQL

MSSQL supports only a limited set of document types after installation. Typically, it does support Microsoft ".doc" files, but does not support ".docx",".xlsx" and ".pdf" files. The list of all supported document types can obtained by the following SQL:

```
SELECT * FROM sys.fulltext_document_types
```

If the list does not contain a document type that you need to include in the full text search, ask your DBA to obtain and install an iFilter for the missing document type.

- Foxit provides a high performance PDF iFilter for 32=bit and x64 systems. For details, go to http://www.foxitsoftware.com/pdf/ifilter.

- Adobe provides a PDF iFilter for 32-bit and x64 systems. For details, go to http://adobe.com.

- Microsoft provides iFilters for MS-Office 2007/2010 document types including docx and xlsx. For details, go to http://support.microsoft.com/default.aspx?scid=kb;en-us;945934.

Enable Full-Text Search in Oracle

To enable full text search, you must create indexes and schedule their update. Use the Oracle **sqlplus** console. Connect to the database using the same credentials used during installation.

The procedure in commands is shown in "Preparing Oracle For Full Text Search using the Scheduling Mechanism". It also shows how to synchronize indexes every midnight.

Note: The database user does not have permission to create FTS indexes by default and must be given that permission.

Preparing Oracle For Full Text Search using the Scheduling Mechanism

```
sqlplus system/password@connect_identifier
-- add permission to create indexes
GRANT EXECUTE ON "CTXSYS"."CTX_DDL" TO user;
-- add "create job" permission to <user>
GRANT CREATE JOB TO user;
exit;

sqlplus user/password@connect_identifier
CREATE INDEX idx_ry_resource_meta ON ry_resource(m_extensions)
  INDEXTYPE IS CTXSYS.CONTEXT PARAMETERS
    ('FILTER CTXSYS.NULL_FILTER SECTION
      GROUP CTXSYS.NULL_SECTION_GROUP
      SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL');

CREATE INDEX idx_ry_resource_data ON ry_resource(data)
  INDEXTYPE IS CTXSYS.CONTEXT PARAMETERS
    ('FILTER CTXSYS.NULL_FILTER SECTION
      GROUP CTXSYS.NULL_SECTION_GROUP
      SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL');
```

To enable full text search of pdf, doc, and other document types, use `AUTO_FILTER` in the definition of the `idx_ry_resource_data` index"

```
CREATE INDEX idx_ry_resource_data ON ry_resource(data)
  INDEXTYPE IS CTXSYS.CONTEXT PARAMETERS
    ('FILTER CTXSYS.AUTO_FILTER');
```

Warning: *Do not* implement index synchronization ON COMMIT. It can cause Oracle thread termination, returning the error message `ORA-error stack (07445[ACCESS_ VIOLATION]) logged in` *filename*`.log`. (Tested on Oracle 10gR2 - 10.2.0.1). Use regular synchronization together with the `TRANSACTIONAL` parameter.

For more information about creating indexes, see the Oracle documentation at http://download-uk.oracle.com/docs/cd/B19306_01/text.102/b14218/toc.htm

Note: Not all document types can be indexed correctly. For details, see http://download.oracle.com/docs/cd/B19306_01/text.102/b14218/afilsupt.htm#i634493.

Synchronizing Indexes

Executing index synchronization manually is shown in the following example:

Synchronizing Indexes in Oracle Manually

```
sqlplus user/password@connect_identifier
CALL CTX_DDL.SYNC_INDEX('idx_ry_resource_meta', '2M');
CALL CTX_DDL.SYNC_INDEX('idx_ry_resource_data', '2M');
```

Creating an Indexing Stoplist

You can optionally manage a stoplist by removing words that could frequently appear in documents. By default, the Oracle index stoplist includes words such as "to". Full-text searches including these words return a false empty result. Alternatively, the database administrator should provide Systinet users with the stoplist, and a warning not to use these terms in full-text searches.

An example of commands to set up a stoplist on Oracle is shown in the following example:

Creating an Oracle Indexing Stoplist

```
call CTX_DDL.CREATE_STOPLIST('MyStoplist');
call CTX_DDL.ADD_STOPWORD('MyStoplist', 'a');
... Add a word that should not be indexed. Repeat the command for each
word to be excluded.

-- Include the DROP INDEX commands only if an index already exists.
DROP INDEX idx_ry_resource_meta;
DROP INDEX idx_ry_resource_data;
CREATE INDEX idx_ry_resource_meta on ry_resource(m_extensions)
indextype is ctxsys.context parameters
  ('filter ctxsys.null_filter section group CTXSYS.NULL_SECTION_GROUP
STOPLIST MyStoplist
    SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL') ;
CREATE INDEX idx_ry_resource_data on ry_resource(data) indextype is
ctxsys.context parameters
  ('filter ctxsys.null_filter section group CTXSYS.NULL_SECTION_GROUP
STOPLIST MyStoplist
    SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL');
```

Configure LDAP over SSL/TLS

You can configure LDAP over SSL (or TLS) with a directory server of your choice. HP recommends that you first install HP Systinet with a connection to LDAP that does not use SSL. You can then verify the configuration by logging in as a user defined in this directory before configuring use of SSL.

The configuration procedure assumes that you have already installed HP Systinet with an LDAP account provider.

HP Systinet must not be running.

- **LDAP over SSL Without Client Authentication**

  In this case only LDAP server authentication is required. This is usually the case.

  To change the LDAP configuration, run the Setup Tool and change Naming Provider URL to use the `ldaps` protocol and the port on which the directory server accepts SSL/TLS connections. An example of such a URL is, `ldaps://ldap.test.com:636`.

  Make sure that the hostname specified in the java.naming.provider.urlproperty matches the name that is in the directory server certificate's subject common name (CN part of certificate's Subject). Otherwise you get an exception during startup of HP Systinet. It informs you of a hostname verification error. The stacktrace contains the hostname that you must use.

- **LDAP over SSL With Mutual Authentication**

  HP Systinet does not support LDAP over SSL with mutual authentication.

- **Ensuring Trust with the LDAP Server**

  The client that connects to the SSL/TLS server must trust the server certificate in order to establish communication with that server. The configuration of LDAP described in this section inherits the default rule for establishing trust from JSSE (the Java implementation of SSL/TLS). This is based on trust stores.

Log4j Configuration

HP Systinet relies on the log4j configuration chosen using the "Default Initialization Procedure", described in http://logging.apache.org/log4j/1.2/manual.html.

This default initialization procedure results in the following configuration:

- The default logging configuration, as detailed in "Log4j Configuration File", is used for the HP Systinet EAR file deployed WebLogic and WebSphere. The file `log4j.properties`, which is contained in the EAR file, contains the default configuration.

- The option, `-Dlog4j.configuration=file:/ABSOLUTE_LOG4J_CONFIG_FILE_PATH`, can be added to the command that starts your application server. This enables you to override the default configuration contained in the EAR file.

  HP Systinet tools execute a java command with a `-Dlog4j.configuration` option that points to a `SYSTINET_HOME/conf/log4j.config`.

  HP Systinet creates log files for these tool executions in the `SYSTINET_HOME/log` directory.

- The logging configuration for an EAR deployed to JBoss is updated during installation, the content of this configuration is similar to the default properties, but is expressed in an XML file.

  - `JBOSS_HOME/server/JBOSS_PROFILE/conf/jboss-log4j.xml`

  The audit log file is created in the `JBOSS_HOME/server/JBOSS_PROFILE/log` directory. The Application log is a part of the default JBoss log output (the console and also the `JBOSS_HOME/server/JBOSS_PROFILE/log/server.log file`).

If you are not sure about the logging configuration, do one of the following:

- Use the HP Systinet Self-Tester, which reports the location of the log4j configuration in use.

- Add the option `-Dlog4j.debug` to the application server start command and restart the application server.

  Log4j then outputs configuration messages to the console.

Default Log4j Configuration

The default log4j configuration from a deployed HP Systinet is shown in "Log4j Configuration File".

Note: HP Systinet tools use the configuration from `SYSTINET_HOME/conf/log4j.config`, which may be different.

Log4j Configuration File

```
# put all logs to console and a log file
log4j.rootLogger=INFO,stdout,file
```

```
# console appender
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.Target=System.out
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%p: %c{2} - %m%n

# file appender
log4j.appender.file=org.apache.log4j.RollingFileAppender
log4j.appender.file.maxFileSize=20MB
log4j.appender.file.maxBackupIndex=5
log4j.appender.file.File=log4j.log
log4j.appender.file.threshold=INFO
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%d{ABSOLUTE} %5p %c -
%m%n

# audit log appender
log4j.appender.Systinet_AUDIT=org.apache.log4j.RollingFileAppender
log4j.appender.Systinet_AUDIT.File=hpsoa_audit.log
log4j.appender.Systinet_AUDIT.MaxFileSize=10000KB
log4j.appender.Systinet_AUDIT.MaxBackupIndex=10
log4j.appender.Systinet_AUDIT.layout=org.apache.log4j.PatternLayout
# see
http://-
log-
ging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html
# for formating rules, following extra arguments can be moreover used
to
# customize the format
#   %X{audit.eventId} - event ID
#   %X{audit.result} - event result
#   %X{audit.category} - event category
#   %X{audit.ctxId} - event context id
#   %X{audit.actor} - event actor
#   %X{audit.resource} - event actor
#   %X{audit.detail} - event detail
log4j.appender.Systinet_AUDIT.layout.ConversionPattern="%d",%X
{audit.category}:%X{audit.eventId},
   %X{audit.result},%X{audit.ctxId},"%X{audit.actor}","%X
{audit.resource}",%X{audit.detail}%n

# configure audit logging
log4j.category.com.hp.systinet.audit.event=DEBUG,Systinet_AUDIT
log4j.additivity.com.hp.systinet.audit.event=true

# limit categories that are too verbose
log4j.category.org.apache.xml.security=ERROR,file,stdout
log4j.additivity.org.apache.xml.security=true
log4j.category.org.hibernate=ERROR,stdout,file
```

```
log4j.additivity.org.hibernate=true
```

This configuration instructs log4j to do the following:

1. Print information,warning, and error messages to the console, and to a file named `log4j.log`, for all logging categories that are not explicitly declared.

   HP Systinet also uses the logging categories which start with one of the following:

   ■ com.hp.systinet

   ■ org.hp.systinet

   ■ com.systinet

   ■ org.systinet

2. Print the audit log to a file named `hpsoa_audit.log`

   The format of the log is specified in the `log4j.appender.Systinet_ AUDIT.layout.ConversionPattern` property in "Log4j Configuration File". Each audit event is a single line that starts with date and time (formatted according to ISO8601), followed by comma separated attributes of the event.

3. A deployed HP Systinet creates the log files in the following locations:

   ■ For JBoss:

   `JBOSS_HOME/server/PROFILE_NAME/log`

   ■ For WebLogic:

   `DOMAIN_HOME`

   ■ For WebSphere:

   `PROFILE_HOME`

4. The logging category, `com.hp.systinet.audit.event`, is used to log audit events. This logging category also has subcategories according to the audit event category. For example, the logging category name for audit events in the *licensing* category is `com.hp.systinet.audit.event.licensing`.

   You can change the output or strip down the audit log for any particular audit category.

5. The other declared logging categories (hibernate, apache xml security) are stripped to only log error messages. These categories are too verbose for printing if information messages are also logged (the default for all categories).

Audit Logging

HP Systinet also uses an audit log to contain events triggered by HP Systinetfunctionality. HP Systinet creates an `hpsoa_audit.log` in the default application server logging directory.

Deploy to the JDKless Environment

To complete deployment to a JDKless envrionment.

In the Build Environment, prepare a final deployment archive.

1. For JBoss, execute JSP script compilation:

   ./4.10/deploy/jboss/jspc/precompile_jsps.sh

2. Copy the precompiled EAR file to the application server and rename it `hp-soa-systinet.ear.`

3. Archive the HP Systinet installation folder (including JBoss or WebLogic domain).

   tar -cjf hp-systinet-4.10-deployment-01.tar.bz2 /opt/hp/systinet

In the Target Environment, extract the archive:

tar -jxvf hp-systinet-4.10-deployment-01.tar.bz2 /opt/hp/systinet

Note: It is useful to keep previous versions of archived deployments, alongside exported data images to speed-up the process of updating or restoring a deployment.

Chapter 8

Upgrading HP SOA Systinet

If you have an installation of HP SOA Systinet 3.x, you can upgrade to Systinet 4.x.

Upgrade from 3.x consists of the following parts:

- "Apply Custom Extensions from HP SOA Systinet 3.x" (on page 137)
- "Migrate Data from HP SOA Systinet 3.x" (on page 138)

Apply Custom Extensions from HP SOA Systinet 3.x

Systinet 4.x contains significant changes to the architecture model. If you have customized extensions, apply them to Systinet 4.x.

To Apply Custom Assertion Extensions:

1. Install Assertion Editor as part of Systinet Workbench 4.x.

2. Create a new assertion project based on the old extension in Assertion Editor 4.x.

3. Assertion Editor highlights any errors in the extension. Repair these errors with reference to "Model Changes" in the *Reference Guide*.

4. Build the extensions in Assertion Editor 4.x.

5. Apply the extensions to Systinet 4.x.

For details, see the *Assertion Editor Guide*.

Caution: If you use other methods to migrate the assertion extension (for example, import an old assertion project folder or opening an old workspace), 3.x assertions contain invalid data in their meta files. Manually remove any `associatedApplication` tags from assertion meta files in your workspace.

To Apply Custom Taxonomy Extensions:

1. Install Taxonomy Editor as part of SystinetWorkbench 4.x.

2. Create a new taxonomy project based on the old extension in Taxonomy Editor 4.x.

3. Taxonomy Editor highlights any errors in the extension. Repair these errors with reference to "Model Changes" in the *Reference Guide*.

4. Build the extensions in Taxonomy Editor 4.x.

5. Apply the extensions to Systinet 4.x.

For details, see the *Taxonomy Editor Guide*.

Caution: If your taxonomy extension contains customized system taxonomies (for example, `lifecycleStages` and `documentTypes`), they are merged with the corresponding system taxonomy in HP Systinet 4.x. In the event of a conflict the old system taxonomy takes precedence.

To Apply Custom Model Extensions:

1. Install Customization Editor as part of Systinet Workbench 4.x.

   Note: If your old extension contains references to assertion or taxonomy projects you must do the following:

   a. Create assertion and taxonomy projects in Systinet Workbench 4.x based on the existing customization extension.

   b. Repair any errors in the assertion and taxonomy projects.

2. Create a new extension project based on the old extension in Customization Editor 4.x.

   Note: If your old extension contains references to assertion or taxonomy projects you must add references to the assertion and taxonomy projects created in the previous step. Use the **Properties->Project References** option or the project references step in the Create Extension Project wizard.

3. Customization Editor highlights any errors in the extension. Repair these errors with reference to "Model Changes" in the *Reference Guide*.

4. Build the extensions in Customization Editor 4.x.

5. Apply the extensions to Systinet 4.x.

For details, see the *Customization Editor Guide*.

Systinet features a redesigned UI, so UI customizations for the 3.x UI are not migrated in customization extensions. UI customization is now an administration feature. For details, see "UI Customization" in the *Administrator Guide*.

Custom Java code in old extensions should be reviewed.

To Apply Custom Reporting Extensions:

1. Install Report Editor as part of Systinet Workbench 4.x.

2. Create a new report project based on the old extension in Report Editor 4.x.

3. Open each report to highlight any errors in the report. Repair these errors with reference to "Model Changes" in the *Reference Guide*.

   Note: The SQL schema is changed so pay special attention to reports that use SQL instead of DQL.

4. Build the extensions in Report Editor 4.x.

5. Apply the extensions to Systinet 4.x.

For details, see the *Report Editor Guide*.

Note: Report categorization does not exist in Systinet 4.x. All custom reports from Report Editor 4.x are available for use in the Reports tab using the Custom Reports **Add Report** functionality. HP advises reviewing the layouts of your old custom reports to fit the Reports tab.

Migrate Data from HP SOA Systinet 3.x

Systinet 4.x is not backwards compatible with *HP SOA Systinet 3.x* data. You can import data images from HP SOA Systinet 3.x into Systinet 4.x using a migration tool provided in the

installation.

If you are migrating from a version of HP SOA Systinet earlier than 3.x or if you encounter problems during custom migration, contact HP Professional Services for assistance.

Tip: Prior to migration, HP recommends purging activity reports and recreating the Activity Report Task. There may be thousands of these reports or revisions of them due to internal reporting activity and removing them may significantly reduce the migration process time.

To Remove Activity Reports in HP SOA Systinet 3.x:

1. Open **View Reports -> All** in the Tools tab.

2. Filter the reports, using name `Activity Report`.

3. Use the selection drop-down and **Select All**.

4. Expand **Select Action**, and select **Delete**.

5. Select **Non-Recoverable Deletion** and **Ignore Incoming Artifacts**, and leave **Delete Sub-Artifacts** unselected.

6. Confirm the deletion.

   Note: The deletion may take some time.

7. Open the detail view of the **Activity Report Update Task** in the Tools tab.

8. Delete the task with Non-Recoverable Deletion option selected.

9. Create a new task using the following parameters:

Parameter	Value
Name	Activity Report Update Task
Tool	Activity Report update job
Recurrence	Daily

To Migrate Data from HP SOA Systinet 3.x to 4.x:

1. In Systinet 3.x, execute the export command:

   SYSTINET_HOME/bin/export *dataimage.zip*

   For details, see the "Export Tool" section of the *Systinet 3.x Administration Guide*.

2. In Systinet 4.x, execute the data migration command:

   SYSTINET_HOME/bin/migrate --image *dataimage.zip* --output *migratedimage.zip* --validate

   Note: Execute **migrate --help** to view the available options for the migrate tool. If you use password encryption, use the passphrase setup up for Systinet 4.x if it is different from that of HP SOA Systinet 3.x.

   The migrate tool creates an image folder matching the output of the export tool ready for import to Systinet 4.x. The validate switch performs XML schema validation on the resulting data image. If errors occur, it typically indicates that your deployment has some non-standard

customization. Depending on the type of error, you need to either follow the upgrade process described in "Apply Custom Extensions from HP SOA Systinet 3.x" or contact HP Technical Support. The migration tool logs progress to `SYSTINET_HOME/log/migrate.log`. When some error occurs during the migration, it is logged in this file.

3. In Systinet 4.x, execute the import tool:

SYSTINET_HOME/bin/import --image *migratedimage.zip*

For more details, see "Import Tool" in the *Administration Guide*.

Caution: The import should not be run using the **--force** switch. This can overwrite built-in core data, such as taxonomies, with data from 3.x which may impact server functionality. Only use **--force** if you know exactly what the effect is.

Details of the migration are reported to a log file accessible at `SYSTINET_ HOME/log/migrate.log`.

Note: HP recommends updating Oracle Database schema statistics after importing large amounts of data. Old statistics may impact the performance of some data queries. Consult your database administrator.

To Update Oracle Schema Statistics:

- Execute the following command:

EXEC DBMS_STATS.GATHER_SCHEMA_STATS (ownname = '&1',no_invalidate = FALSE,options = 'GATHER');

This command does not require database admin privileges and can be run by the schema owner (ownname).

Pay particular attention to the following migrations:

- **Group Membership**

During import, the group membership of the migrated image is merged with any existing group membership.

Note: Import of a 4.x image replaces the current group membership with the imported group membership.

- **SOAP Services Imported from BSM / UCMDB**

Systinet 4.x automatically creates Service artifacts associated with SOAP Services imported from BSM / UCMDB. In 3.x, these Service artifacts are only created when the imported SOAP Service is entered into governance. HP recommends processing imported SOAP Services in HP SOA Systinet 3.x before performing migration. If you cannot process all SOAP Services before migration, then review the UCMDB Import page in Systinet 4.x after migration, and create appropriate Service artifacts and relations to the imported SOAP Services before entering them into governance.

- **Assertions**

In Systinet 4.x, existing assertions, `Has Approved References`, `Has At Least One Approved Reference`, and `Has Documentation`, have existing parameters that have

been changed to only support the value of categories in taxonomies, `Lifecycle stages`, `Artifact types`, and `Document types`.

If you have custom technical policies which use these assertions and you have modified these taxonomies, you should review the parameters in those technical policies.

- **Business Policies**

  Business Policies have been replaced in Systinet 4.x with Policy Reports. In the following rare cases the migration tool does not translate a business policy to a policy report:

  - Business Policies with included/excluded artifacts are not migrated.

  - 'Not in Categories' properties are skipped during migration.

  These report as a `WARNING` in the log file, 'A BP was not automatically migrated and must be migrated manually'.

  The migrated policy report name may be unattracted. Use the Policy Report Details page Edit context action to open the Edit page for the report, which automatically fixes the name, and Save the report.

- **UI Customizations for the Business Analyst, Business Partner, and Custom Tabs**

  UI customizations for the Business Analyst, Business Partner, and custom tabs from HP SOA Systinet 3.2x migrate as part of the data image. Use the UI customization features in the Administration tab in Systinet 4.x to verify and change these customizations after data migration is complete. For details, see "UI Customization" in the *Administration Guide*.

  Caution: After migration, if your UI customization still contains references to UI components with `/impl/` in their name, they should be removed. Systinet 4.x no longer supports these components.

The following data from HP SOA Systinet 3.x does not migrate to 4.x:

- **Rebranding** - rebranding is related to the UI which has changed extensively in 4.x. To rebrand the new UI, see "Rebranding Systinet" in the *Administration Guide*.

- **Customized Dashboards** - the Dashboard in HP SOA Systinet 3.x is replaced by the Reports tab in Systinet 4.x with similar features. For details, see "Reporting Overview" in the *User Guide*.

- **Validation Data** - validation data is not migrated.

- **Areas of Interest Reports** - areas of interest no longer exist in Systinet 4.x.

- **Tasks** - the model relating to tasks is changed in Systinet 4.x so tasks and their related data does not migrate. To setup up tasks, see "Administration Task Management" in the *Administration Guide*.

- **Stored Searches** - the model relating to stored searches in changed in Systinet in 4.x so stored searches and their related data does not migrate. To setup saved searches, see "How to Use Saved Searches" in the *User Guide*.

- **Trend Reports** - trend reports no longer exist in Systinet 4.x.

Chapter 9

Starting and Configuring Systinet

After deployment, you should start Systinet and apply any required final configuration.

For details, see the following sections:

Start Systinet in JBoss

Execute the following command:

- **SYSTINET_HOME/bin/serverstart**

- For some production environments, **serverstart** may not be appropriate.

  Execute **JBOSS_HOME/bin/run** instead.

Start Systinet in WebLogic

After installation, start Systinet using WebLogic.

To Start Systinet in WebLogic:

1. Start a node manager:

   WL_HOME/server/bin/startNodeManager

2. Start an administration server:

   DOMAIN_HOME/startWebLogic

3. Start the server hosting Systinet:

   DOMAIN_HOME/bin/startManagedWebLogic *MY_MANAGED_SERVER*

Start Systinet in WebSphere

- Start Systinet in WebSphere with the following command:

  WS_HOME/AppServer/profiles/PROFILE_NAME/bin/startServer

- To start the WebSphere cluster:

  - In your browser, open the WebSphere Administration Console:

    ```
    http://localhost:9060/admin
    ```

    Note: The port may vary depending on your settings.

- Select **Servers**, and then **Clusters**.

- Click your CLUSTER_NAME.

- Click **Start**.

- When the server starts, you can validate if the requests are load balanced across the cluster.

  In your browser, use the URL:

  http://localhost/snoop

  The Snoop servlet page should appear, displaying the port number.

  Every time you refresh the page, the port number should change.

  http://localhost/systinet/web should display the HP Systinet user interface.

Enable Full-Text Search in Systinet

Full-text search must also be enabled in the Systinet UI.

To Enable FTS:

1. Sign in to Systinet as the administrator.

2. In the Administration tab Administration menu, click **Configuration** to open the Configuration page.

3. In the Basic Settings tab, select **Full Text Search**.

4. Click **Save** to apply the setting.

Turn Off Systinet Self-Test

The self-test output is accessible to anyone using the URL. For security reasons, you can switch off access to the self-test output after a completed deployment of Systinet passes the self-test.

To Switch Off Self-Test Output:

1. Sign in to Systinet as the administrator.

2. In the Administration tab Administration menu, click **Configuration** to open the Configuration page.

3. In the Configuration page, select the **Self Test** tab.

4. Click **Disable** to switch Self-Test off.

To disable the standalone self-tester, undeploy the self-test-standalone.war package from your server.

To verify that the self-test has been disabled, check the self-test output URL:
http://*hostname*:*port*/*context*/self-test.