HP Systinet

For the Windows and Linux operating systems

Software Version: 10.00

Installation and Deployment Guide

Document Release Date: November 2014

Software Release Date: November 2014

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 2003-2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Intel® Xeon® and Intel® Core i7® are registered trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®,Windows®,Windows® XP and Windows 7® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of TheOpenGroup.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Contents ... 3
In this Guide ... 7
Prerequisites and Supported Platforms ... 8
Design Your Deployment ... 8
Prerequisites for Hardware ... 9
Prerequisites - JDK Software ... 10
Recommended Environments ... 10
Supported Database Types ... 11
Supported Application Servers ... 11
Prerequisites - Operating Systems ... 11
Prerequisites - Browsers ... 12
Prerequisites - Mail Clients ... 12
Supported LDAP Implementations ... 12
Prerequisites - Adobe Flash ... 13
Supported Product Integrations ... 13
Deploying to Environments without a JDK ... 13
HTTP Proxy Server Requirement ... 14
Install Systinet with a Proxy Server ... 14
How to Install a Proxy Server ... 14
How to Configure Systinet with a Proxy Server ... 16
Test the Proxy Server Installation ... 17
Preparing Databases ... 18
Database Installation Types ... 18
Set Up Oracle Database ... 20
Set Up an Oracle Power User ... 21
Set Up an Oracle Common User ... 22
Set Up Microsoft SQL Database ... 23
Set Up an MSSQL Power User ... 25
Set Up an MSSQL Common User ... 25

Setting Up Application Servers 27
Deploy Systinet Self-Test 27
Setting Up JBoss 29
Configure a Data Source for JBoss 30
Configure JMS for JBoss 32
Modify the JBoss Run Script 34
Set the JBoss Data Source Maximum Pool Size 35
Preparing LDAP and SiteMinder 36
Prepare LDAP Integration 36
Set Up SiteMinder Endpoint Authentication 37
Using the Systinet Wizard Installer 39
Step 1 - Start the Systinet Installation 41
Step 2 - Welcome 43
Step 3 - License 44
Step 4 - Installation Folder 45
Step 5 - Scenario Selection 46
Step 6 - Updates 47
Step 7 - Custom Extensions 48
Step 8 - Password Encryption 49
Step 9 - Database Selection 51
Step 10 - Database Setup 52
Step 11 - Database Parameters 52
MSSQL Create Database 53
MSSQL Create Schema 54
Oracle Create Tablespace 55
Oracle Create Schema 57
Step 12 - JDBC Drivers 59
Step 13 - Repository Import 61
Step 14 - Application Server Selection 62
Application Server Configuration 62
Step 15 - Endpoint Properties 64

Step 16 - User Management Integration 65
LDAP Service Properties 66
LDAP Search Rules 67
LDAP User Properties Mapping 68
LDAP Group Search Rules 70
LDAP Group Properties Mapping 71
Step 17 - System Email Configuration 72
Step 18 - Administrator Account Configuration 73
Step 19 - SMTP Server Authentication 74
Step 20 - License Information 75
Step 21 - Confirmation 76
Step 22 - Installation Progress 76
Completing the HP Systinet Installation 76
Decoupled Database Script Execution 76
Finish Decoupled Database Installation 77
Create an Archive for JDKless Deployment 77
Deploying Systinet 78
Set Up Authentication 78
Set Up Role Mapping 79
Set Up SiteMinder Integration 80
Deploying Systinet to JBoss 80
Enable SSO in JBoss Clusters 81
Modify JBoss Logging 81
Enable Non-Latin HTTP Parameters in JBoss 82
Redeploy the EAR File to JBoss 82
Enable Full-Text Search in MSSQL 83
Enable Full-Text Search in Oracle 84
Configure LDAP over SSL/TLS 86
Log4j Configuration 87
Deploy to the JDKless Environment 90
Upgrading HP Systinet 91

Apply Custom Extensions from HP Systinet 4.x 91
Migrate Data from HP Systinet 4.x 93
Starting and Configuring HP Systinet 97
Start Systinet in JBoss 97
Enable Full-Text Search in Systinet 97
Turn Off Systinet Self-Test 97

Chapter 1

In this Guide

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

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 8

  Design your environment for Systinet.

- "Preparing Databases" on page 18

  Set up and configure your database for Systinet.

- "Preparing LDAP and SiteMinder" on page 36

  Set up LDAP and SiteMinder for Systinet.

- "Using the Systinet Wizard Installer" on page 39

  Use the GUI Installer to install Systinet.

- "Deploying Systinet" on page 78

  Configure your environments and deploy Systinet.

- "Upgrading HP Systinet" on page 91

  Migrate extensions and data from previous versions of Systinet.

- "Starting and Configuring HP Systinet" on page 97

  Start Systinet and perform UI-based final configuration.

Chapter 2

Prerequisites and Supported Platforms

Before installing 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" below
- "Prerequisites for Hardware" on the next page
- "Prerequisites - JDK Software" on page 10
- "Recommended Environments" on page 10
- "Supported Database Types" on page 11
- "Supported Application Servers" on page 11
- "Prerequisites - Operating Systems" on page 11
- "Prerequisites - Browsers" on page 12
- "Prerequisites - Mail Clients" on page 12
- "Supported LDAP Implementations" on page 12
- "Prerequisites - Adobe Flash" on page 13
- "Supported Product Integrations" on page 13
- "Deploying to Environments without a JDK" on page 13
- "HTTP Proxy Server Requirement"

Also see the "Support Matrix Guide" for information about the supported hardware and software and software and configurations that are compatible with Systinet.

Design Your Deployment

- **Trial Version**
  If you want to evaluate Systinet, you can download a Virtual Appliance (VA) trial version. You must have a VM host on your computer to run the VA trial version. The trial version contains a 60 instant-on license, which can be renewed.

To download the trial version, go to http://www.hp.com. Select **For Work > Software > See all Software > Free & Trial Software > On-premise software** tab. Search for the HP Systinet VA product name and click **Download now**.

- **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. Systinet comes with a embedded JBoss.

  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.

- **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 Systinet Wizard Installer.

  Systinet supports a silent non-wizard installation that can be executed at the command-line in one step. The silent installation can easily be plugged in to higher-level orchestration and deployment engines. For advanced security hardening, decoupled DBA scenarios, or recovery and failover procedures, see the HP Live Network or the advanced documentation at the HP Support website.

  For information about a silent installation, run the jar file using the `-help` option:

  ```
  java -jar hp-systinet-10.00.jar -help
  ```

Prerequisites for Hardware

HP recommends the following minimum hardware for each physical node of a distributed production environment for both application and database servers:

- Intel Xeon E processor family, 8 cores, 16 GB RAM, 40 GB free disk space, 1Gbps network card.
- Network bandwidth of 1 Gb/sec or higher.

For customization and evaluation purposes, Systinet requires the following hardware:

- Intel Core i7 processor, 8 GB RAM, 40 GB free disk space, 1Gbps network card.
- Network bandwidth of 100Mb/sec or higher.

SPARC machines are not suitable for Systinet deployments.

Example:

It is possible to evaluate Systinet on a system that has the following configuration:

- x64-based PC Intel(R) Core(TM) i7-3720QM CPU @ 2.60GHz, 4 Core(s), 8 Logical Processor (s)
- Physical Memory (RAM) 8 GB
- 500GB HDD Intel(R) 7 Series Chipset Family SATA
- Intel(R) 82579LM Gigabit Network

Prerequisites - JDK Software

Each machine runningSystinet 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.

Systinet supports JDK 1.7.

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.

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 1.7 then proceed with installation.
   - If JAVA_HOME does not point to JDK 1.7 then reset the JAVA_HOME environment variable to a valid JDK 1.7.

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

Recommended Environments

HP recommends the following environments:

- Oracle (Sun) JDK 1.7 64-bit

Supported Database Types

Systinet supports the following databases:

- Oracle 11g (11.2.0.3.0)
- Oracle 12c (12.1.0.1.0)
- Microsoft SQL 2014
- Microsoft SQL 2012 (SP1)

Systinet supports deployment to the following database and driver combinations:

Supported Database Drivers

Database	DB Version	Driver Packages	Driver Version	Driver Class
Oracle Database	11.2.0.3.0	ojdbc6.jar, orai18n.jar	11.2.0.3.0	oracle.jdbc.driver. OracleDriver
	12.1.0.1.0	ojdbc7.jar, orai18n.jar	12.1.0.1.0	
Microsoft SQL Server	2012 SP1 2014	sqljdbc4.jar	4.0	com.microsoft.sqlserver.jdbc. SQLServerDriver

Supported Application Servers

HP Systinet can be deployed to the JBoss 7 or JBoss EAP 6.2 server which is integrated in the installation package (Embedded JBoss7).

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 Server 2012 R2
- Windows Server 2008 R2
- Linux (RedHat 5.6, 6)
- Linux (Ubuntu 12, 12.4)

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:

- Google Chrome (latest version)
- Microsoft Internet Explorer 10 or newer
- Mozilla Firefox (latest version)
- Mozilla Firefox ESR (latest version)
- Chrome latest

Prerequisites - Mail Clients

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

- Microsoft Outlook 2013
- Microsoft Outlook 2010
- Microsoft Outlook 2007
- GMail

Supported LDAP Implementations

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

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

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 HP Systinet require Adobe Flash Player version 11.0 or newer.

Supported Product Integrations

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).
HP Business Service Management (BSM)	9.2x	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 Application Lifecycle Manager	11.50, 11.52, 12.00	Service test monitoring for ALM 11.50, 11.52. Requirement repository for ALM 12.00.
Layer7	7.1, 8.1	Service proxy and policy discovery. Contract deployment and status synchronization.
DataPower	6.0.1.0	Service proxy and policy discovery. Contract deployment and status synchronization.

Deploying to Environments without a JDK

The Systinet installation framework supports deployment of 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 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.

HTTP Proxy Server Requirement

Due to security and cluster support, an HTTP proxy server must be installed before installing Systinet. Apache is the recommended proxy server. The HTTP proxy server will mitigate the impact of existing and future security defects in the embedded JBoss application server.

This section describes how to install Systinet with a Proxy Server in the following topics:

"Install Systinet with a Proxy Server" below

"Test the Proxy Server Installation" on page 17

Install Systinet with a Proxy Server

Follow the steps below to enable accessing Systinet through a proxy server.

1. "How to Install a Proxy Server" below as follows:
   a. Install the Apache Web Server

   b. Configure the Apache Web Server as a Reversed Proxy

   c. (Optional) Enable SSL in the Apache Web Server

2. "How to Configure Systinet with a Proxy Server" on page 16.

How to Install a Proxy Server

1. Install the Apache Web Server.

   It is recommended that you use the Apache web server as the proxy server by enabling `mod_proxy`. A stable version of the Apache Web Server (2.4.10) can be downloaded from the Apache website http://httpd.apache.org/ .

2. Configure the Apache Web Server as a Reversed Proxy:

   a. After the Apache web server is installed, go to `APACHE_HOME\conf` and `backup httpd.conf`.

   b. Edit `the httpd.conf` file as follows:

      - Change the HTTP port: Listen **80**

      - Enable the Proxy modules:

        ```
        LoadModule proxy_module modules/mod_proxy.so
        ```

```
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

- Add these lines at the end:

  ProxyRequests Off

  ProxyPass `/systinet http://[host]:[port]/systinet`

  ProxyPassReverse `/systinet http://[host]:[port]/systinet`

- If SSL is enabled for this proxy server, also add the line:

  SSLProxyEngine on

c. Restart the Apache Web Server.

3. Configure SSL for the Apache Web Server:
   a. Prepare the folder:
      - Create `openssl` directory inside Apache home.
      - Copy `openssl.cnf` from `/conf` to `/openssl`
      - CD to `/openssl`
   b. Generate a new certificate request:

      ```
      ..\bin\openssl req -config .\openssl.cnf -new -out cert.csr
      ```

      Provide the following information:

      - Enter PEM pass phrase: **<password>**

      - Verifying - Enter PEM pass phrase: **<password>**

      - Country Name (2 letter code) [AU]:**<country>**

      - State or Province Name (full name) [Some-State]:**<state>**

      - Locality Name (such as city)[]:**<city>**

      - Organization Name (such as company) [Internet Widgits Pty Ltd]:**<company>**

      - Organizational Unit Name (such as section) []:**<organization unit>**

      - Common Name (such as server FQDN or YOUR name) []:**<hostname>**

      - Email Address []: **<email>**

- A challenge password []:

- An optional company name []:

c. Convert the private key file:

```
..\bin\openssl rsa -in privkey.pem -out cert.key
```

Provide below information:

- Enter pass phrase for privkey.pem:**<password>**

d. Create a self-signed certificate (output is also a CA certificate):

```
..\bin\openssl x509 -in cert.csr -out cert.crt -req -signkey cert.key -da
ys 365
```

e. Edit or add the following lines in httpd-ssl.cnf

- Change SSL port: Listen **443**

  <VirtualHost _default_:443>

- Set certificate paths

  SSLCertificateFile "C:/Program Files (x86)/Apache Software Foundation/Apache2.2/openssl/cert.csr"

  SSLCertificateKeyFile "C:/Program Files (x86)/Apache Software Foundation/Apache2.2/openssl/cert.key"

  SSLCertificateChainFile "C:/Program Files (x86)/Apache Software Foundation/Apache2.2/openssl/cert.crt"

f. Restart the Apache Web Server.

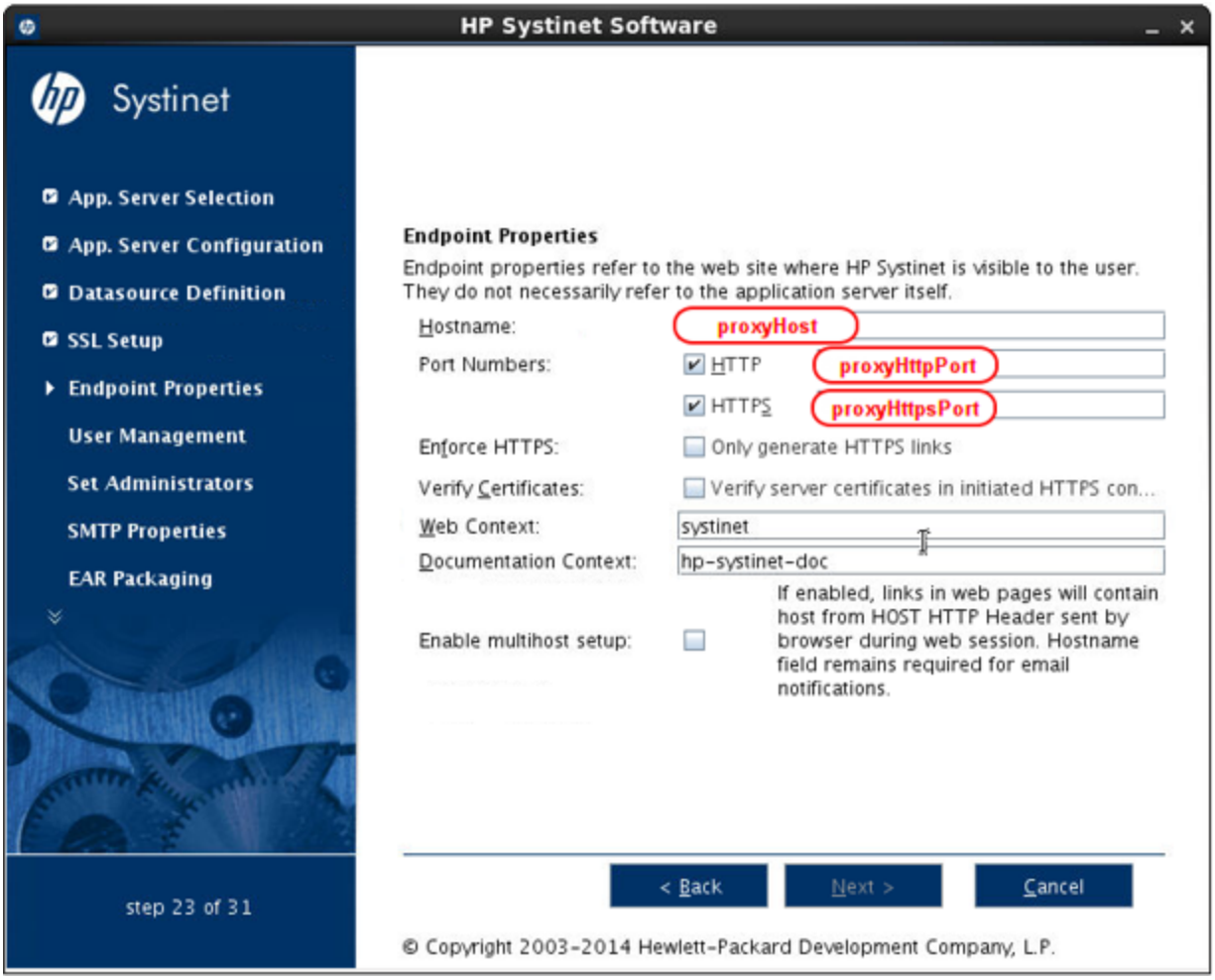
g. On the client browser, add **cert.crt** to Trusted Root CA.

If openssl is installed with Apache web server, make sure it is patched frequently to avoid security issues.

How to Configure Systinet with a Proxy Server

To configure Systinet with proxy server, provide proxy server hostname and ports instead of real server hostname and ports during Systinet installation or by running **Setup** tool after Systinet is installed.

If we install Systinet on an application server rather Embedded JBoss 7, we have to redeploy **hp-soa-systinet.ear** file after changing Endpoint Properties in Setup tool.



Test the Proxy Server Installation

Access the proxy server with URL: `http://[proxyHost]:[proxyPort]/systinet`

A successful configuration should result in:

1. Systinet login is shown.
2. Browser address bar shows URL of the proxy server instead of the Systinet server.

Chapter 3

Preparing Databases

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

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

Read "Database Installation Types" below 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 acceptable.

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 Microsoft SQL Database" on page 23
- "Set Up an MSSQL Power User" on page 25

Database Installation Types

- **Create Schema**

  The Create Schema option is available in the GUI installer and command-line deployment. Power users can select this option to create tables and indexes in the default schema in an existing database or tablespace.

  You can select this option if you meet the following guidelines

  - The database administrator must provide a database or table space.
  - HP recommends that you begin with an empty schema.
  - The database administrator must create a power user.

> **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:

  - **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 4.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 11.2.0.3.0 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	11.2.0.3.0	ojdbc6.jar, orai18n.jar	11.2.0.3.0	oracle.jdbc.driver. OracleDriver
	12.1.0.1.0	ojdbc7.jar, orai18n.jar	12.1.0.1.0	

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.

  Note: Oracle 11g does not support full-text searching of Microsoft 2010 files. To use this capability, you need to upgrade to Oracle 12c.

- 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" below
- "Set Up an Oracle Common User" on the facing page

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.
5. Grant permissions required for XA transactions:

   ```
   DEFINE us = &username;
   ```

```
DEFINE pass = &pass;

GRANT SELECT ON sys.dba_pending_transactions TO &&us;
GRANT SELECT ON sys.pending_trans$ TO &&us;
GRANT SELECT ON sys.dba_2pc_pending TO &&us;
GRANT EXECUTE ON sys.dbms_system TO &&us;
GRANT EXECUTE ON sys.dbms_xa TO &&us;
```

For Oracle 12C, grant the following explicit previleges:

```
GRANT Unlimited tablespace TO &&us;

GRANT CREATE SESSION, CREATE PROCEDURE, CREATE SEQUENCE TO &&us;
```

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_na
me || ';' 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
```

4. For more information see step 5 "Grant permissions required for XA transactions:" on page 21

Set Up Microsoft SQL Database

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 4.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	2014, 2012 SP1	sqljdbc4.jar	4.0	com.microsoft.sqlserver.jdbc.SQLServerDriver

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 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 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.

> **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 Power User" below
- "Set Up an MSSQL Common User" below

Set Up an MSSQL Power User

You can use the Create Schema option during installation or for a manual database arrangement. The database administrator must create a power user with appropriate privileges to the database .

To Set Up a Power User in MSSQL:

1. Create an account that has *public* Server Role.
2. Add the `SqlJDBCXAUser` database role on the *master* database.
3. Add the `db_datareader`, `db_datawriter`, and `db_ddladmin`, *public* database roles on the Systinet database.

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

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

The deployment of the Systinet Self-Test and the set up of the JBoss application server are explained in the following sections:

- "Deploy Systinet Self-Test" below
- "Setting Up JBoss" on page 29

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-10.00.jar -x SYSTINET_HOME

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

2. Deploy the WAR file in one of the following ways:
   - Use the functionality of your JBoss application server.
   - Copy the WAR file to your JBoss deploy directory.
3. Create a marker file with the name: `self-test-standalone.war.dodeploy` in the same directory. See the `JBOSS_HOME/standalone/deployments/README.txt` for more information.

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 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 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 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 Systinet EAR file and starting Systinet. At this point all checks should pass if the application server and 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.

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 `SYSTINET_HOME/jboss`.

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

- "Configure a Data Source for JBoss" on the next page
- "Configure JMS for JBoss" on page 32
- "Modify the JBoss Run Script" on page 34
- "Set the JBoss Data Source Maximum Pool Size" on page 35

There are additional steps to complete deployment to JBoss after installation. For details, see "Deploying Systinet to JBoss" on page 80.

Configure a Data Source for JBoss

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.

- "Set Up the MSSQL Data Source" below
- "Set Up the Oracle Data Source" on the facing page

Set Up the MSSQL Data Source

To Set Up the data source for MSSQL:

1. Copy the MSSQL JDBC driver to `JBOSS_HOME/jboss/modules/systinet/jdbc/main`.
2. Open the file `JBOSS_HOME/standalone/configuration/standalone-full.xml`, and add the `xa-datasource` element, which contains information regarding the `connectionURL`, `driver`, `user-name`, and `password` elements. Edit these elements to match your local environment.
3. Add a driver element with the value of `systinet` under these elements:

   `xa-datasource` element

   `drivers` element which uses the `xa-datasource-class` element
4. Change the value of the `xa-datasource-class` element to `com.microsoft.sqlserver.jdbc.SQLServerXADataSource`.
5. Set the `jndi-name` attribute to `java:jboss/hpsoasystinetDS` and the `pool-name` attribute to `hpsoasystinetDS`.
6. Add a `max-pool-size` element as the direct child of the `xa-pool` element, which is at the same level as `security`.
7. 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 standalone-full.xml

```
    <subsystem xmlns="urn:jboss:domain:datasources:1.0">
        <xa-datasource jndi-name="java:/hpsoasystinetDS" pool-name="hpsoasy
stinetDS">
            <xa-datasource-property name="URL">
                [connectionURL]
            </xa-datasource-property>
```

```
            <driver>systinet</driver>
            <transaction-isolation>TRANSACTION_READ_COMMITTED</transaction-
isolation>
            <xa-pool>
                <min-pool-size>5</min-pool-size>
                <max-pool-size>100</max-pool-size>
                <prefill>false</prefill>
            </xa-pool>
            <security>
                <user-name>[username]</user-name>
                <password>[password]</password>
             </security>
         </xa-datasource>
         <drivers>
             <driver name="systinet" module="systinet.jdbc">
                <xa-datasource-class>com.microsoft.sqlserver.jdbc.SQLServer
XADataSource</xa-datasource-class>
             </driver>
         </drivers>
     </subsystem>
```

8. Save `standalone-full.xml`.

Set Up the Oracle Data Source

To Set Up the data source for Oracle:

1. Copy the Oracle JDBC driver to `JBOSS_HOME/jboss/modules/systinet/jdbc/main`.
2. Open the file `JBOSS_HOME/standalone/configuration/standalone-full.xml`, and add the `xa-datasource` element, which contains information regarding the `connectionURL`, `driver`, `user-name`, and `password` elements. Edit these elements to match your local environment.
3. Add a driver element with the value of `systinet` under these elements:

   `xa-datasource` element

   `drivers` element which uses the `xa-datasource-class` element
4. Change the value of the `xa-datasource-class` element to `oracle.jdbc.xa.client.OracleXADataSource`.
5. Set the `jndi-name` attribute to `java:jboss/hpsoasystinetDS` and the `pool-name` attribute to `hpsoasystinetDS`.
6. Add a `max-pool-size` element as the direct child of the `xa-pool` element, which is at the same level as `security`.
7. 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 standalone-full.xml

```
     <subsystem xmlns="urn:jboss:domain:datasources:1.0">
         <xa-datasource jndi-name="java:/hpsoasystinetDS" pool-name="hpsoasy
stinetDS">
             <xa-datasource-property name="URL">
                [connectionURL]
             </xa-datasource-property>
             <driver>systinet</driver>
             <transaction-isolation>TRANSACTION_READ_COMMITTED</transaction-
isolation>
             <xa-pool>
                 <min-pool-size>5</min-pool-size>
                 <max-pool-size>100</max-pool-size>
                 <prefill>false</prefill>
             </xa-pool>
             <security>
                 <user-name>[username]</user-name>
                 <password>[password]</password>
             </security>
         </xa-datasource>
         <drivers>
             <driver name="systinet" module="systinet.jdbc">
                <xa-datasource-class>oracle.jdbc.xa.client.OracleXADataSourc
e</xa-datasource-class>
             </driver>
         </drivers>
     </subsystem>
```

8. Save `standalone-full.xml`.

Configure JMS for JBoss

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

To configure JMS:

1. Open the `JBOSS_HOME/standalone/configuration/standalone-full.xml` file.

2. Define a proper re-delivery method for all topics and queues by inserting the following fragment

into the `<address-settings>` element of `<subsystem xmlns="urn:jboss:domain:messaging:1.1">`:

```
  <address-setting match="systinet.#">
    <redelivery-delay>60000</redelivery-delay>
    <max-delivery-attempts>5</max-delivery-attempts>
  </address-setting>
```

3. Systinet requires persistent queues and topics. Therefore, change the value of the `<persistence-enabled>enable` element to `true`. The `<persistence-enabled>` element is a direct child of the `subsystem` element.

4. Systinet requires insecure access to JMS. Therefore, change the value of the `<security-enabled>` enable element to `false`, which is also a direct child of the `subsystem`element.

   Following is the code snippet for the direct child of a messaging subsystem:

```
    <persistence-enabled>true</persistence-enabled>
    <security-enabled>false</security-enabled>
    <journal-file-size>102400</journal-file-size>
    <journal-min-files>2</journal-min-files>
```

5. JMS Connection factories should also limit its pools (50 threads by default) by setting up `<thread-pool-max-size>50</thread-pool-max-size>` in each JMS connection factory found in the configuration property. The `thread-pool-max-size` can be configured using the `install.jboss7.jms.client.thread.pool.max.size` configuration property.

6. Insert the following elements into the `jms-destinations` part of the JMS module configuration to define the topics and queues:

```
<jms-queue name="systinet.scheduleTimerQueue">
   <entry name="queue/scheduleTimerQueue"/>
</jms-queue>
<jms-queue name="systinet.taskProcessorQueue">
   <entry name="queue/taskProcessorQueue"/>
</jms-queue>
<jms-queue name="systinet.ReportingExecutions">
   <entry name="queue/ReportingExecutions"/>
</jms-queue>
<jms-queue name="systinet.Validation">
   <entry name="queue/Validation"/>
</jms-queue>
<jms-queue name="systinet.PriorityValidation">
   <entry name="queue/PriorityValidation"/>
</jms-queue>
<jms-topic name="systinet.taskStopperTopic">
   <entry name="topic/taskStopperTopic"/>
</jms-topic>
```

Modify the JBoss Run Script

When you launch Systinet with the `SYSTINET_HOME/bin/serverstart` script, it calls `standalone.conf` 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 `standalone` 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 `standalone` 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/standalone.conf` 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.

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.

Memory sizing should take performance requirements into consideration for the deployed system. HP recommends that maximum heap size (-Xmx) should be at least 4096m.

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 Data Source Maximum Pool Size

The default JBoss Data Source Maximum Pool Size is not adequate for a production environment. For example, the default MaxPoolSize is based on the default Oracle configuration, which 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/standalone/configuration/standalone-full.xml` in an editor.
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.

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" below
- "Set Up SiteMinder Endpoint Authentication" on the next page

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/api/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/api/javax/naming/Context.html#INITIAL_CONTEXT_FACTORY

Property Name	Property Description	API Link
Security Principal	The name of the security principal for read access to the directory service.	http://java.sun.com/j2se/1.5.0/docs/api/javax/naming/Context.html#SECURITY_PRINCIPAL
Password	Password of security principal.	http://java.sun.com/j2se/1.5.0/docs/api/javax/naming/Context.html#SECURITY_CREDENTIALS
Security Protocol	Name of the security protocol. Default is "simple."	http://java.sun.com/j2se/1.5.0/docs/api/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 Systinet Wizard Installer

Using the Systinet Wizard Installer is the easiest way to install Systinet. However, it may not be suitable for all the configuration options required by production environments.

If the Systinet Wizard Installer is not suitable for your environment, you can use the silent installation. For information, run the jar file using the `-help` option:

```
java -jar hp-systinet-10.00.jar -help
```

You can also set advanced configuration options as described in these chapters: "Preparing Databases" on page 18 and "Deploying Systinet" on page 78.

Before using the Systinet Installer, make sure that your environment is set up correctly.

For hardware and software requirements, as well as supported platforms, see "Prerequisites and Supported Platforms" on page 8.

For an evaluation environment, you need valid credentials for a configured database. For details, see "Preparing Databases" on page 18.

JBoss does not require any additional configuration for evaluation purposes.

Systinet installation consists of the following steps:

1. "Step 1 - Start the Systinet Installation" on page 41
2. "Step 2 - Welcome" on page 43
3. "Step 3 - License" on page 44
4. "Step 4 - Installation Folder" on page 45
5. "Step 5 - Scenario Selection" on page 46
6. "Step 6 - Updates" on page 47
7. "Step 7 - Custom Extensions" on page 48
8. "Step 8 - Password Encryption" on page 49
9. "Step 9 - Database Selection" on page 51
10. "Step 10 - Database Setup" on page 52
11. "Step 11 - Database Parameters" on page 52

- "MSSQL Create Database" on page 53
- "MSSQL Create Schema" on page 54
- "Oracle Create Tablespace" on page 55
- "Oracle Create Schema" on page 57

12. "Step 12 - JDBC Drivers" on page 59
13. "Step 13 - Repository Import" on page 61
14. "Step 14 - Application Server Selection" on page 62
    - "Application Server Configuration" on page 62
15. "Step 15 - Endpoint Properties" on page 64
16. "Step 16 - User Management Integration" on page 65
    a. "LDAP Service Properties" on page 66
    b. "LDAP Search Rules" on page 67
    c. "LDAP User Properties Mapping" on page 68
    d. "LDAP Group Search Rules" on page 70
    e. "LDAP Group Properties Mapping" on page 71
17. "Step 17 - System Email Configuration" on page 72
18. "Step 18 - Administrator Account Configuration" on page 73
19. "Step 19 - SMTP Server Authentication" on page 74
20. "Step 20 - License Information" on page 75
21. "Step 21 - Confirmation" on page 76
22. "Step 22 - Installation Progress" on page 76

Step 1 - Start the Systinet Installation

1. Make sure the application server is not running.
2. Do one of the following:
   - Execute the file `hp-systinet-10.00.jar`, located on the installation CD or in your distribution directory.
   - Execute the following command:

     java -jar hp-systinet-10.00.jar
   - For manual database deployment, execute the following command:

     java -jar hp-systinet-10.00.jar -a
   - For deployment not using the JDK, generate the installation configuration file:

     java -jar hp-systinet-10.00.jar -s deployment.properties
   - **Caution:** For JBoss with HP-UX, execute the following command instead:

     java -jar hp-systinet-10.00.jar -Dshared.as.jboss.preloading.classes.at.startup=true

   The GUI Installation wizard opens displaying the Welcome page.

Continue to "Step 2 - Welcome" on page 43.

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 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 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***

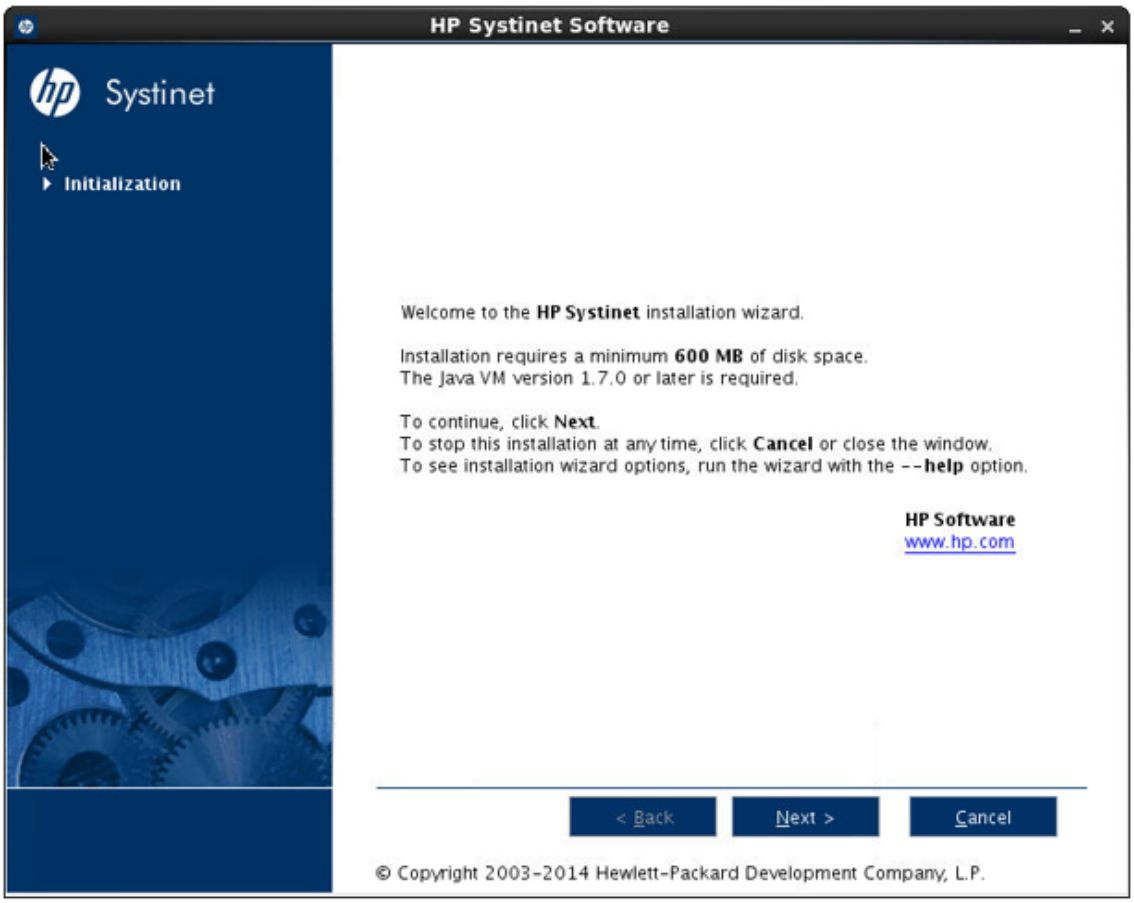
  If you want to use password encryption, specify the passphrase to use for encryption.

- **-d, --debug**

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

Step 2 - Welcome

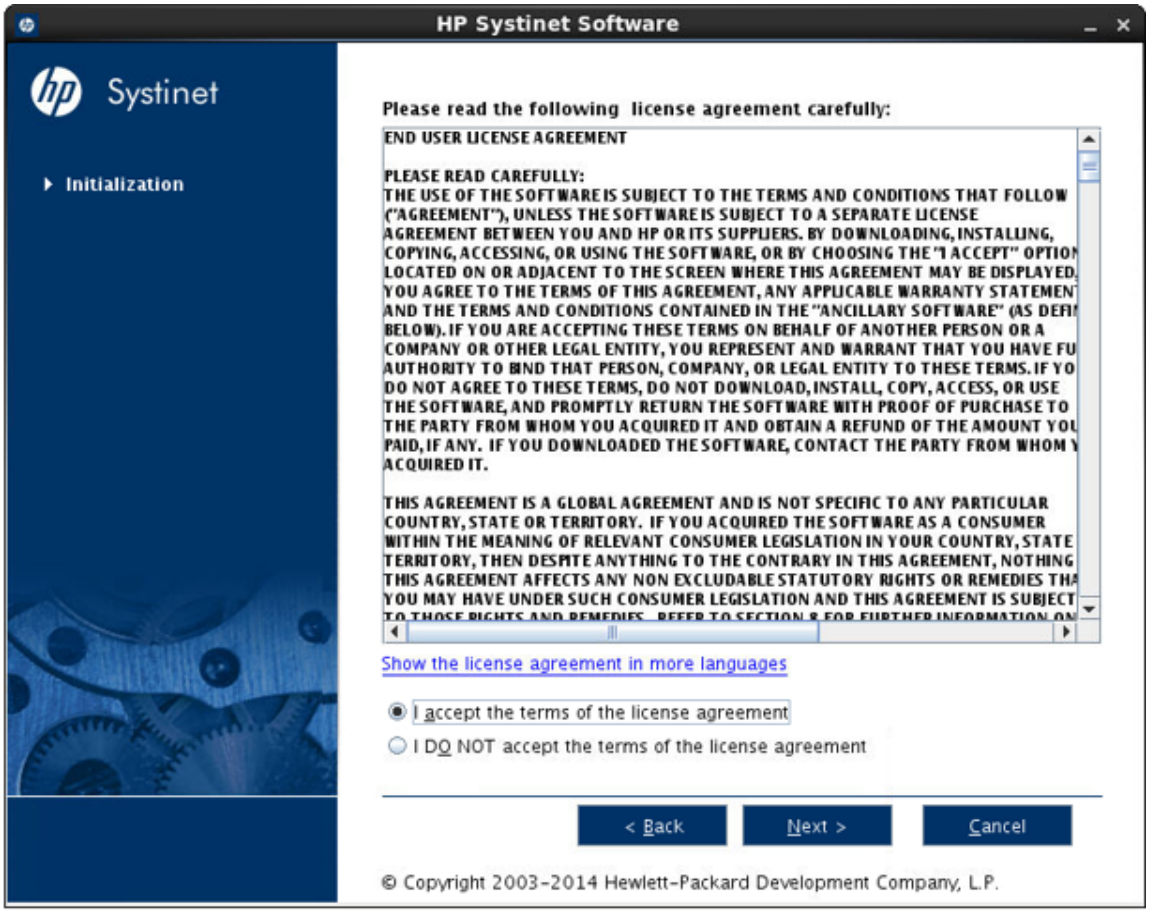
In the Welcome page, review the hardware and software requirements.



Click **Next** to continue to "Step 3 - License" on page 44.

Step 3 - 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.

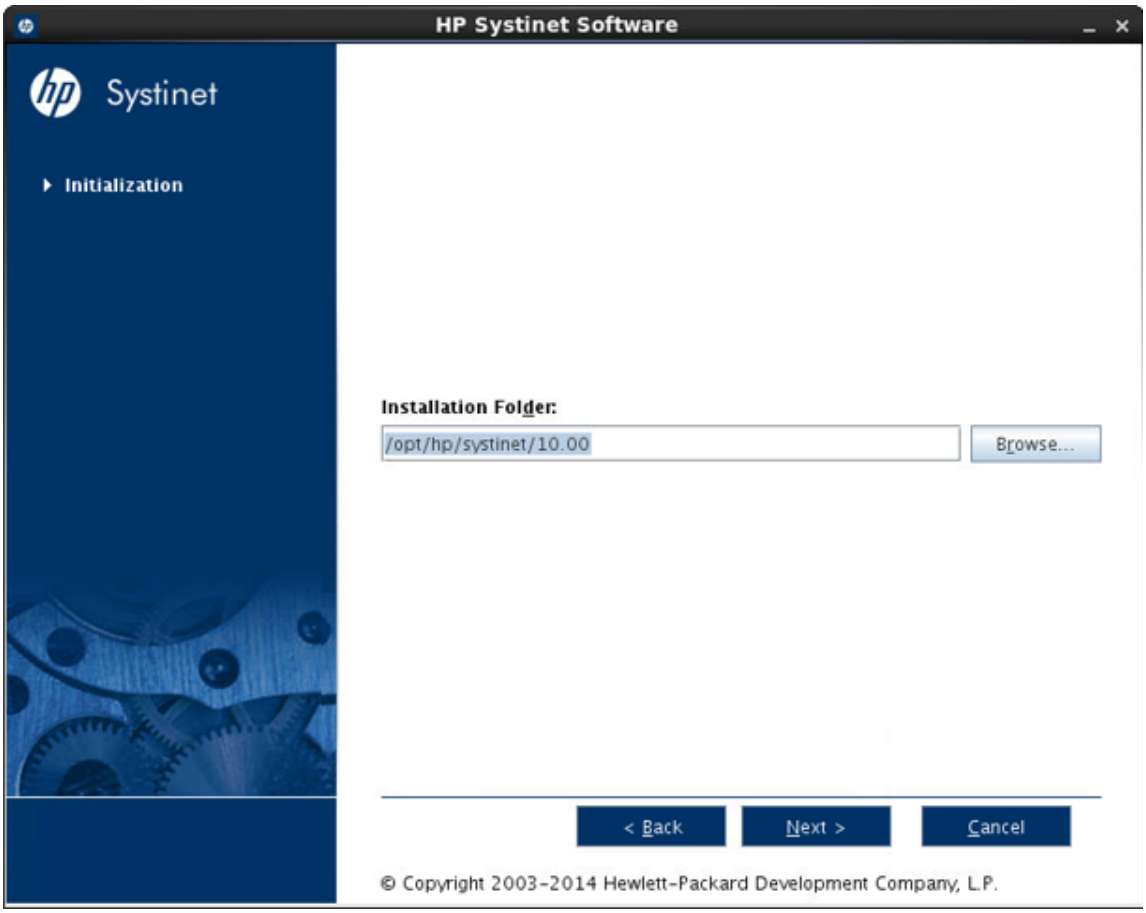
Select **I Accept the Terms of the License Agreement**.

Click **Next** to continue to "Step 4 - Installation Folder" on page 45.

Step 4 - Installation Folder

In the Installation Folder page, input or click **Browse** to select the location you want to use as your Systinet installation folder.

Note: The location name cannot contain more than 80 characters.



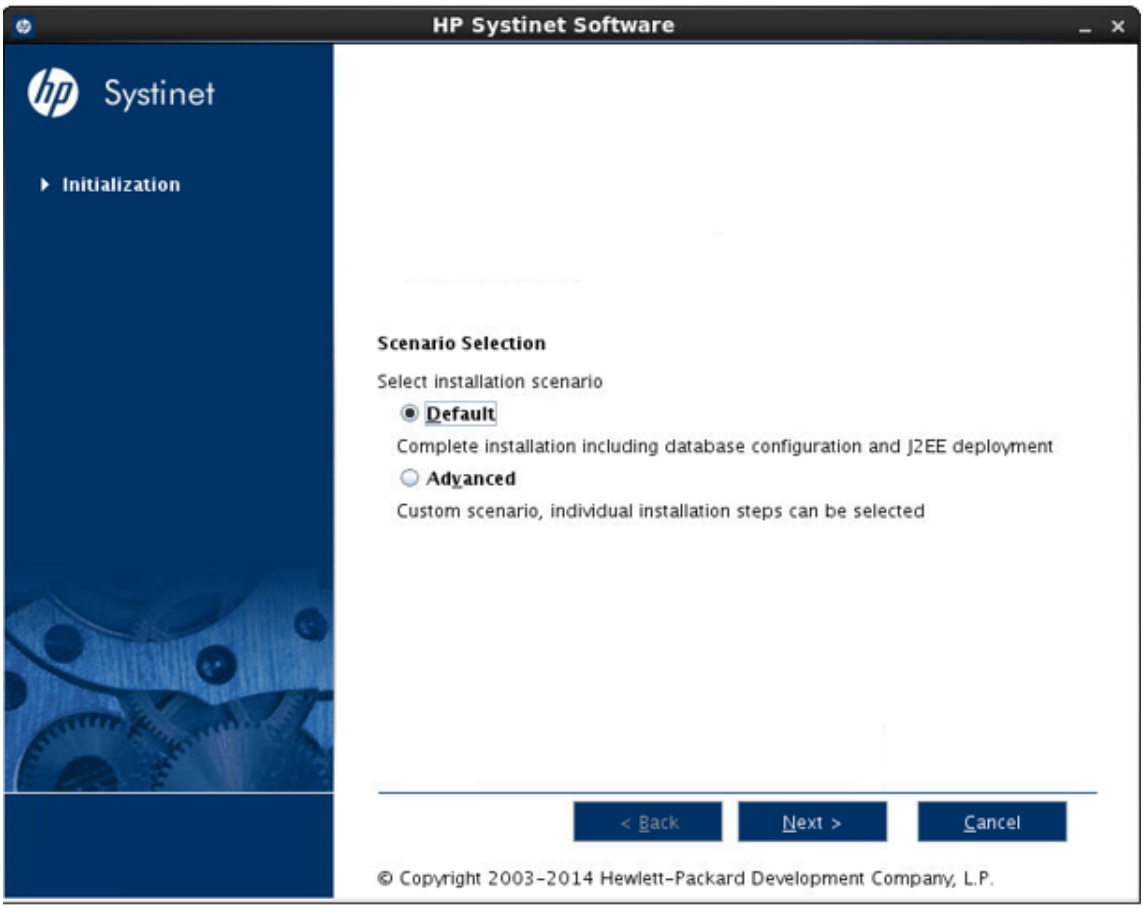
Caution: If you are upgrading from HP SOA Systinet 4.x, install to a new installation directory.

Note: In this document, the installation location is referred to as `SYSTINET_HOME`.

Click Next to unpack the distribution files to the chosen location and continue to "Step 5 - Scenario Selection" on page 46.

Step 5 - Scenario Selection

In the Scenario Selection page, select **Default**.

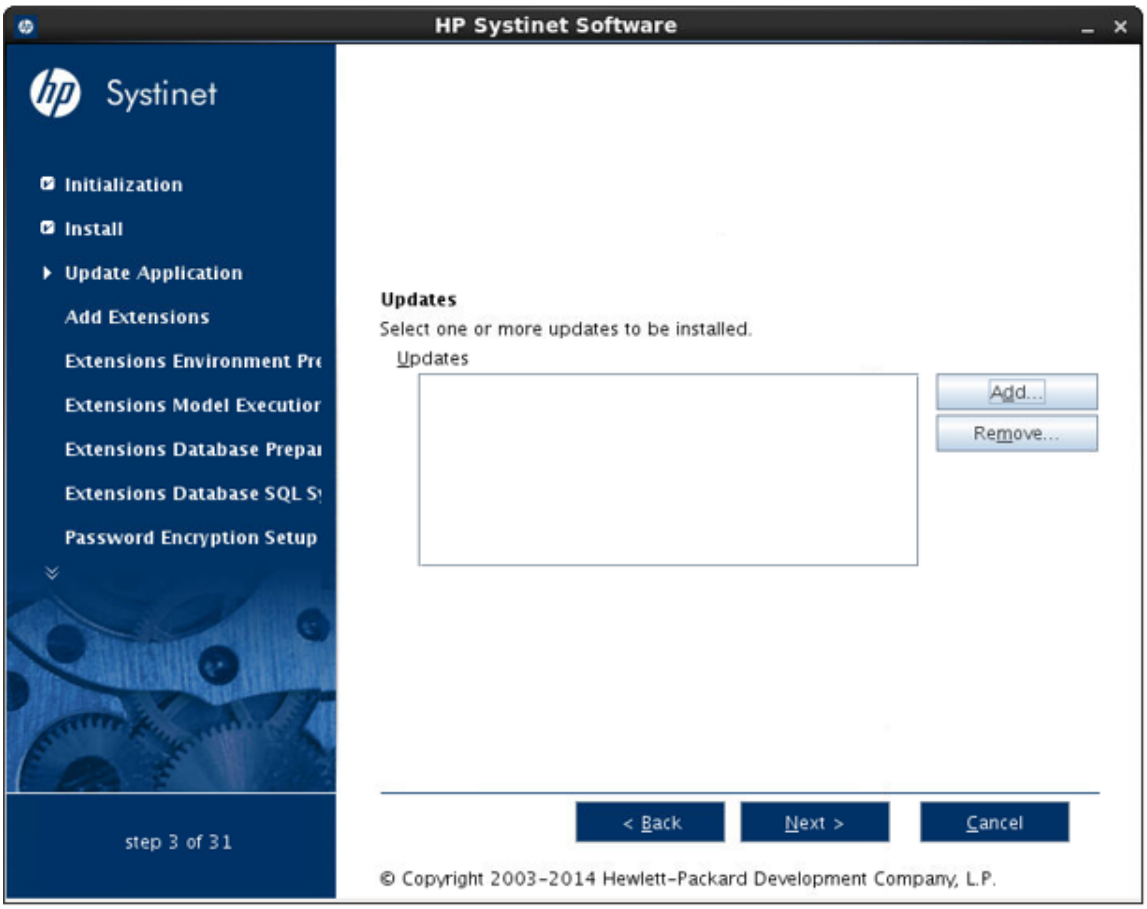


Note: The **Advanced** scenarios enable you to perform parts of the installation separately. These functions are duplicated by the Setup Tool and are discussed as administration functions. For details, see "Setup Tool" in the *Administrator Guide*.

Click **Next** to validate the installation and continueto "Step 6 - Updates" on page 47.

Step 6 - Updates

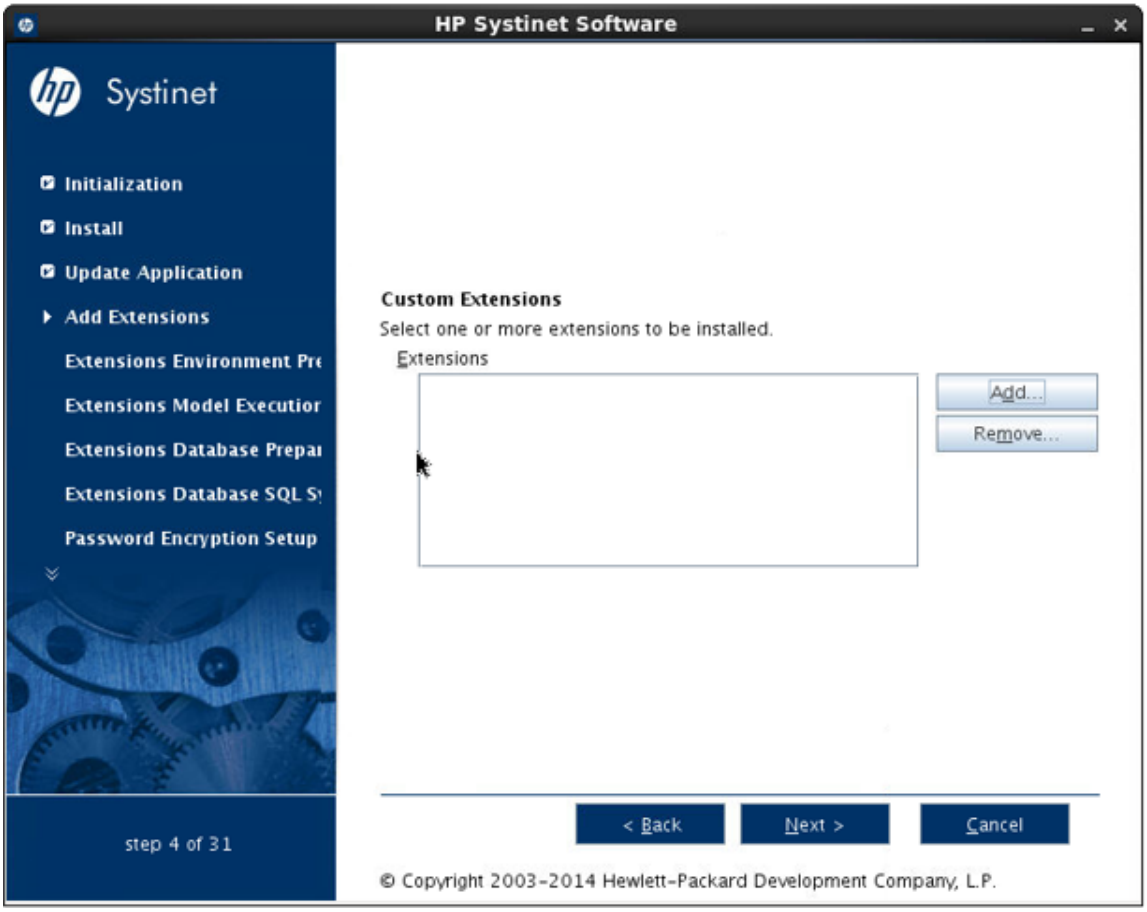
In the Updates page, use **Add** and **Remove** to select updates to apply during installation.



Click **Next** to verify any selected updates and continue to "Step 7 - Custom Extensions" on page 48.

Step 7 - Custom Extensions

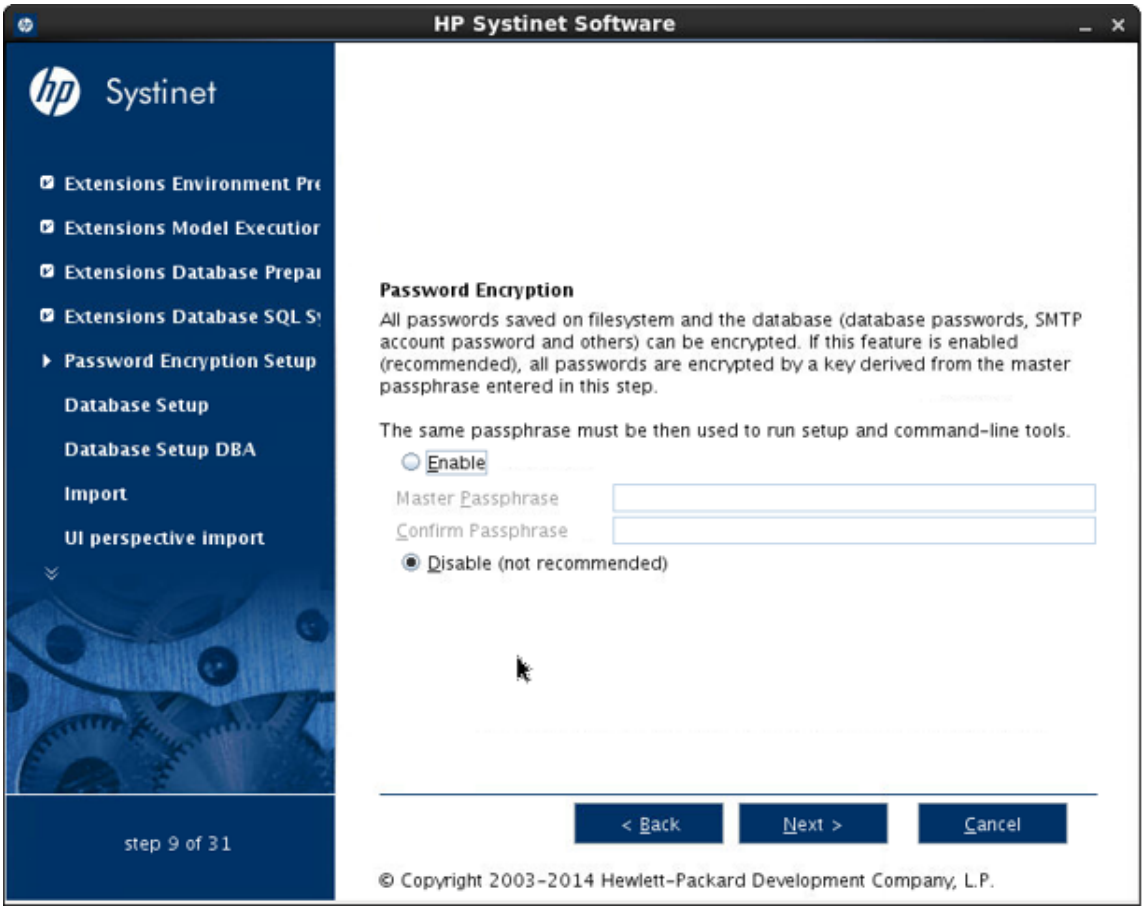
In the Custom Extensions page, use **Add** and **Remove** to select existing extensions that will extend the functionality of Systinet. The selected extensions will be applied during the installation.



Click **Next** to validate any selected extensions and continue to "Step 8 - Password Encryption" on page 49.

Step 8 - Password Encryption

In the Password Encryption page select whether Systinet protects credentials for access to other systems with strong encryption.



Do one of the following

- For production or sensitive installations, select **Enable** and type the **Master Passphrase** and **Confirm Passphrase**.
- For demo installations, select **Disable**.

Note: After installing with encryption, all passwords stored in the configuration file are in an encrypted, unreadable form without the provided passphrase. To execute the Setup Tool and some other command line tools, you may need to enter a passphrase or provide it using the **--passphrase** command line option.

Caution: Exported image is encrypted using Master Passphrase by default. If you want to

export an image without the passphrase, you must turn off the server passphrase, export the image, and then turn on the server passphrase.

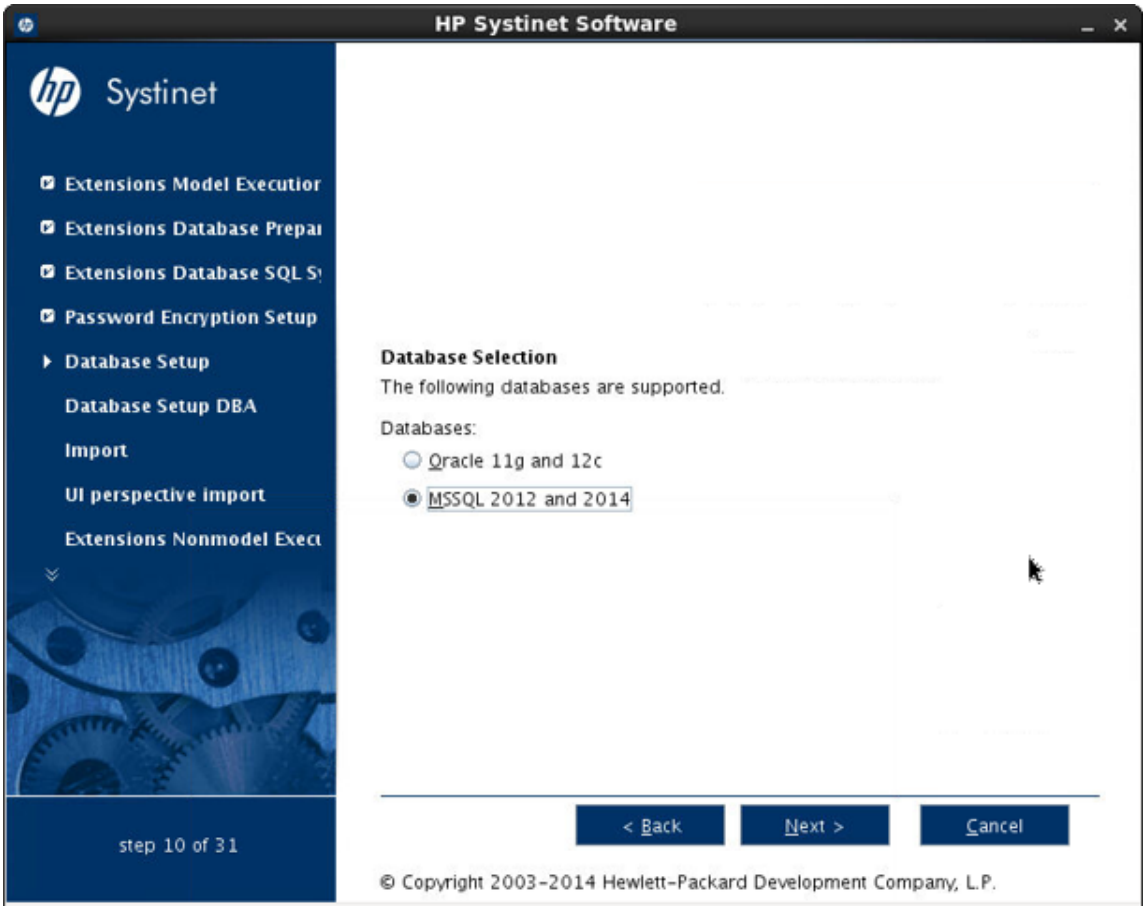
If you want to export an image without using the passphrase, you must turn off the server passphrase, export the image, and then turn on the server passphrase. Otherwise you will get an error.

If you enabled encryption, click **Next** to validate the encryption and continue to "Step 9 - Database Selection" on page 51.

If you disabled encryption, click **Next** to continue to "Step 13 - Repository Import" on page 61.

Step 9 - Database Selection

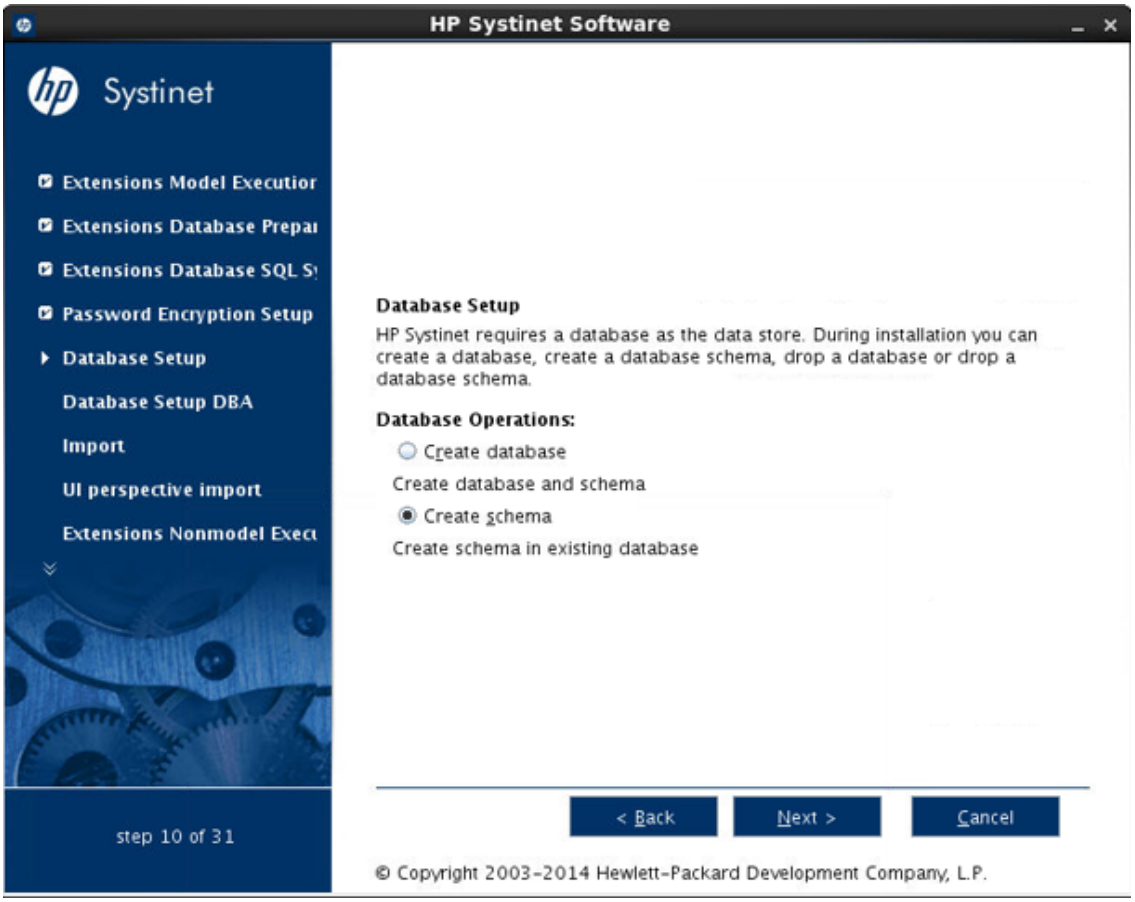
In the Database Selection Page, select the database type to use:



Select your database type and click **Next** to continue to "Step 10 - Database Setup" on page 52.

Step 10 - Database Setup

In the Database Setup Operations page, select your database installation type.



Click **Next** to open the Database Options page specific to the database and database installation type.

Continue to "Step 11 - Database Parameters" below.

Step 11 - Database Parameters

The required database parameters vary depending on your database type and setup type.

For details, see the appropriate section:

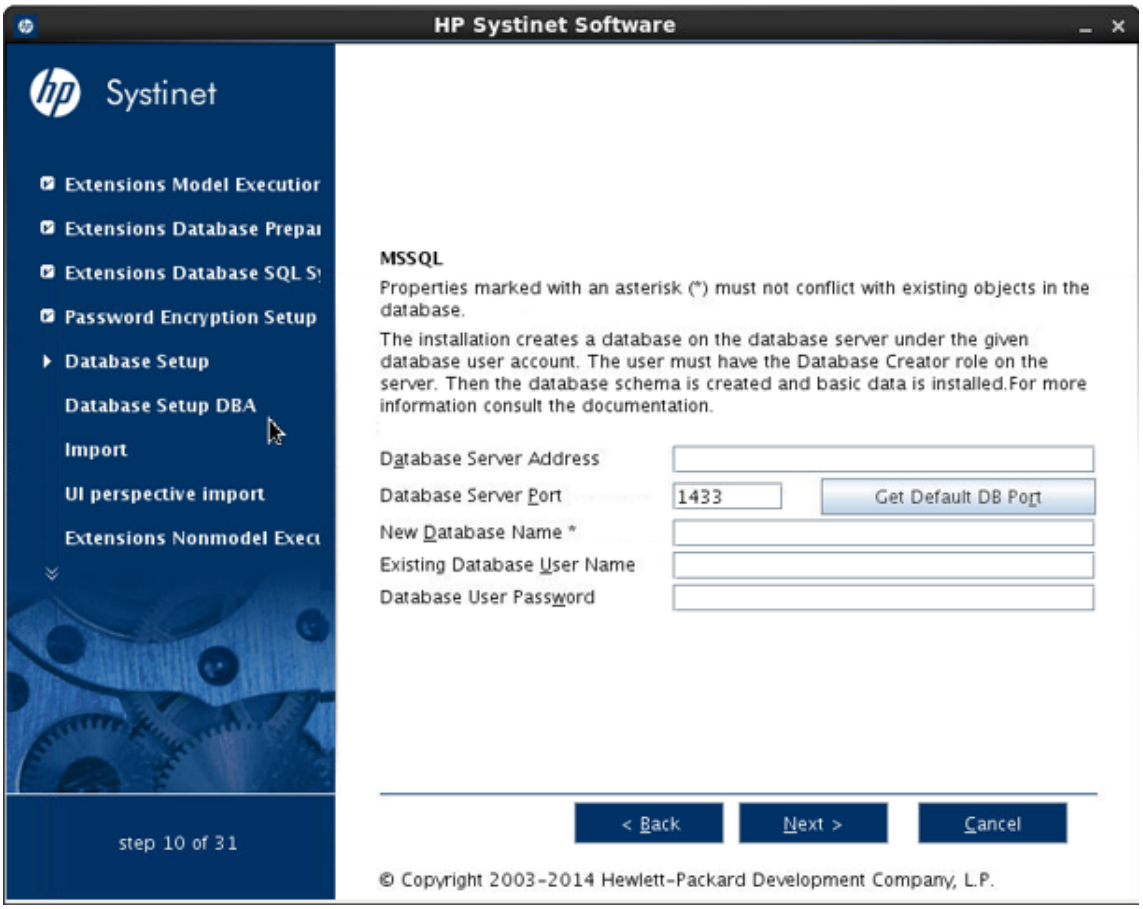
- "MSSQL Create Database" on the next page
- "MSSQL Create Schema" on page 54
- "Oracle Create Tablespace" on page 55
- "Oracle Create Schema" on page 57

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	For the Create Database option the user must have the database creator role. When using `integratedSecurity`, just fill non-blank text (dummy).	—
Database User Password		



Click **Next** to continue to "Step 12 - JDBC Drivers" on page 59.

MSSQL Create Schema

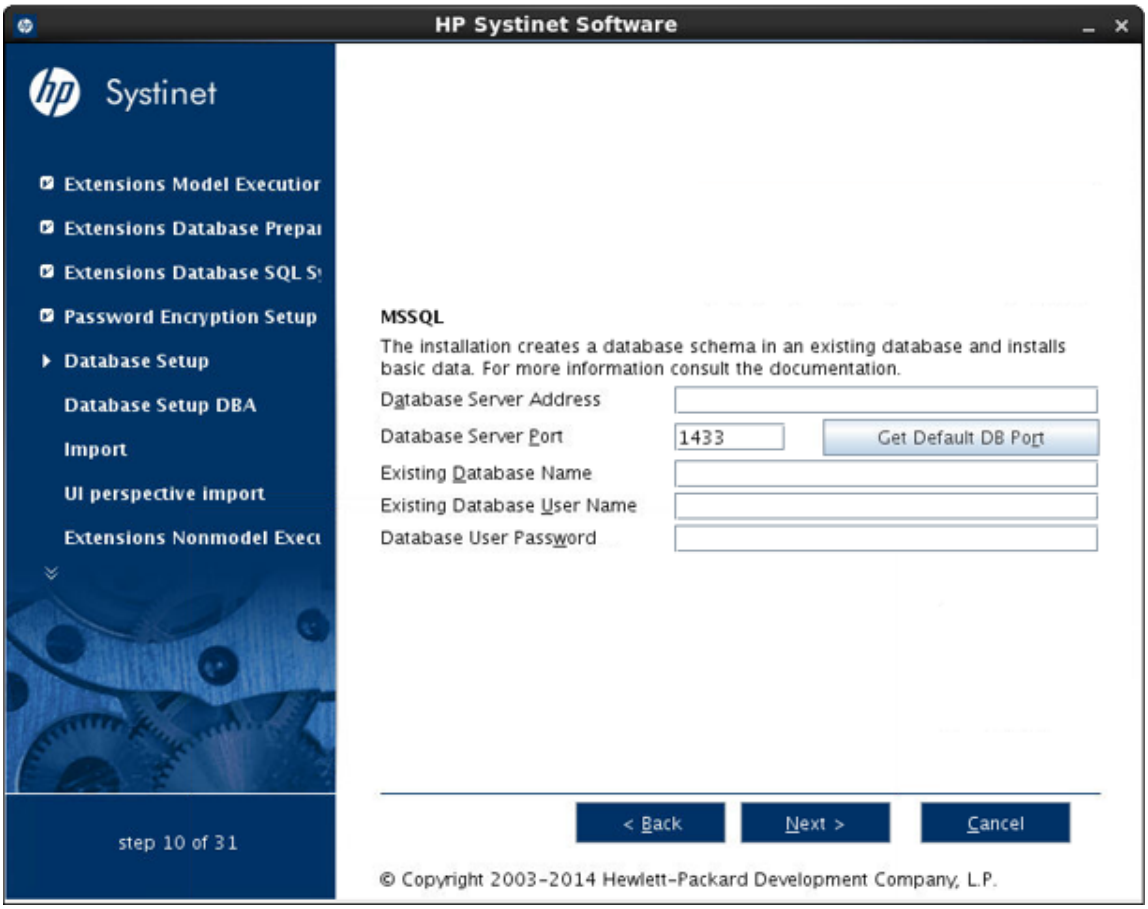
To create a new schema in MSSQL, set the following parameters:

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`.

MSSQL Create Schema Parameters, continued

Parameter	Description	Notes
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		



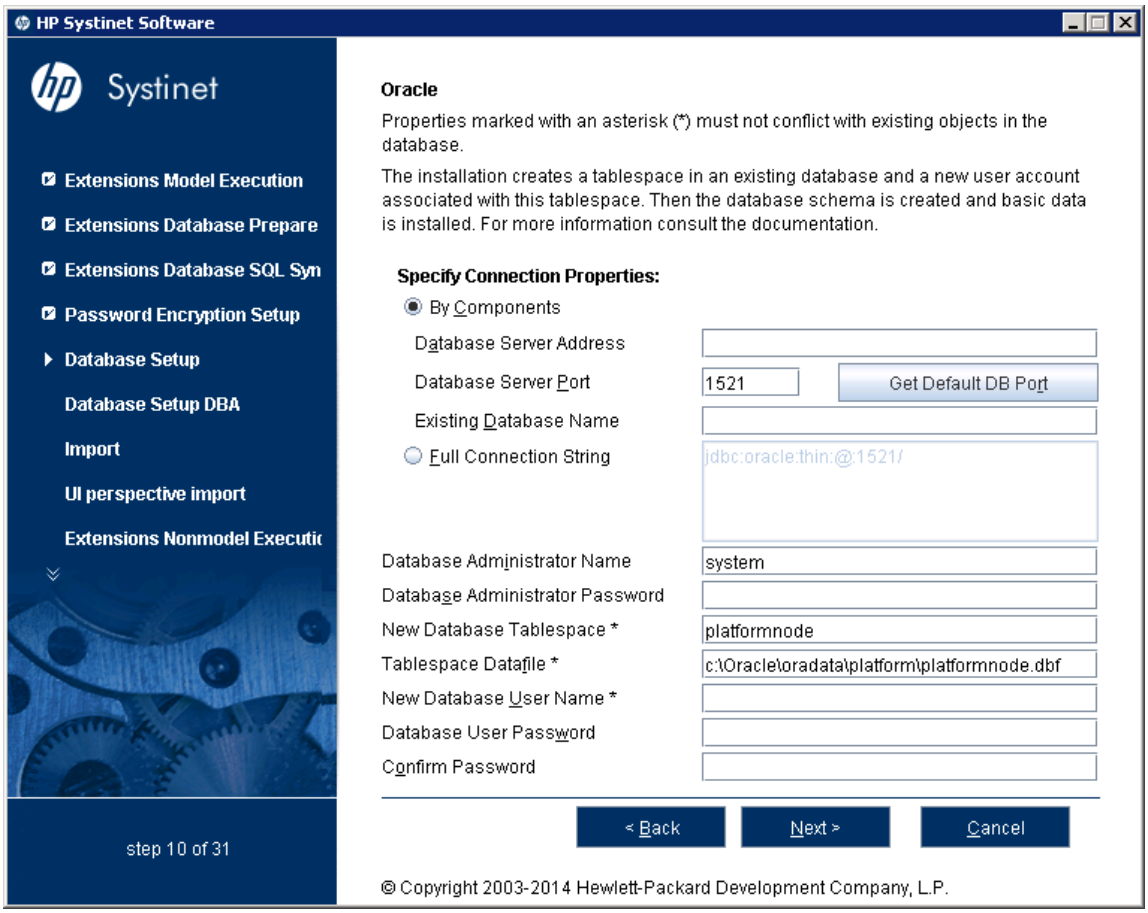
Click **Next** to continue to "Step 12 - JDBC Drivers" on page 59.

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 continue to "Step 12 - JDBC Drivers" on page 59.

Oracle Create Schema

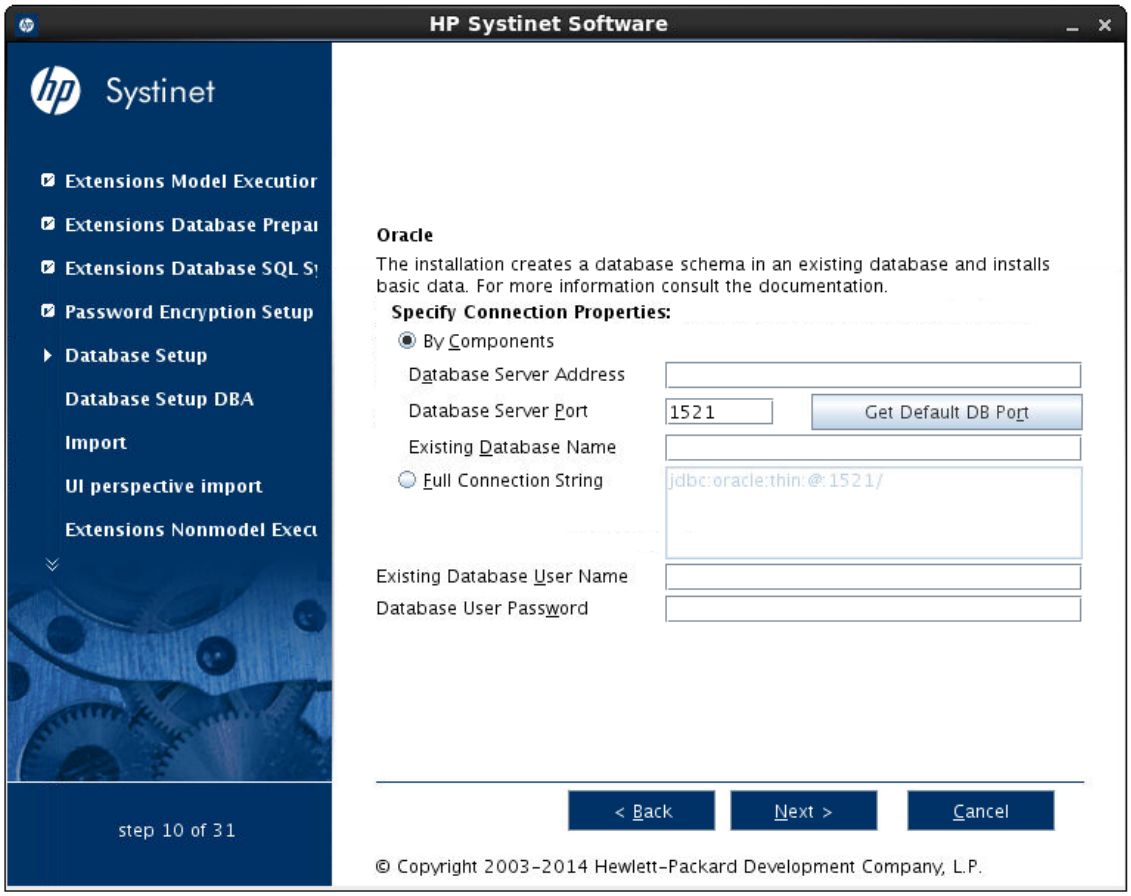
To create a new schema in Oracle, set the following parameters:

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`.

Oracle Create Schema Parameters, continued

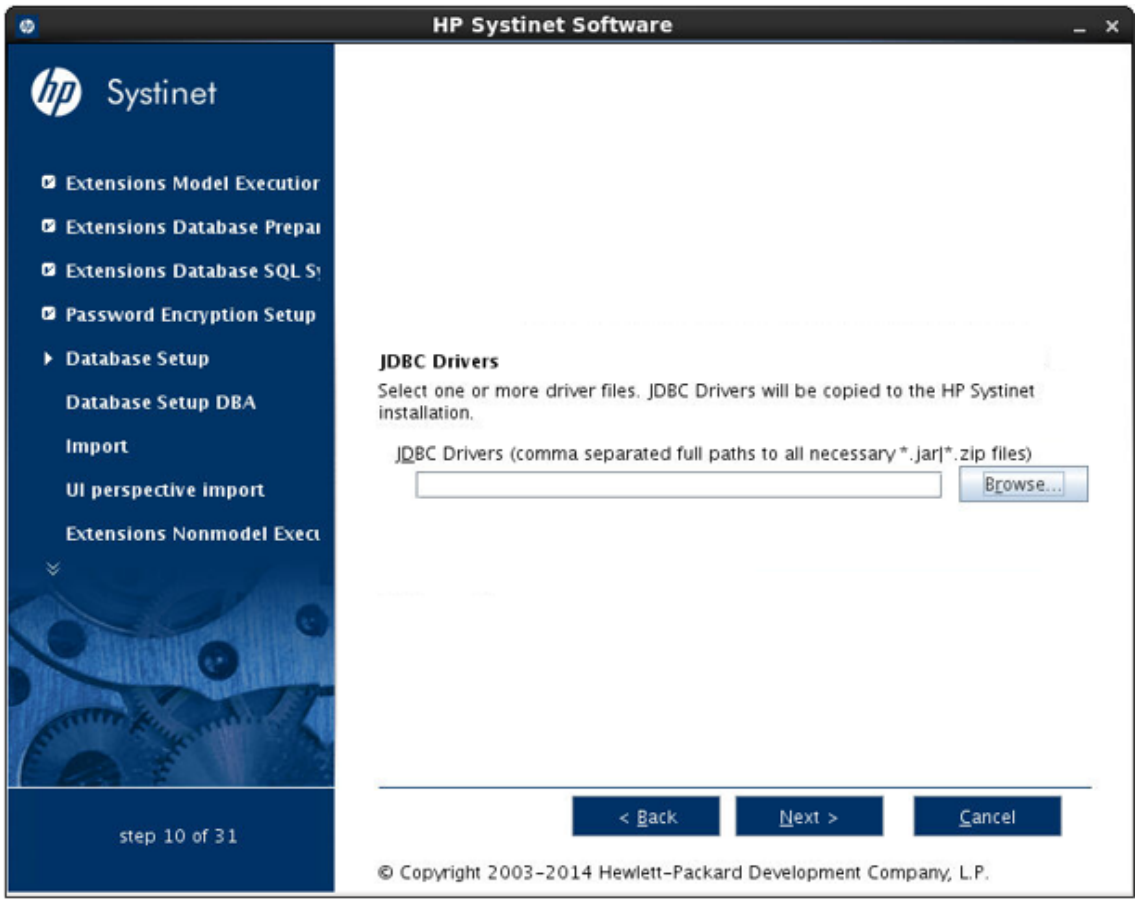
Parameter	Description	Notes
Full Connection String	Full connection string to the database.	Select this as option an alternative to inputting the individual connection parameters.
Existing Database User Name	User name and password to connect to the database.	—
Database User Password		



Click **Next** to continue to "Step 12 - JDBC Drivers" on page 59.

Step 12 - 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	11.2.0.3.0	ojdbc6.jar, orai18n.jar	11.2.0.3.0	oracle.jdbc.driver. OracleDriver
	12.1.0.1.0	ojdbc7.jar, orai18n.jar	12.1.0.1.0	

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

Supported MSSQL Drivers

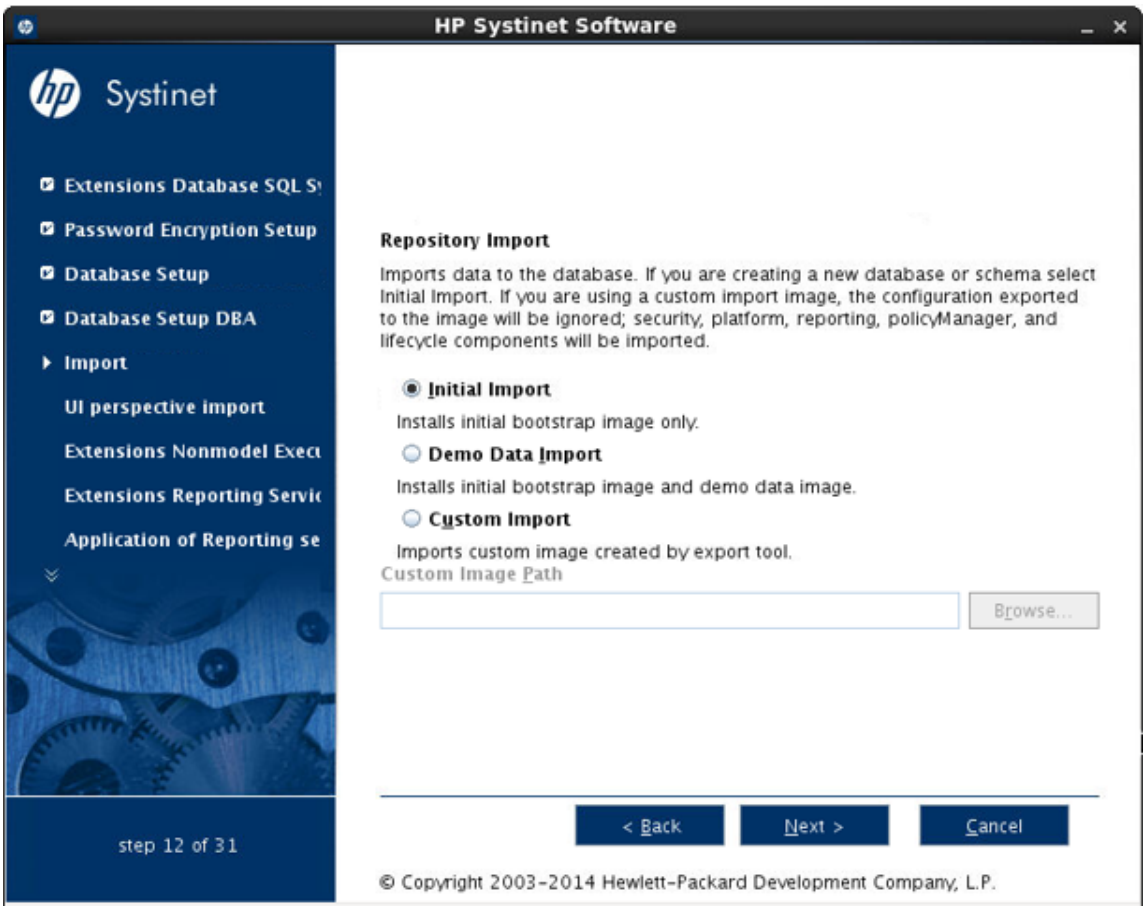
Database	DB Version	Driver Packages	Driver Version	Driver Class
Microsoft SQL Server	2012 SP1 2014	sqljdbc4.jar	4.0	com.microsoft.sqlserver.jdbc.SQLServerDriver

Click **Next** to validate the database parameters, the configuration tables, and the driver.

Continue to "Step 13 - Repository Import" on page 61.

Step 13 - Repository Import

In the Repository Import page, select the initial data you want to upload to Systinet.



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.

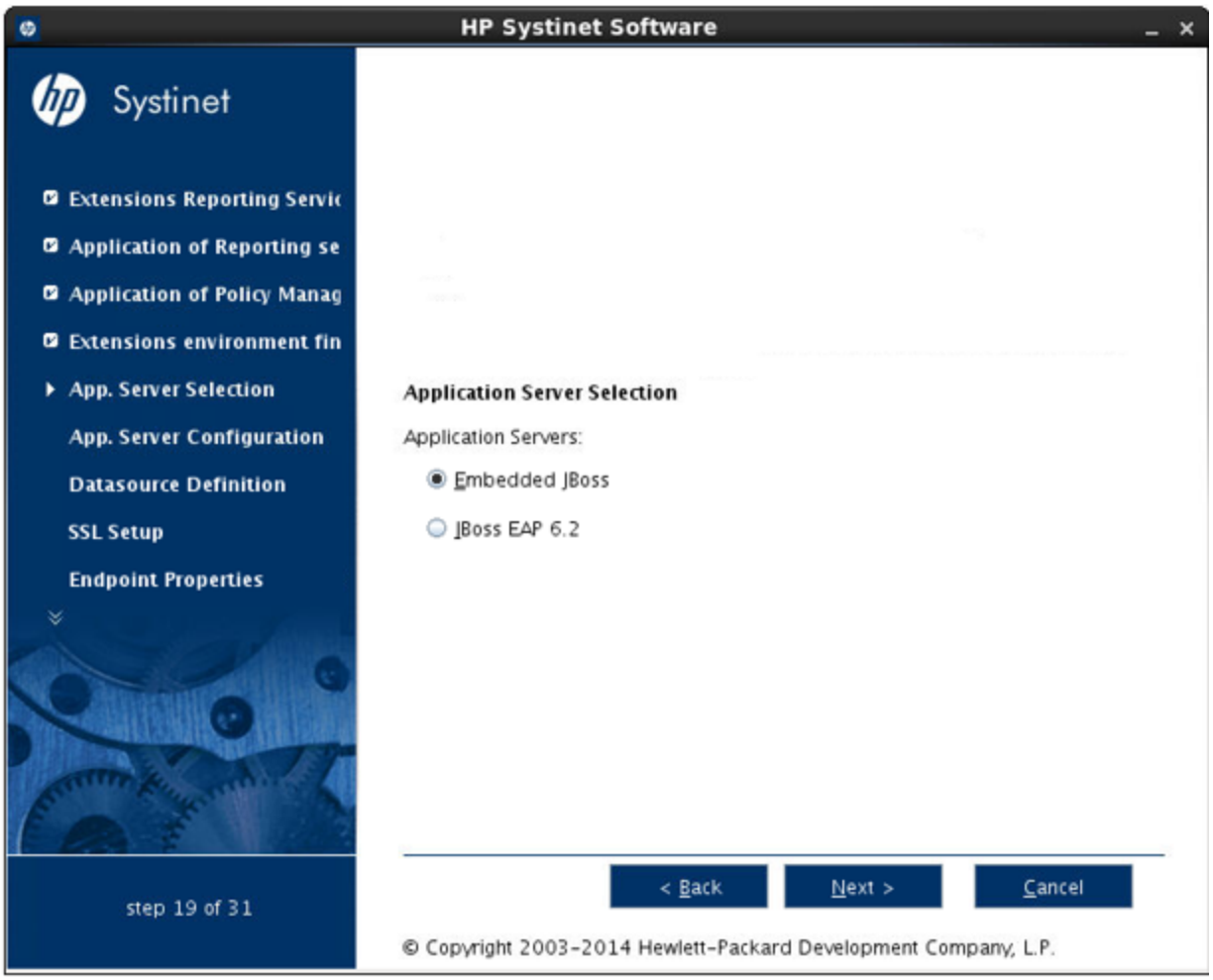
  Note: The compliance status of artifacts included in the demo data does not reflect their initial status as the import does not contain any policy validation data. Regenerate the validation data manually or allow the automatic validation task to regenerate it.

- Select **Custom Import**, and input or **Browse** to select a custom image.

Click **Next** to validate the data image and continue to "Step 14 - Application Server Selection" on the next page.

Step 14 - Application Server Selection

In the Application Server Selection page, select the application server to use.



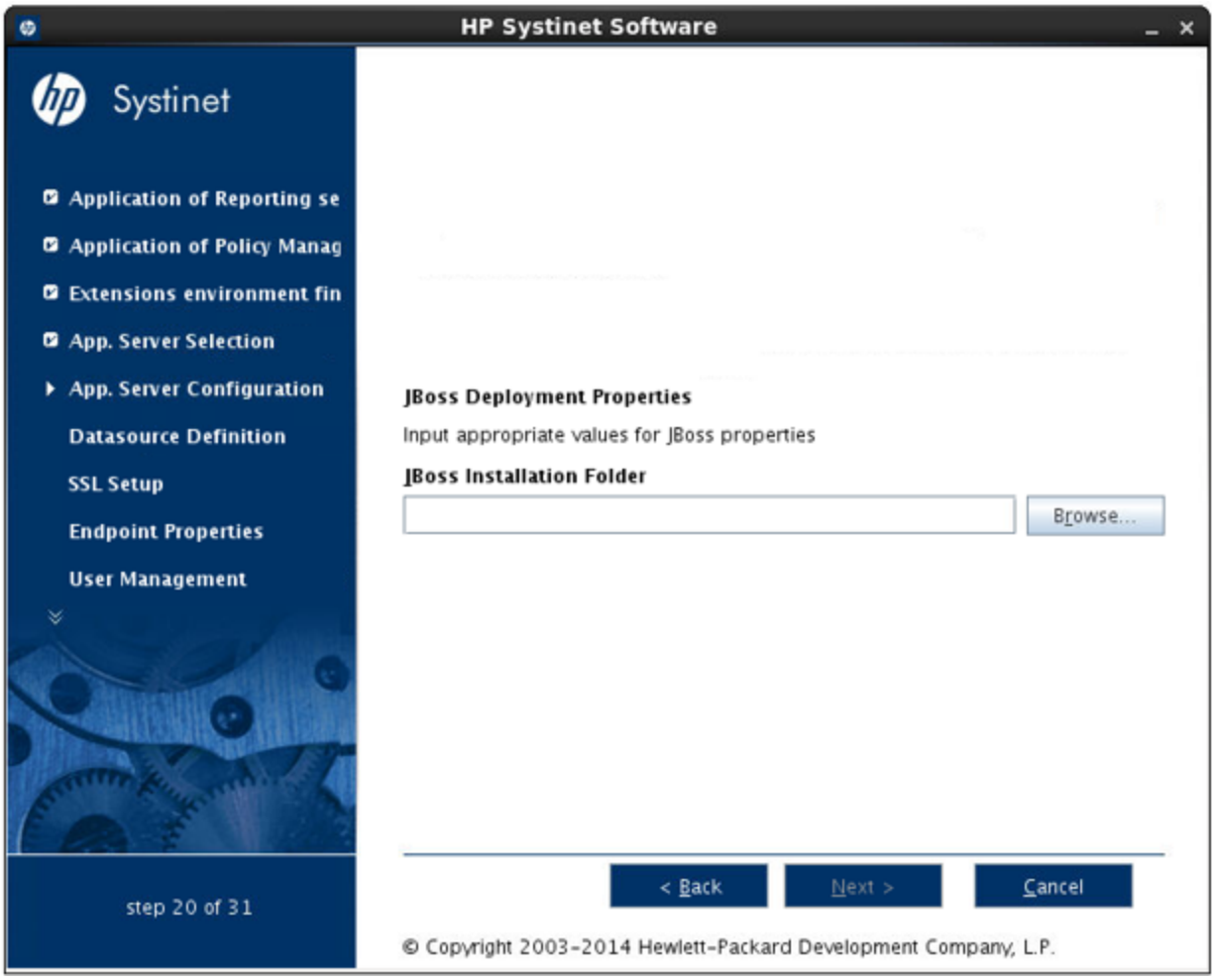
Select your application server type and click **Next**.

If you selected Embedded JBoss, continue to "Step 15 - Endpoint Properties" on page 64.

If you selected JBoss EAP 6.2, continue to "Application Server Configuration" below".

Application Server Configuration

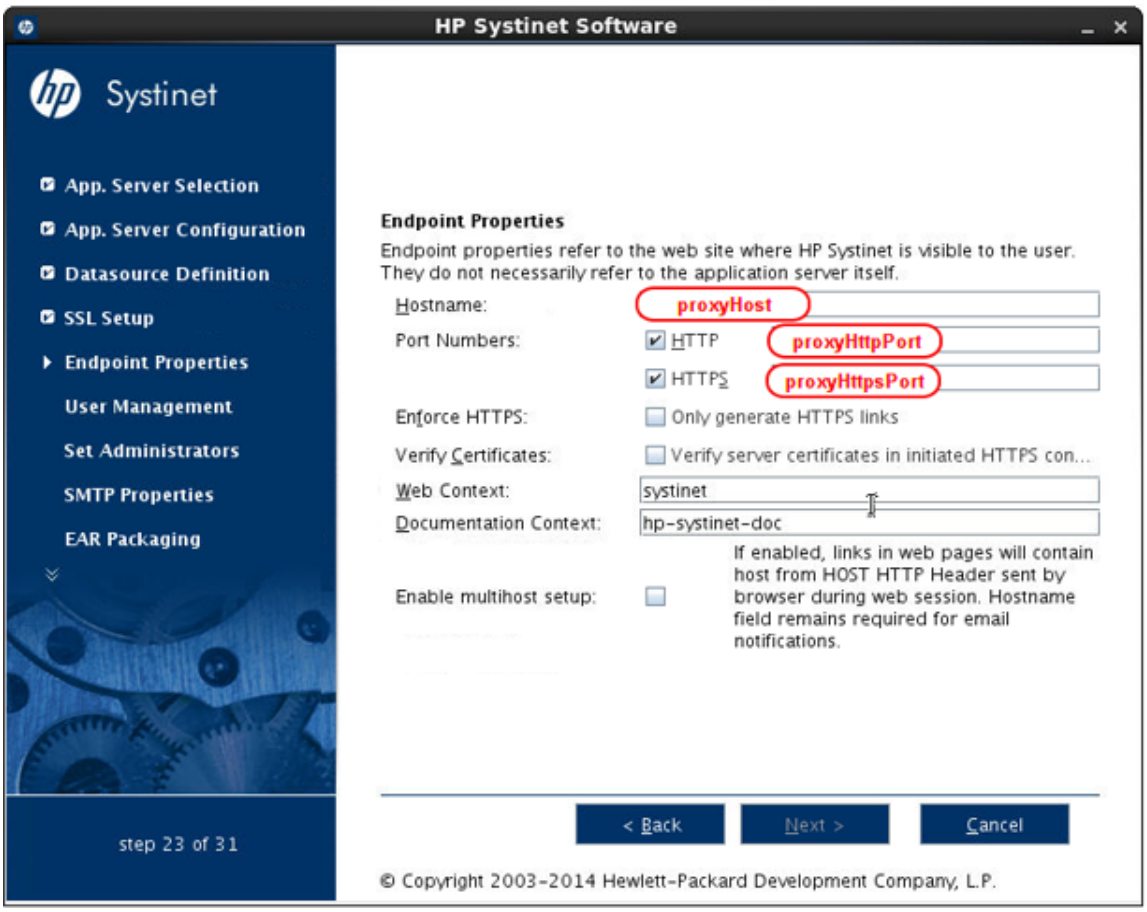
In the JBoss Deployment Properties page, input or click **Browse** to select the JBoss EAP 6.2 installation folder.



Click **Next** to extract and verify the JBoss application server, and continue to "Step 15 - Endpoint Properties" on page 64.

Step 15 - Endpoint Properties

In the Endpoint Properties page, specify the endpoint properties:



1. Enter the **Hostname**.
   - 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.
2. If necessary, change the default **Port Numbers**: HTTP = 8080, HTTPS = 8443. You select one or both port numbers.

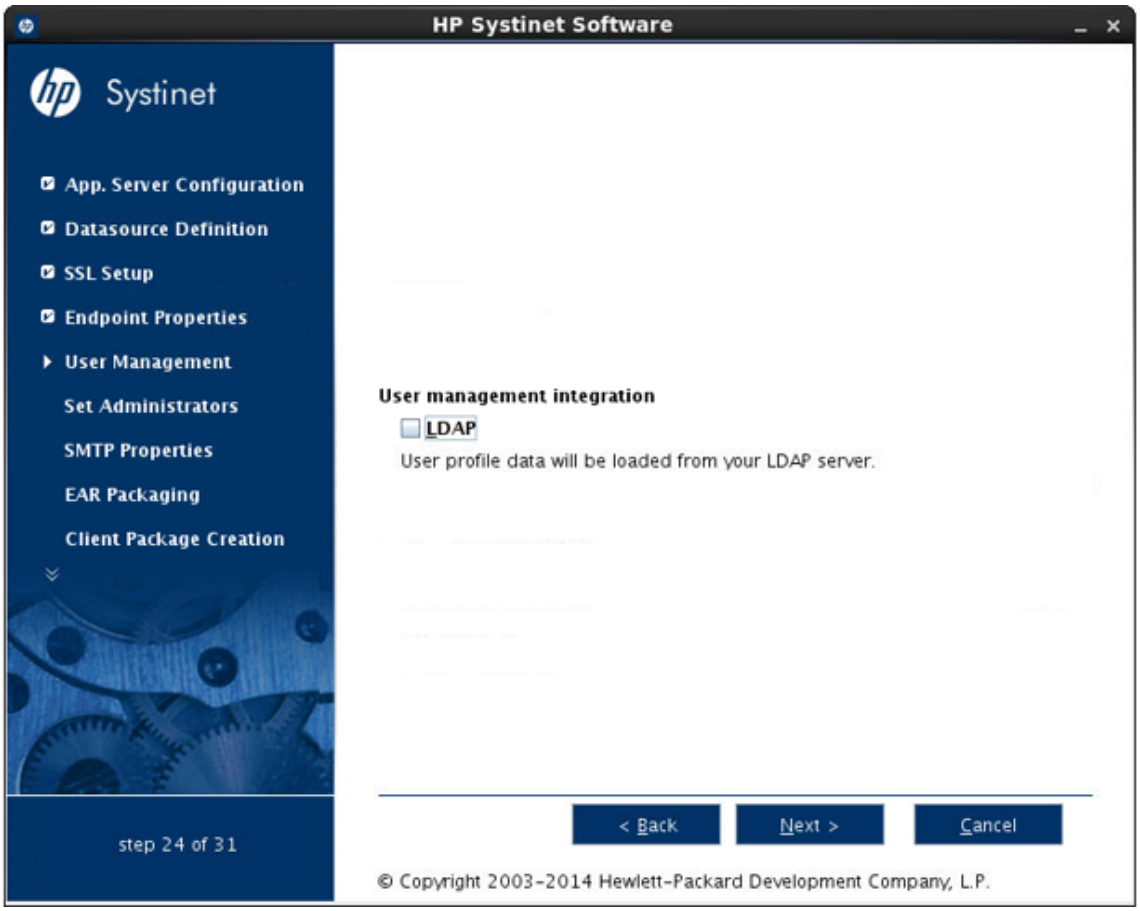
   Caution: Caution: If you change the port numbers from their default values, you must also change the application server configuration to use these ports.
3. (Optional) Select **Enforce HTTPS** if you want to generate only HTTPS links.

4. (Optional) Select **Verify Certificates** if you want the server certificates to be verified in initiated HTTPS connections.
5. Use the default **Web Context**: **systinet**.
6. Use the default **Documentation Context**: **hp-systinet-doc**.
7. (Optional) Select **Enable multihost setup** to use the specified **Hostname** in the HTTP header for all web pages during the web session.

Click **Next** to continue to "Step 16 - User Management Integration" below.

Step 16 - User Management Integration

In the User Management Integration page. select if you want to integrate with LDAP or store accounts in your database.

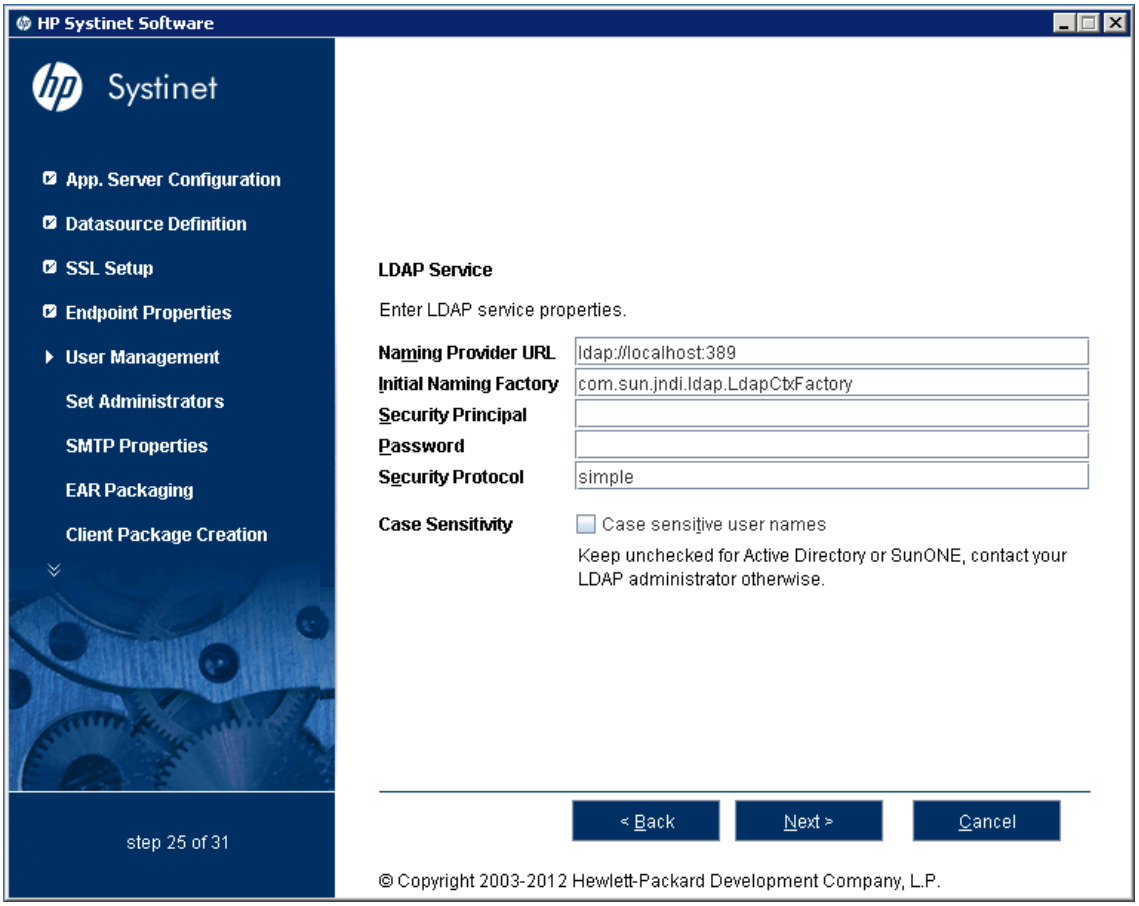


If you selected LDAP, click **Next** to continue to "LDAP Service Properties" on the facing page.

If you did not select LDAP, click **Next** to continue to "Step 17 - System Email Configuration" on page 72.

LDAP Service Properties

In the LDAP Service page, set the LDAP connection parameters, credentials, and case sensitivity.



LDAP Service Properties

Property	Description
Naming Provider URL	URL on which LDAP is installed (for example: ldap://localhost:389).
Initial Naming Factory	Keep the default.
Security Principal	Principal to login to LDAP (for example: uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot).
Password	Username password.

LDAP Service Properties, continued

Property	Description
Security Protocol	Keep the default.
Case Sensitivity	When checked, sets all user names to be case sensitive. The default for Systinet logins is case-insensitive. If you 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*. **Note:** You must ensure that the application server uses matching case-sensitive or -insensitive authentication.

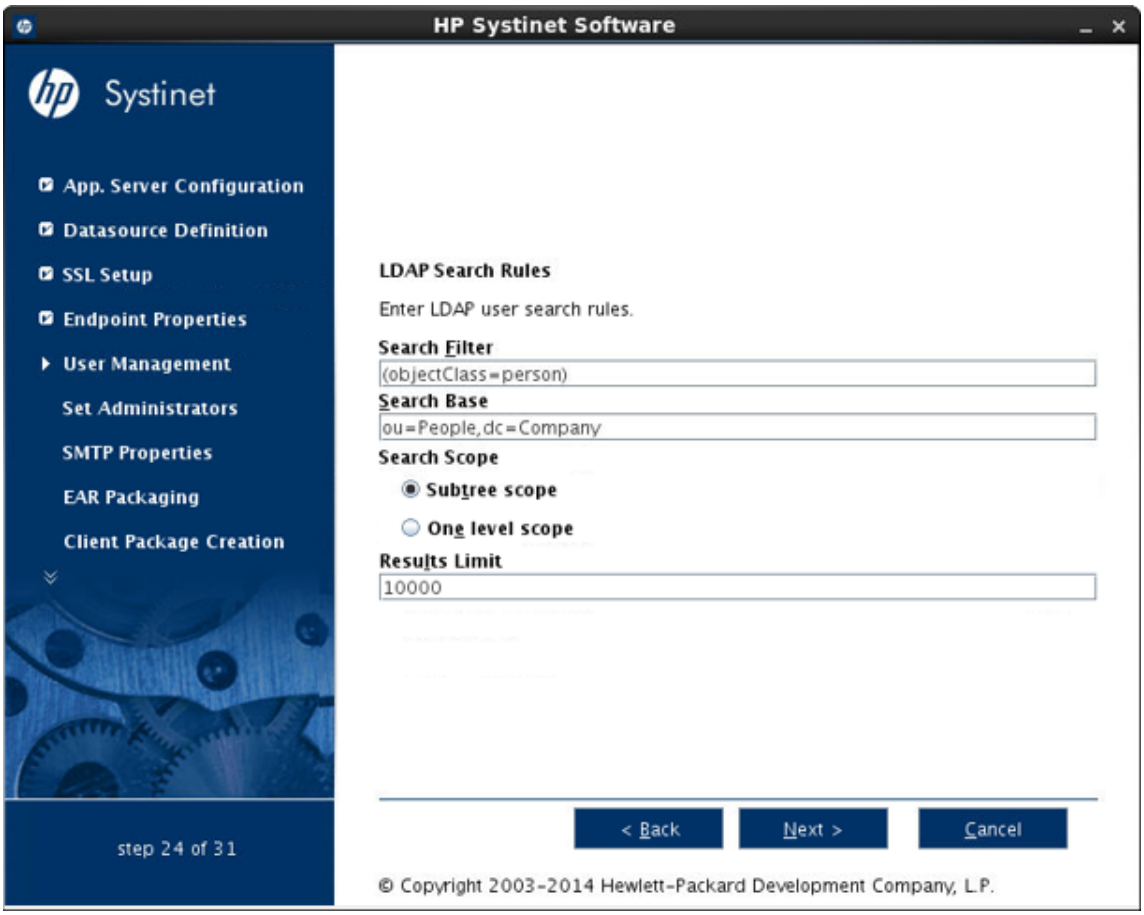
Click **Next** to continue to "LDAP Search Rules" below.

LDAP Search Rules

In the LDAP Search Rules page enter the following parameters:

LDAP Search Rules Properties

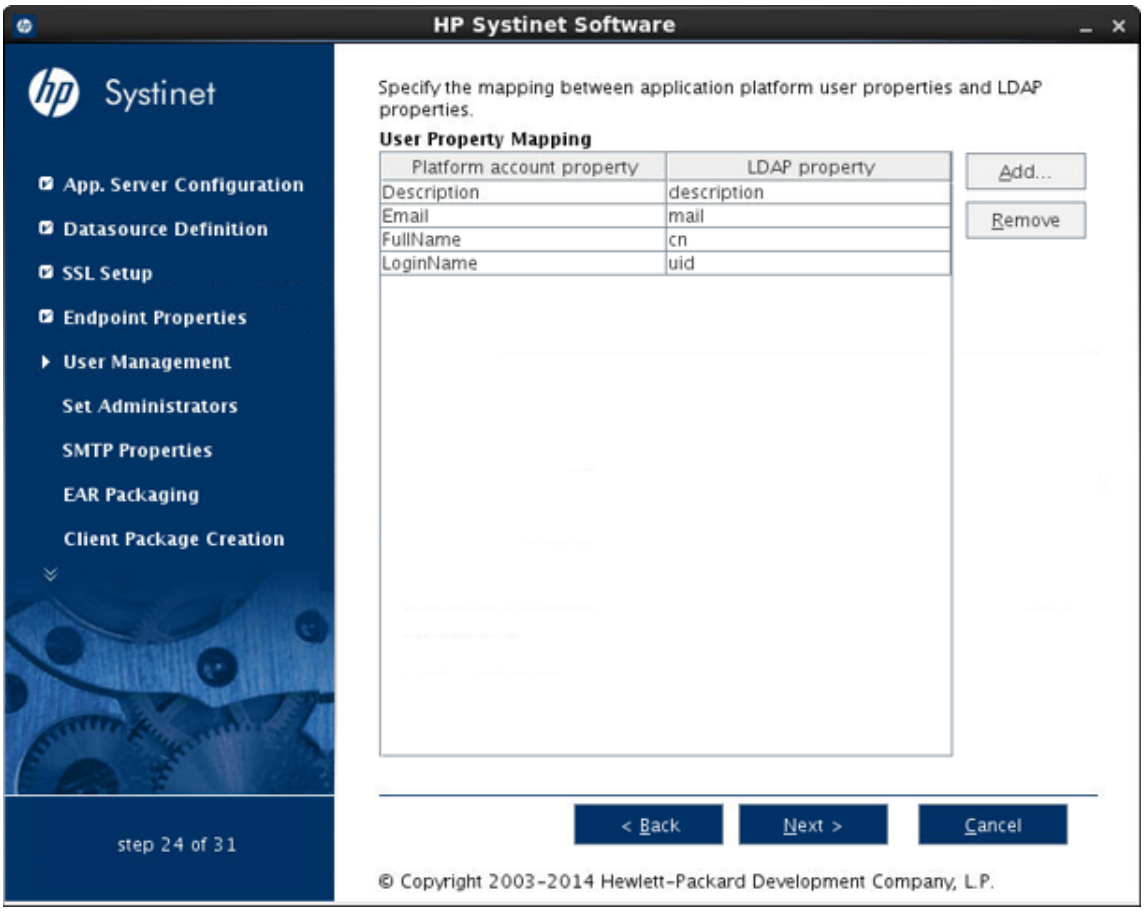
Property	Description
Search Filter	The notation of the search filter conforms to the LDAP search notation. You can specify the LDAP node property that matches the user account or group.
Search Base	LDAP is searched from this base according to the Search Scope settings.
Search Scope	• One-level Scope: 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 continue to "LDAP User Properties Mapping" below.

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.

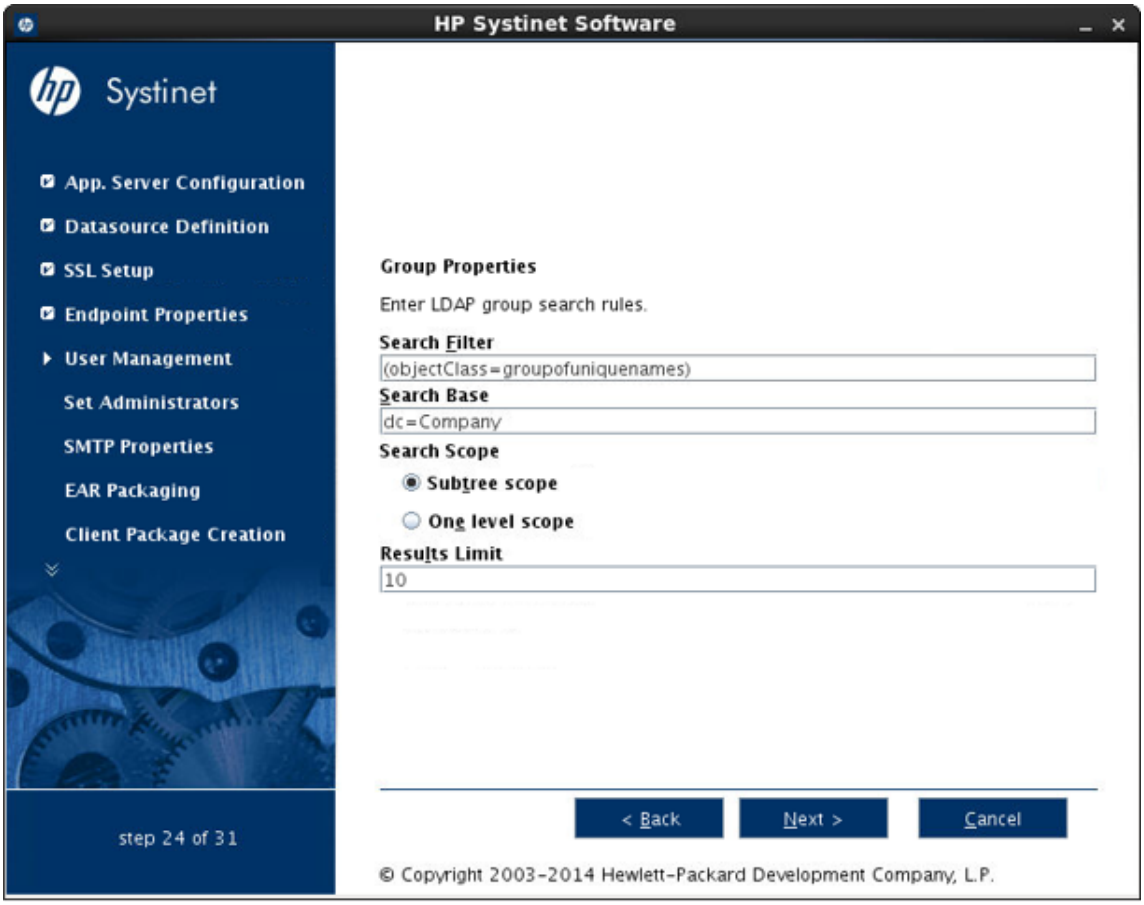
Click **Next** to continue to "LDAP Group Search Rules" on the facing page.

LDAP Group Search Rules

In the Group Properties page, enter the following parameters:

LDAP Search Rules Properties

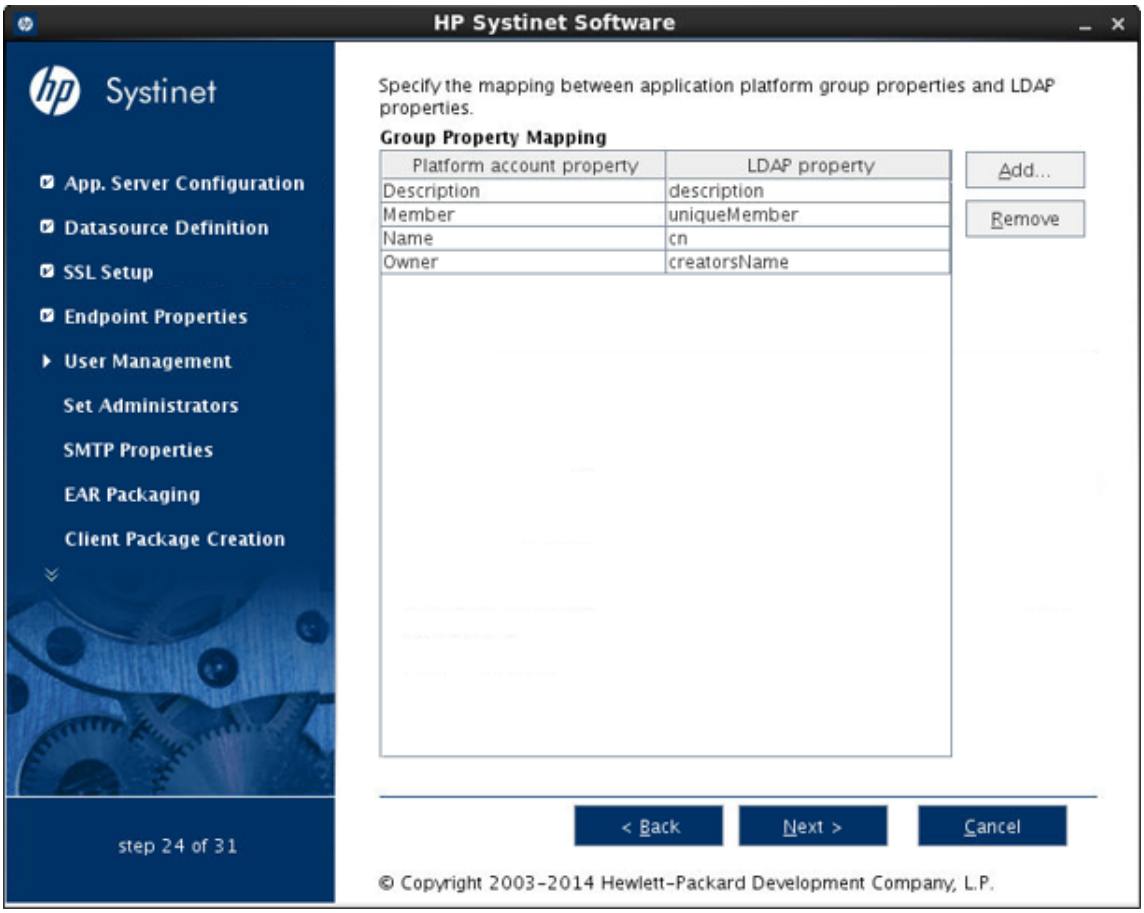
Property	Description
Search Filter	The notation of the search filter conforms to the LDAP search notation. You can specify the LDAP node property that matches the user account or group.
Search Base	LDAP is searched from this base according to the Search Scope settings.
Search Scope	• One-level Scope: 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 continue to "LDAP Group Properties Mapping" below.

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:

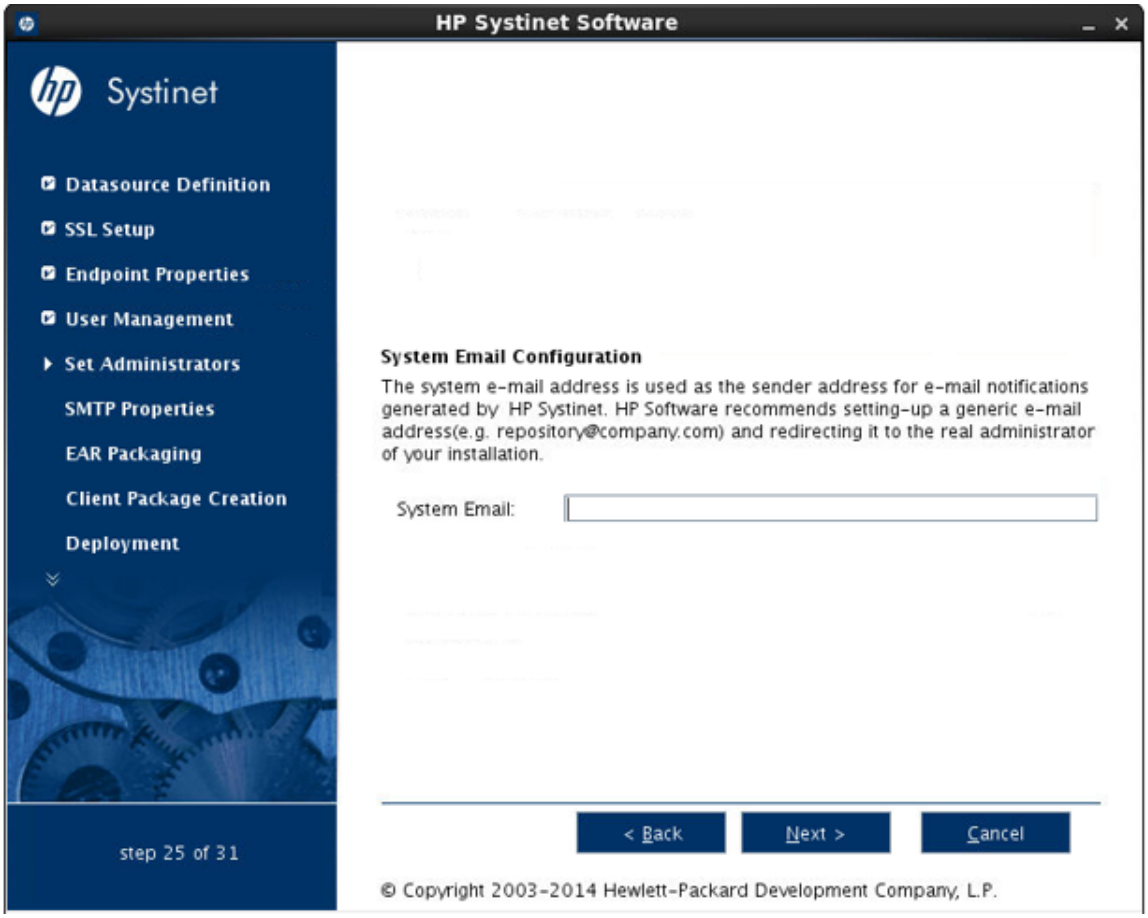
```
java.lang.string Owner
java.lang.String Description
```

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 continue to "Step 17 - System Email Configuration" on page 72.

Step 17 - System Email Configuration

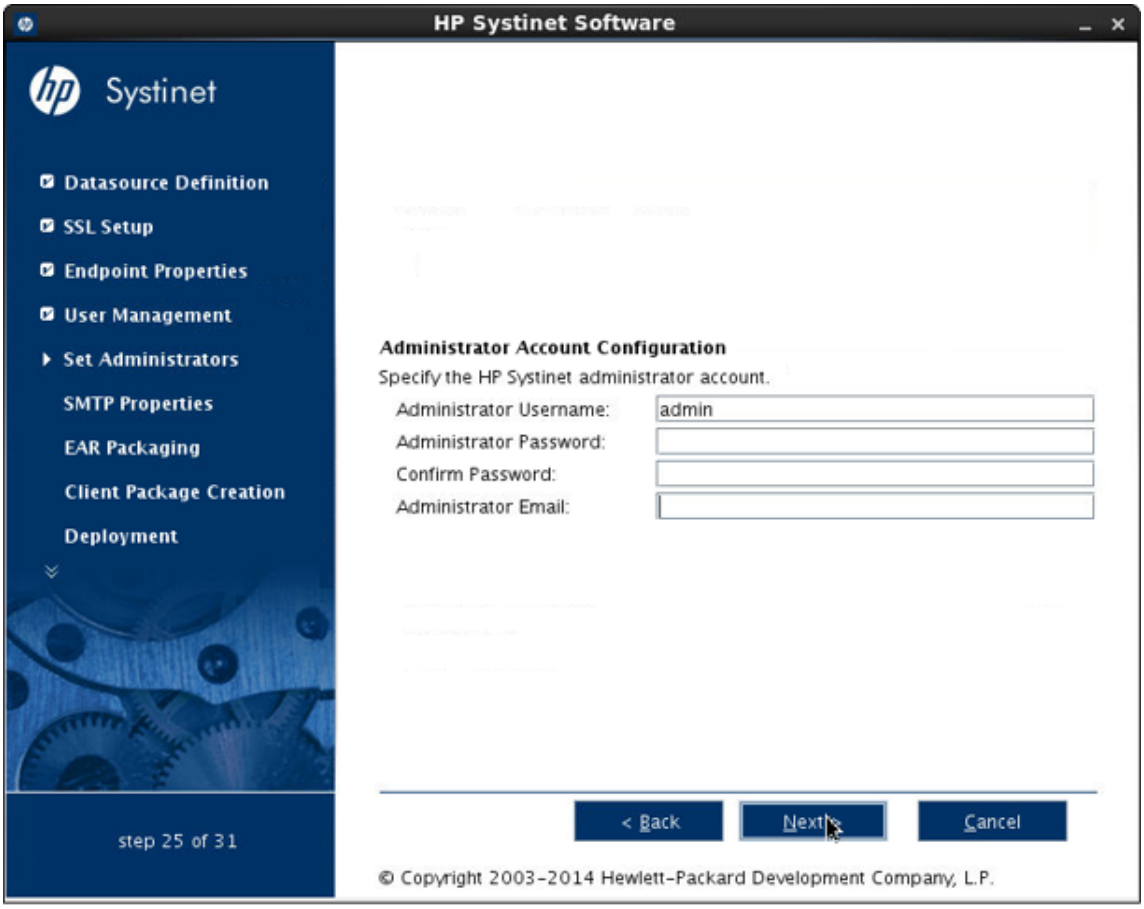
Enter the system mail account to be used as the source of automatic notification mails and system messages.



Click **Next** to continue to "Step 18 - Administrator Account Configuration" on page 73.

Step 18 - Administrator Account Configuration

In the Administrator Account Configuration page, set the administrator credentials.



1. Enter the **Administrator Username**.

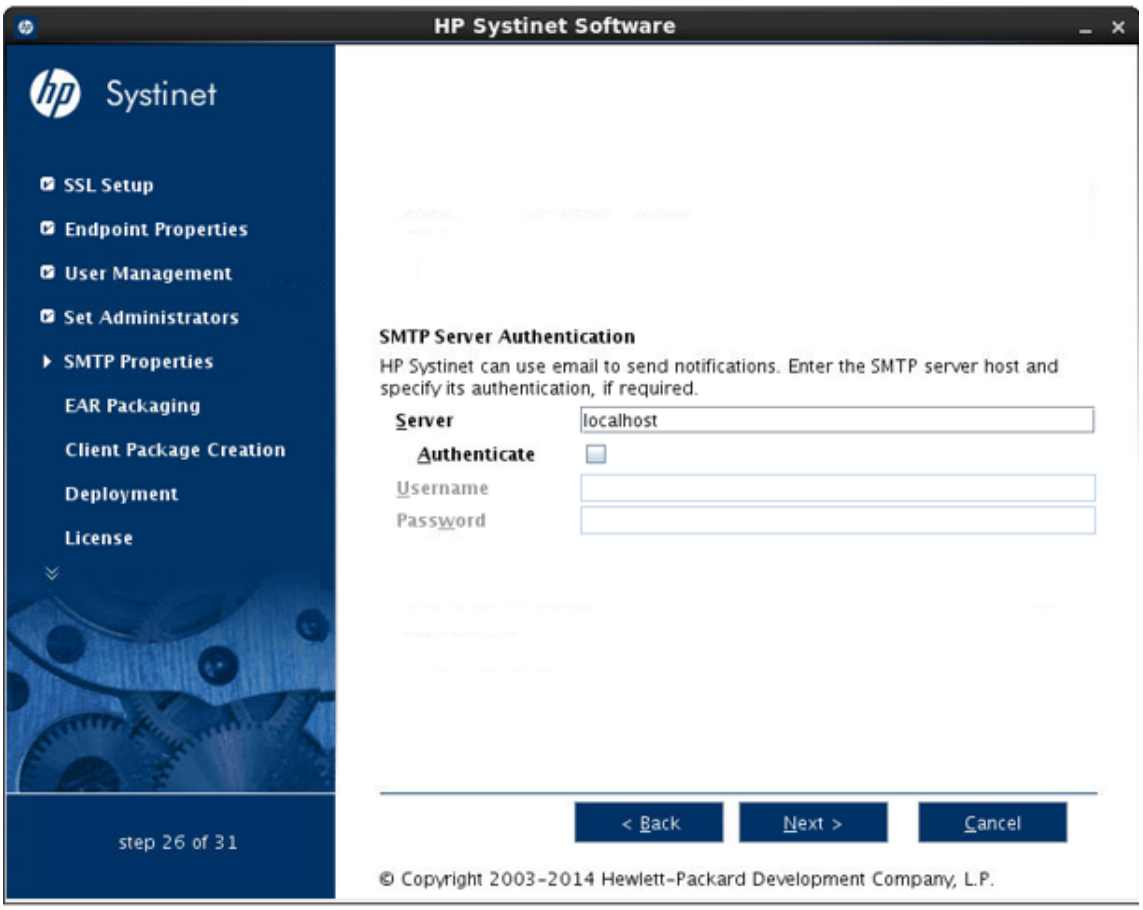
   Note: The administrator login name must be valid for the selected application server instance. The user with the specified name becomes an HP Systinet administrator. For JBoss the specified administrator account is automatically created.

2. Enter the **Administrator Password**.
3. **Confirm** the Administrator **Password**.
4. Enter the **Administrator Email**.

Click **Next** to continue to "Step 19 - SMTP Server Authentication" on page 74.

Step 19 - SMTP Server Authentication

If you want mail notifications, set the mail server host.

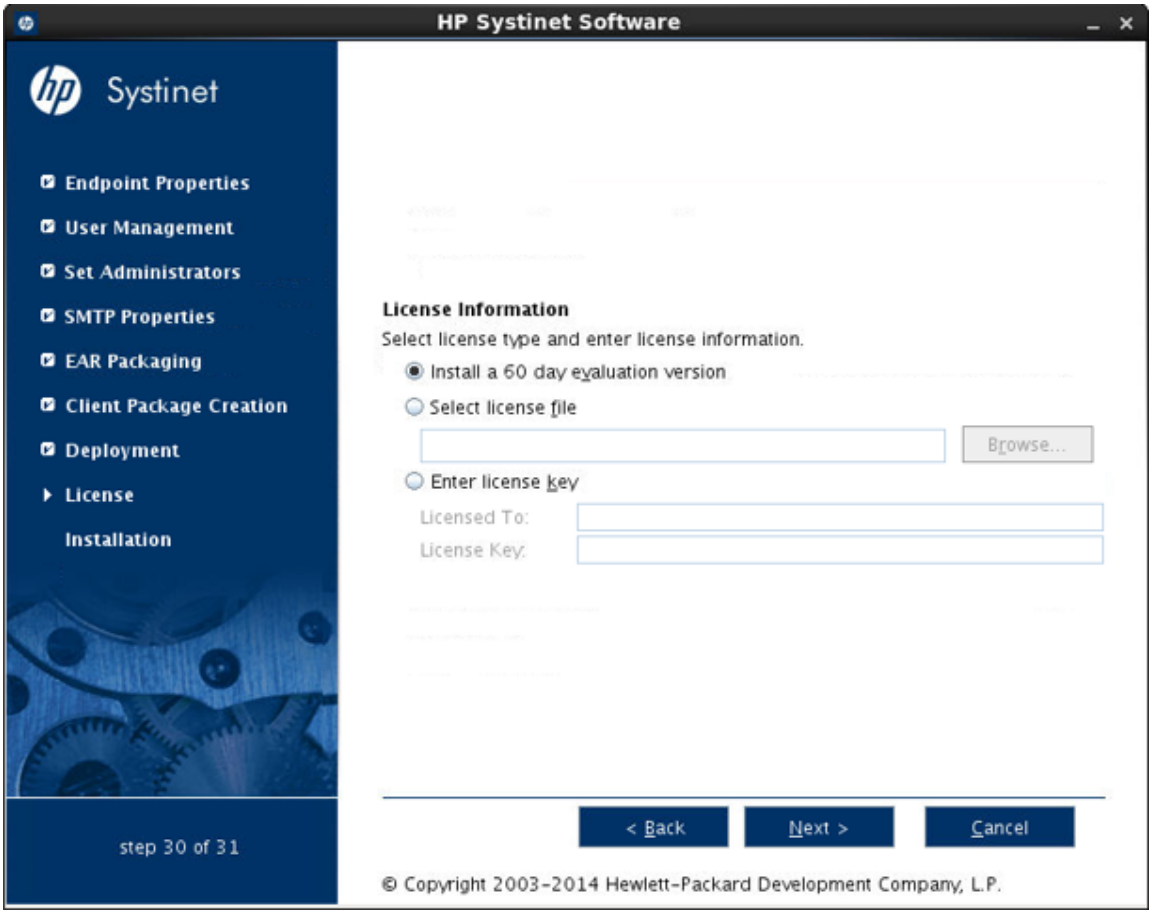


To authenticate, select **Authenticate** and enter the SMTP server credentials.

Click **Next** to create the client package and continue to "Step 20 - License Information" on page 75.

Step 20 - License Information

In the License Information page set which license to use.



Do one of the following:

- Select **Install a 60 day evaluation version**.
- Select **Select license key** and browse the lince license file.
- Select **Enter license key** and type the license details provided by your sales representative.

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 "Step 21 - Confirmation" on the next page.

Step 21 - Confirmation

In the Confirmation page, click **Next** to start the installation process.

Continue to "Step 22 - Installation Progress" below.

Step 22 - 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.

Click **Finish** to exit the Installation Wizard.

Completing the HP Systinet 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" below
- "Finish Decoupled Database Installation" on the next page
- "Create an Archive for JDKless Deployment" on the next page

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 Systinet extraction folder and execute the installation command:

   java -jar hp-systinet-10.00.jar -u deployment.properties -i /opt/hp/systinet/10.00
3. Archive the clean deployment:

   tar -cjf hp-systinet-10.00-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" below
- "Set Up Role Mapping" on the next page
- "Set Up SiteMinder Integration" on page 80
- "Deploying Systinet to JBoss" on page 80
- "Enable Full-Text Search in MSSQL" on page 83
- "Enable Full-Text Search in Oracle" on page 84
- "Configure LDAP over SSL/TLS" on page 86
- "Log4j Configuration" on page 87
- "Deploy to the JDKless Environment" on page 90

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)

Authentication Methods, continued

Authentication Method	URL Patterns
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*)
	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.

Embedded JBoss7 provides a single-sign-on (SSO) solution for this situation. SSO is set up during the 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.

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:

- "Modify JBoss Logging" on the next page
- "Enable Non-Latin HTTP Parameters in JBoss" on page 82

- "Redeploy the EAR File to JBoss" on the facing page

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.

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/standalone/configuration/standalone-full.xml` with a text editor.
2. Edit the child element of the `subsystem` element `<subsystemxmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host"native="true">` as follows:

```
<sso domain="localhost" reauthenticate="false"/>
```

3. In the jboss-web.xml file, declare the Valve that will be used to handle SSO. Every request goes through this valve and it acts according to what you specified in re-authenticate flag.

```
<jboss-web>
  <security-domain>sso</security-domain>
  <valve>
    <class-name>org.apache.catalina.authenticator.SingleSignOn</class-name>
  </valve>
</jboss-web>
```

4. Save the changes and restart the application server.

For more details about SSO in JBoss, see Configuring Single Signon on JBoss AS 7.

Modify JBoss Logging

By default, Systinet logs messages to the hosting application server log files. When Systinet is deployed to JBoss, log messages are sent to the following file:

`SYSTINET_HOME\log\server.log`

Note: `JBOSS_DEPLOY` is the deployment directory on the JBoss application server where Systinet is deployed.

The message threshold level, by default, is *`INFO`*.

To Modify the Log File Parameters:

1. Stop the Systinet server.
2. Save `JBOSS_HOME\standalone\configuration\logging.properties` to a recoverable backup location in case you need it later.
3. Open `JBOSS_HOME\standalone\configuration\logging.properties` with a text editor.
4. Edit the logging level and filename.
5. Save `JBOSS_HOME\standalone\configuration\logging.properties`.
6. Start the 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/standalone/configuration/standalone-full.xml` with a text editor.
2. In all `connector` elements defined in `standalone-full.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.

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 POP
ULATION
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 b
e 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 ctxs
ys.context parameters
  ('filter ctxsys.null_filter section group CTXSYS.NULL_SECTION_GROUP STOPLIST M
yStoplist
    SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL') ;
CREATE INDEX idx_ry_resource_data on ry_resource(data) indextype is ctxsys.conte
xt parameters
  ('filter ctxsys.null_filter section group CTXSYS.NULL_SECTION_GROUP STOPLIST M
yStoplist
    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 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 Systinet with an LDAP account provider.

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 Systinet. It informs you of a hostname verification error. The stacktrace contains the hostname that you must use.

- **LDAP over SSL With Mutual Authentication**

  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

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 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.

  Systinet tools execute a java command with a *`-Dlog4j.configuration`* option that points to a `SYSTINET_HOME/conf/log4j.config`.

  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/standalone/configuration/jboss-log4j.xml`

  The audit log file is created in the `JBOSS_HOME/standalone/log` directory. The Application log is a part of the default JBoss log output (the console and also the `JBOSS_HOME/standalone/log/server.log`) file.

If you are not sure about the logging configuration, do one of the following:

- Use the 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 Systinet is shown in the "Log4j Configuration File".

Note: 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://logging.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{au
dit.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.

   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 Systinet creates the log files in the following location:

   `JBOSS_HOME/standalone/log`

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

Systinet also uses an audit log to contain events triggered by Systinet functionality. 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:

   ./10.00/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 Systinet installation folder (including JBoss or WebLogic domain).

   tar -cjf hp-systinet-10.00-deployment-01.tar.bz2 /opt/hp/systinet

In the Target Environment, extract the archive:

tar -jxvf hp-systinet-10.00-deployment-01.tar.bz2 /opt/hp/systinet

Note: 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 Systinet

If you have an installation of HP Systinet 4.x, you can upgrade to Systinet 10.00.

Upgrade from 4.x consists of the following parts:

- "Apply Custom Extensions from HP Systinet 4.x" below
- "Migrate Data from HP Systinet 4.x" on page 93

Apply Custom Extensions from HP Systinet 4.x

Systinet 10.00 contains significant changes to the architecture model. If you have customized extensions, apply them to Systinet 10.00.

To Apply Custom Assertion Extensions:

1. Install Systinet Workbench 10.00.
2. Create a new assertion project based on the old extension in Assertion Editor.
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.
5. Apply the extensions to Systinet 10.00.

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), 4.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 Systinet Workbench 10.00.
2. Create a new taxonomy project based on the old extension in Taxonomy Editor.
3. The 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.
5. Apply the extensions to Systinet 10.00.

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 Systinet 10.00. In the event of a conflict the old system taxonomy takes precedence.

To Apply Custom Model Extensions:

1. Install Systinet Workbench 10.00.

   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 10.00 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.

   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 the Customization Editor.
5. Apply the extensions to Systinet 10.00.

For details, see the *Customization Editor Guide*.

Systinet features a redesigned UI, so UI customizations for the 4.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 Systinet Workbench 10.00.
2. Create a new report project based on the old extension in Report Editor.
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.
5. Apply the extensions to Systinet 10.00.

For details, see the *Report Editor Guide*.

Note: Report categorization does not exist in Systinet 10.00. All custom reports from Report Editor 10.00 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 Systinet 4.x

Systinet 10.00 is not backwards compatible with Systinet 4.x data. You can import data images from Systinet 4.x into Systinet 10.00 using a migration tool provided in the installation.

Note: Systinet 10.00 migrate tool supports Systinet 4.03 and 4.10 only. If you are migrating from a version of Systinet earlier than 4.03 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 Systinet 4.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 Systinet 4.x to 10.00:

1. In Systinet 4.x, execute the export command:

   SYSTINET_HOME/bin/export -image *dataimage.zip*

   For details, see the "Export Tool" section of the *Systinet 4.x Administration Guide*.

2. In Systinet 10.00, execute the data migration command:

   SYSTINET_HOME/bin/migrate --image *dataimage.zip* --output *migratedimage.zip*

   Note: Execute **migrate --help** to view the available options for the migrate tool. If you use password encryption, use the passphrase setup for Systinet 10.00 if it is different from that of Systinet 4.x.

   The migrate tool creates an image folder matching the output of the export tool ready for import to Systinet 10.00. 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 Systinet 4.x" on page 91 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 10.00, execute the import command line:

   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 4.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:

- **Model Change**
  SDM is extensively changed from 4.x to 10.00. For details, see “Model Changes” in the *Reference Guide*.
- **Lifecycle-Based Contracts**
  Contract states are extensively re-designed to employ the standard Lifecycle feature. For details, see “Contract Management” in the *User Guide*.
- **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 if they exist.

- **UI Customizations**

  UI customizations from Systinet 4.x are migrated along with data image. Use the UI customization features in the Administration tab in Systinet 10.00 to verify and change these customizations after data migration is complete. For details, see "UI Customization" in the *Administration Guide*.

The following data from Systinet 4.x are not migrated to 10.00:

- **L7 Gateways and IBM XI50 Devices** - Due to the new implementation of Runtime Gateway Interoperability Framework (formerly iPEP), L7 Gateway and IBM XI50 Device artifacts are no longer compatible and will be dropped after migration. Administrator is advised to deploy out-of-the-box remote adapters for Layer7 and Datapower, then re-enter connection information. For details, see "Adding RGIF Servers" in the *User Guide*.
- **Rebranding** - Rebranding is a part of server installation. To rebrand the new Systinet 10.00 installation, see "Rebranding Systinet" in the *Administration Guide*.

Chapter 9

Starting and Configuring HP Systinet

After deployment, you should start Systinet and apply any required final configuration.

For details, see the following sections:

- "Start Systinet in JBoss" below
- "Enable Full-Text Search in Systinet" below
- "Turn Off Systinet Self-Test" below

Start Systinet in JBoss

- Execute the following command:

  SYSTINET_HOME/bin/serverstart

- For some production environments, `serverstart` may not be appropriate. Execute the following command instead:

  JBOSS_HOME/bin/standalone

Enable Full-Text Search in Systinet

Full-text search must also be enabled in the Systinet UI.

> **Note:** Oracle 11g does not support full-text searching of Microsoft 2010 files. To use this capability, you need to upgrade to Oracle 12c.

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`.