Systinet

Software Version: 10.04
Windows and Linux Operating Systems

Installation and Configuration Guide

Document Release Date: July 2017
Software Release Date: July 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

© 2003 - 2017 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** 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 HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com/.

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Install and Configure

Installation guide provides information about supported hardware and software, prerequisites, and steps to successfully install and run Installation and Configuration Guide 10.04.

Following are the steps required to set up an environment and configure HPE Systinet:

- "Compatibility" on page 7 - Understand the suitability and usability.
- "Prerequisites and Supported Platforms" on page 9 - Design your environment for HPE Systinet.
- "Preparing Databases" on page 15 - Set up and configure your database for HPE Systinet.
- "Preparing LDAP and CA Single Sign On" on page 25 - Set up LDAP and CA Single Sign On for HPE Systinet.
- "HTTP Proxy Requirement" on page 28 - Install HTTP Proxy for HPE Systinet.
- "Using the HPE Systinet Installer Wizard " on page 33 - Steps to install HPE Systinet using installer wizard.
- "Advanced HPE Systinet Installation" on page 70 - Additional install command options.
- "Configuration" on page 72 - Configure your environments and deploy HPE Systinet.
- "Applying Custom Extensions " on page 80 - Applying customized extensions for HPE Systinet.
- "Starting HPE Systinet" on page 82 - Start and perform UI-based final configuration for HPE Systinet.
- "Setting JBOSS Clustering" on page 84 - Configuring Systinet in JBoss cluster environment.

Chapter 2: Compatibility

This section covers the following topics:

Languages

The user interface of HPE Systinet uses the English language out-of-the-box. Systinet allows data input in local languages.

Internationalization Variances

This version of Systinet runs on all locales described in this document. There are no known variances.

Virtualization Products

Transparent Technology and Virtualization Support

In recent years, a number of “transparent” hardware and software technologies and virtualization solutions (such as Citrix, Microsoft Cluster Software, and VMware) have become increasingly prevalent. These solutions operate in the technology layers adjacent to the operating systems or, in some cases, as extensions of the operating systems. Similarly, database solutions offer transparent components as supported elements.

HPE supports Systinet running on operating systems and databases on particular platforms, not specific hardware and software configurations. HPE will support Systinet customers who run HPE software products on supported operating systems and databases, irrespective of whether they are running transparent or virtualization solutions in their environment. HPE does not support these transparent or virtualization technologies directly. Since the providers of these technologies support a set of certified operating systems and hardware, the customer and the providers of these technologies will be responsible for any interactions or issues that arise due to the usage of hardware or operating system.

HPE will not require customers to re-create and troubleshoot every issue in a non-transparent environment; however, HPE does reserve the right to request that its customers diagnose certain issues in a native certified operating system environment without the transparent technology. HPE will only make this request when there is reason to believe that the environment is a contributing factor to the reported issue.

While Systinet is expected to function properly with these transparent technologies in place, there may be performance implications, which can invalidate HPE's typical sizing recommendations. Analysis must be performed within the context of the specific application to be hosted in a virtual environment to minimize potential resource overload, which can have significant impact on performance and scalability under peak load.

Chapter 3: Prerequisites and Supported Platforms

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

The following sections describe the requirements and options available:

Design Your Deployment

- **Development**

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

  HPE Systinet ships with an embedded application server. Before you run the HPE Systinet installer, you must setup database and install and configure Java. Oracle XE or MSSQL Express and Oracle JDK 1.8 are satisfactory prerequisites for HPE Systinet.

Use the HPE Systinet installation wizard to install the product following the default settings. Server configuration for the application server is handled within this wizard and in the serverstart and serverstop scripts.

- **Trial Version**

  If you want to evaluate HPE 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 https://www.hpe.com/us/. Select **Products > Software > Software A-Z > Free & Trial Software**. Search for the HPE Systinet Virtual Appliance related downloads and click the **Download** link.

- **Production**

  Deploying HPE Systinet for use in a production environment is flexible enough 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 design your HPE Systinet production environment, you may need additional configuration options that are available in the HPE Systinet installer wizard as well as in the configuration files.

  HPE 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 HPE Live Network or the advanced documentation at the HPE Support website.

  For information on silent installation (command line), run the jar file using the `-help` option:

  ```
  java -jar hpe-systinet-10.04.jar -help
  ```

Prerequisites - Hardware

HPE recommends the following minimum hardware configuration for each physical node of a distributed production environment:

- Intel Xeon E processor family, 8 cores, 32 GB RAM, 40 GB free disk space, 1Gbps network card.
- Network bandwidth of 1 Gb/sec or higher.

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

- Intel Core i7 processor, 16 GB RAM, 40 GB free disk space, 1Gbps network card.
- Network bandwidth of 100Mb/sec or higher.

Warning: SPARC machines are not suitable for HPE Systinet deployments.

Example:

It is possible to evaluate HPE 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) 16 GB
- 500GB HDD Intel(R) 7 Series Chipset Family SATA
- Intel(R) 82579LM Gigabit Network

Prerequisites - JDK Software

HPE Systinet supports the following JDK:

- Oracle (Sun) JDK 1.8 64-bit
- OpenJDK 1.8 64-bit (Linux OS only)

> **Note:** HPE Systinet supports OpenJDK 1.8 in Development Mode only.

> **Caution:** As best practice for security and avoid risk, HPE recommends using the latest version of Oracle JDK.
>
> HPE also 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 HPE Systinet.

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 1.8 then proceed with installation.
   - If JAVA_HOME does not point to JDK 1.8 then reset the JAVA_HOME environment variable to a valid JDK 1.8.

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

Supported Database Types

HPE Systinet supports the following databases:

- Oracle 12c
- Microsoft SQL Server 2014
- PostgreSQL 9.5

> **Note:** HPE Systinet supports PostgreSQL database in Development Mode only.

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

Supported Database Drivers

Database	DB Version	Driver Packages	Driver Version	Driver Class
Oracle Database	12.1.0.1.0	ojdbc7.jar. orai18n.jar	12.1.0.1.0	oracle.jdbc.driver.OracleDriver
Microsoft SQL Server	2014	sqljdbc4.jar	4.0	com.microsoft.sqlserver.jdbc.SQLServerDriver
PostgreSQL	9.5	postgresql-9.4.1208.jar	9.4-1208	org.postgresql.Driver

> **Tip:** For optimal performance, HPE recommends running a dedicated server for Systinet database. Hosting Systinet database together with other application databases on the same server also impacts the performance of Systinet significantly.

Supported Application Servers

Systinet supports only the embedded JBoss application server. This application server is built by HPE, based on JBoss EAP 6.4.0.GA sources.

> **Tip:** For optimal performance, HPE recommends running a dedicated server for Systinet application. Hosting Systinet application together with other applications and services may also impact the performance of Systinet significantly.

Prerequisites - Operating Systems

The server running HPE Systinet must use a supported operating system.

HPE recommends the following operating systems:

- Windows Server 2012 R2
- Red Hat Enterprise Linux 7.1 and 7.2 64-bit
- Oracle Enterprise Linux 7.1 64-bit
- CentOS 7.1 64-bit
- Ubuntu 16.04 64-bit
- Debian 8.5 64-bit

> **Caution:** HPE 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 HPE Systinet.

Prerequisites - Browsers

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

- Google Chrome 50
- Microsoft Internet Explorer 11
- Mozilla Firefox 46
- Mozilla Firefox ESR 45

Prerequisites - Mail Clients

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

- Microsoft Outlook 2013

Supported LDAP Implementations

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

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

HPE Systinet supports the following LDAP implementations:

- Oracle Directory Server Enterprise Edition 11g
- Microsoft Windows Server 2008 Active Directory

Prerequisites - Adobe Flash

Client machines accessing HPE Systinet require Adobe Flash Player version 20.0.

Chapter 4: Preparing Databases

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

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

Read "Database Installation Types" below for information about the different database installation scenarios which vary according to the required level of access to the database.

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

> **Caution:** Encryption keys for password encryption are stored in the EAR file. It is recommended that this file be protected with system file permissions.

The following sections describe database specific prerequisites and procedures to create user types required by different database installation scenarios.

Database Installation Types

- **Create Schema**

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

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

> indexes.

- **Create Database / Tablespace**

  The option to create a database or tablespace is available in the HPE Systinet installer wizard and command-line deployment. This option automates database arrangement as much as possible, but requires database administrator credentials. The process creates users with the necessary permissions/access, 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 HPE Systinet data separately and creates a new database account which uses the new tablespace as its default tablespace.

  - **PostgreSQL**

    This option requires an existing database administrator or super user credentials.

    This option creates a new physical database. It creates a new schema with the name "systinet" to hold data separately. It creates a new database account which belongs to the owner of the new database.

- **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 HPE 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 HPE Systinet administrator to configure the application server datasource.

Set Up Oracle Database

Configure the Oracle database as follows:

- If you are upgrading from older HPE Systinet versions, create a new database. Else, you may loose the data in the database.
- If you are clustering Oracle database (RAC), use Oracle Database 10.2.0.4 or higher. HPE Systinet does not support earlier versions of RAC.
- HPE Systinet installation requires a JDBC driver. Refer to the Supported Database Types for versions of JDBC driver to be used for different database servers.
- To use HPE Systinet Full Text Search, include the "Oracle Text" extension when installing the Oracle server. The "Oracle Text" extension is applied to Oracle by default.
- HPE 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.
- HPE recommends setting the `cursor_sharing` parameter to `FORCE` to improve performance and economize shared pool usage.
- In Oracle 12c, if exception `ORA04036: PGA memory used by the instance exceeds PGA_AGGREGATE_LIMIT` occurs, run the below command:

  ```
  alter system set pga_aggregate_limit=0 scope=both;
  ```

- Create accounts based on the database installation type selected for HPE 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 HPE 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: HPE 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 next 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. HPE recommends creating a new tablespace to hold HPE 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, sequences, and views.

```
sqlplus <system/password>@<connect_identifier>
/* add "connect", "resource" roles to <user> */
grant connect to <user>;
grant resource to <user>;
/* add "create view", "create materialized view" privileges to <user> */
grant create any view to <user>;
grant create any materialized view to <user>;
/* Oracle 12c has revoked some system privileges from the RESOURCE role. In
this case EM database
user needs to be granted with explicit privileges */
grant unlimited tablespace to <user>;
grant CREATE ANY TABLE, SELECT ANY TABLE, DROP ANY TABLE, INSERT ANY TABLE,
UPDATE ANY TABLE,
DELETE ANY TABLE, CREATE SESSION, CREATE PROCEDURE, CREATE SEQUENCE to <user>;
/* add "create synonym", "drop synonym" privileges to <user>; required for
setting up common user only */
grant create any synonym to <user>;
grant drop any synonym to <user>;

exit;
```

> **Note:** In Oracle 12c multitenant mode, user names must start with 'c##'.

4. Grant privileges for the user by executing the following commands:

```
GRANT SELECT ON sys.dba_pending_transactions TO <user>;
GRANT SELECT ON sys.pending_trans$ TO <user>;
GRANT SELECT ON sys.dba_2pc_pending TO <user>;
GRANT EXECUTE ON sys.dbms_xa TO <user>;
```

Otherwise, you will get the following error in the server log:

```
WARN [com.arjuna.ats.jta.logging.loggerI18N]
[com.arjuna.ats.internal.jta.recovery.xarecovery1]
Local XARecoveryModule.xaRecovery got XA exception
javax.transaction.xa.XAException, XAException.XAER_RMERR
```

5. Optionally, disable the default password expiry policy (so that the database password need not be changed every 6 months).

```
alter profile default limit password_life_time unlimited;
```

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

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

Set Up an Oracle Common User

In cases where the database administrator restricts access to the database to just select, insert,

update, and delete operations, HPE Systinet requires a user with these privileges.

> **Note:** This setup is applicable to database decoupled installation mode only. The HPE Systinet schema must exist before you create the common user. For more details, see "Manual Database Deployment" on page 71.

To Set Up a Common User in Oracle:

1. Login as database administrator and create an account that is used by HPE Systinet at runtime.

2. 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 &1' || '.' || table_name || '
TO &2;' FROM user_tables;
SELECT 'GRANT SELECT ON &1' || '.' || sequence_name || ' TO &2;' FROM user_
sequences;
spool off
spool ./synonyms.sql
SELECT 'CREATE SYNONYM &2' || '.' || table_name || ' FOR &1' || '.' || table_
name || ';' FROM user_tables;
SELECT 'CREATE SYNONYM &2' || '.' || sequence_name || ' FOR &1' || '.' ||
sequence_name || ';' FROM user_sequences;
spool off
```

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

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

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

4. As the *power_user* or database administrator, execute `synonyms.sql` and `grant.sql` in sequence.

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

Set Up Microsoft SQL

You can use HPE Systinet with a Microsoft SQL database. The database requires set up and configuration prior to installing HPE Systinet.

1. Use SQL Server Configuration Manager to enable the TCP/IP protocol and use a static port (for example 1433).
2. HPE Systinet installation requires a JDBC driver:

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

3. HPE 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

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

6. Create users based on the database installation type selected for the HPE 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. HPE 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 HPE 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 and then create the schema manually. Optionally, you can create a common user account with minimal privileges.

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

7. To activate snapshot isolation for the Systinet database, execute the following statements:

```
ALTER DATABASE [database_name] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [database_name] SET READ_COMMITTED_SNAPSHOT ON;
```

For additional MSSQL setup details, see the "Set Up an MSSQL Common User" below.

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, HPE 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 HPE Systinet (`sysdb`).

   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 [sysdb]
GO
CREATE USER [common_user] FOR LOGIN [common_user]
GO
```

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

For example, execute the following statements:

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

Set Up PostgreSQL Database

Configure the PostgreSQL database as follows for use with HPE Systinet:

- If you are upgrading from older versions, create a new database. Else, you may loose the data in the database.
- If you are clustering PostgreSQL database, you must initialize a database storage area on the disk. For more detail, refer to the following PostgreSQL document: https://www.postgresql.org/docs/8.3/static/creating-cluster.html.
- PostgreSQL JDBC driver is embedded during installation itself.
- To enable *Prepared Transaction* parameter in PostgreSQL:
  - Access the PostgreSQL server.
  - Open *postgresql.conf* file in *{POSTGRESQL_INSTALL_FOLDER}\data\ directory*. Uncomment this line: `max_prepared_transactions and set its value to non-zero`.

For more details, refer to the document in the following URL: https://www.postgresql.org/docs/current/static/runtime-config-resource.html.

- HPE Systinet recommends using a super user in the database server to create HPE Systinet database with ownership rights. The super user must have the DATABASE and ROLE creator roles.
  - For the Create Database option, the installer uses the super user credentials to create the database, schema and an account which is the owner of this new database.

> **Note:** If the database name already exists, the schema is overwritten wiping out previous data.

> **Caution:** If the super user credentials were not used to install, it could result in issues related to convert char type to number, when using Systinet. To resolve this,use a super user to connect to the database and execute the following SQL statements:
>
> - *create cast (varchar as float) with inout as implicit;*
> - *create cast (varchar as bigint) with inout as implicit;*
> - *create cast (char as bigint) with inout as implicit;*
> - *create cast (text as bigint) with inout as implicit;*
> - *update pg_cast set castcontext = 'i' , castmethod = 'i' where castsource = 701 and casttarget =1700;*

For additional information on PostgreSQL setup, see "Set Up PostgreSQL Super User" below.

Set Up PostgreSQL Super User

To use the Create Database option during installation, the database administrator must create a super user with appropriate privileges to the database.

To Set Up a Super User for PostgreSQL:

To set up a Super User for PostgreSQL, create a super user account, create the database and then create roles.

CREATE USER name PASSWORD password SUPERUSER CREATEDB CREATEROLE

Example: CREATE USER postgres PASSWORD postgres SUPERUSER CREATEDB CREATEROLE

Chapter 5: Preparing LDAP and CA Single Sign On

You can set up authentication based on your deployments. You can use LDAP or CA Single Sign On for authentication. The configuration for LDAP or CA Single Sign On is explained in the following sections:

Prepare LDAP Integration

Automatic Service Discovery

The automatic discovery of LDAP servers means you do not have to hardwire the URL and port of the LDAP server. Instead you can use `ldap:///o=JNDITutorial,dc=example,dc=com` as a URL, and the real URL is deduced from the distinguished name `o=JNDITutorial,dc=example,dc=com`.

Automatic discovery of the LDAP service using the URL's distinguished name is supported only in Java 2 SDK, versions 1.4.1 and later. Hence ensure 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 set in 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

Property Name	Property Description	API Link
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
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 CA Single Sign On Endpoint Authentication

In CA Single Sign On, configure HPE Systinet endpoint authentication.

By default, HPE Systinet performs the following authentication on HPE Systinet endpoints:

- **FORM authentication**:
  - /web/service/catalog/*
  - /web/policy-manager/*

- /web/shared/*
- /web/artifactIconList.htm

- **HTTP basic authentication**:
  - /em/platform/restBasic/*
  - /platform/restSecure/*
  - /policymgr/restSecure/*
  - /reporting/restSecure/*
  - /remote/navigator/*
  - /remote/upload/*
- **Unauthenticated URL patterns:**
  - /em/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: HTTP Proxy Requirement

Due to security and cluster support, an HTTP proxy server must be installed before installing HPE 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.

The following sections describes how to install HPE Systinet with a proxy server:

Install HPE Systinet with a Proxy Server

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

1. "How to Install HPE Systinet with a Proxy Server" below:
   a. Install the Apache Web Server.
   b. Configure the Apache Web Server as a Reversed Proxy.
   c. Enable SSL in the Apache Web Server (Optional).
2. "How to Configure HPE Systinet with a Proxy Server" on page 31

How to Install HPE Systinet with 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 /em http://[host]:[port]/em
ProxyPassReverse /em http://[host]:[port]/em
```

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

- Organizational Unit Name (example: section) []:**<organization unit>**
- Common Name (example: server FQDN or YOUR name) []:**<hostname>**
- Email Address []:**<email>**
- A challenge password []:**<password>**
- An optional company name []:**<company>**

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 -days
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.

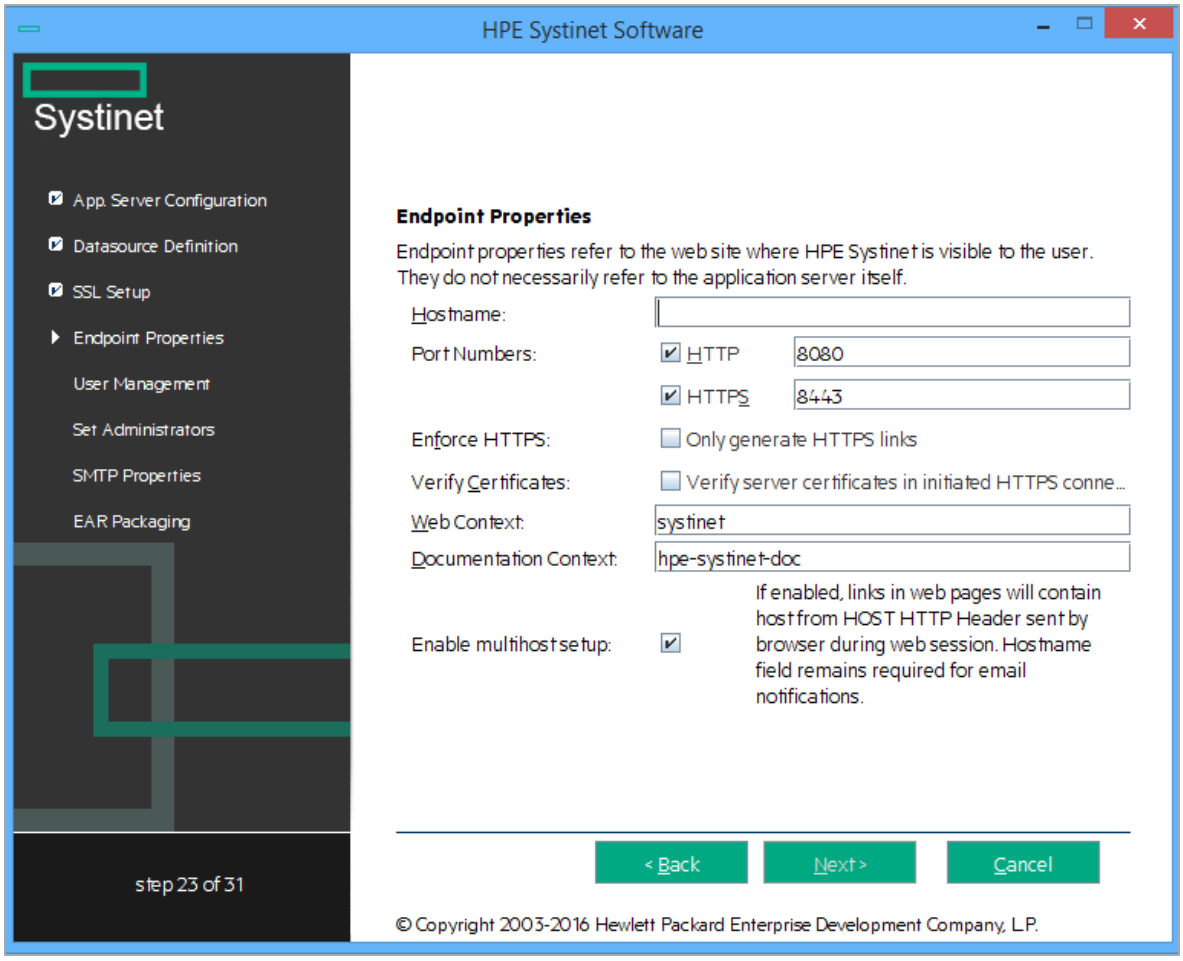
g. On the client browser, add **cert.crt** to Trusted Root CA.

> **Caution:** If **openssl** is installed with Apache web server, make sure it is patched frequently to avoid any security issues.

How to Configure HPE Systinet with a Proxy Server

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

> **Note:** Make sure you redeploy **hp-soa-systinet.ear** file after changing Endpoint Properties in Setup tool (step 'Enterprise Application Deployment' in Advanced scenario).



Test the Proxy Server Installation

Access the proxy server with URL (*http://[proxyHost]:[proxyPort]/em*).

A successful configuration must result in the following:

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

Chapter 7: Using the HPE Systinet Installer Wizard

The HPE Systinet installer wizard is the easiest way to install HPE Systinet. However, it may not be suitable for all the configuration options required by production environments.

Before using the HPE Systinet installer, make sure that you have set the environment correctly.

For hardware and software requirements, as well as supported platforms, see "Prerequisites and Supported Platforms" on page 9.

For an evaluation environment, you need valid credentials to a configured database. For details, see "Preparing Databases" on page 15.

JBoss does not require any additional configuration for evaluation purposes.

The following image briefly describes the steps to install HPE Systinet:

HPE Systinet installation wizard consists of the following steps:

20. "Step 20 - Confirmation" on page 68

Step 1 - Start the HPE Systinet Installation

1. Make sure the application server is not running.
2. Do one of the following:
   - Execute the file `hpe-systinet-10.04.jar`, located on the installation CD or in your distribution directory.
   - Execute the following command:

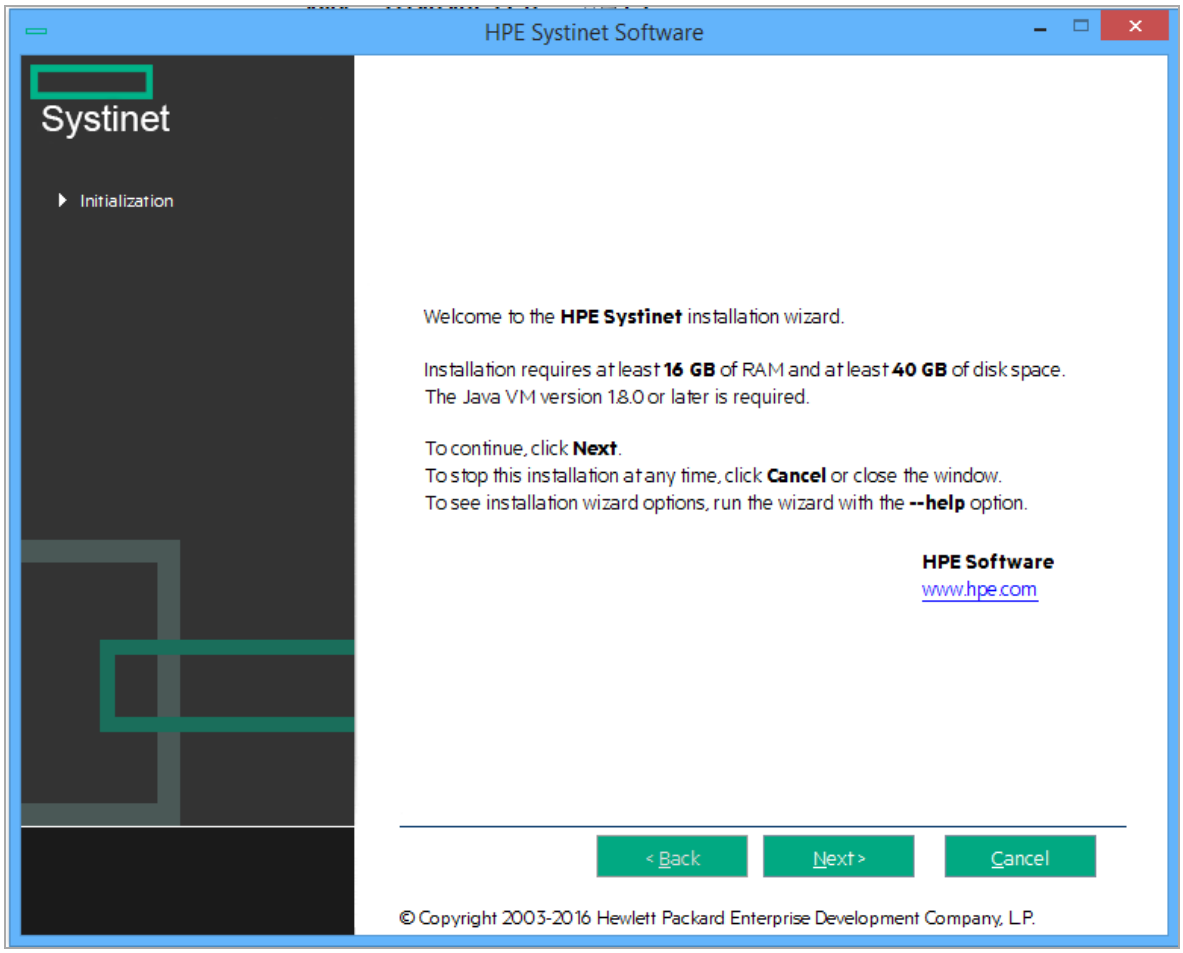
     ```
     java -jar hpe-systinet-10.04.jar
     ```

   The HPE Systinet Installation wizard displays the Welcome page.

Continue to "Step 2 - Welcome" below.

Step 2 - Welcome

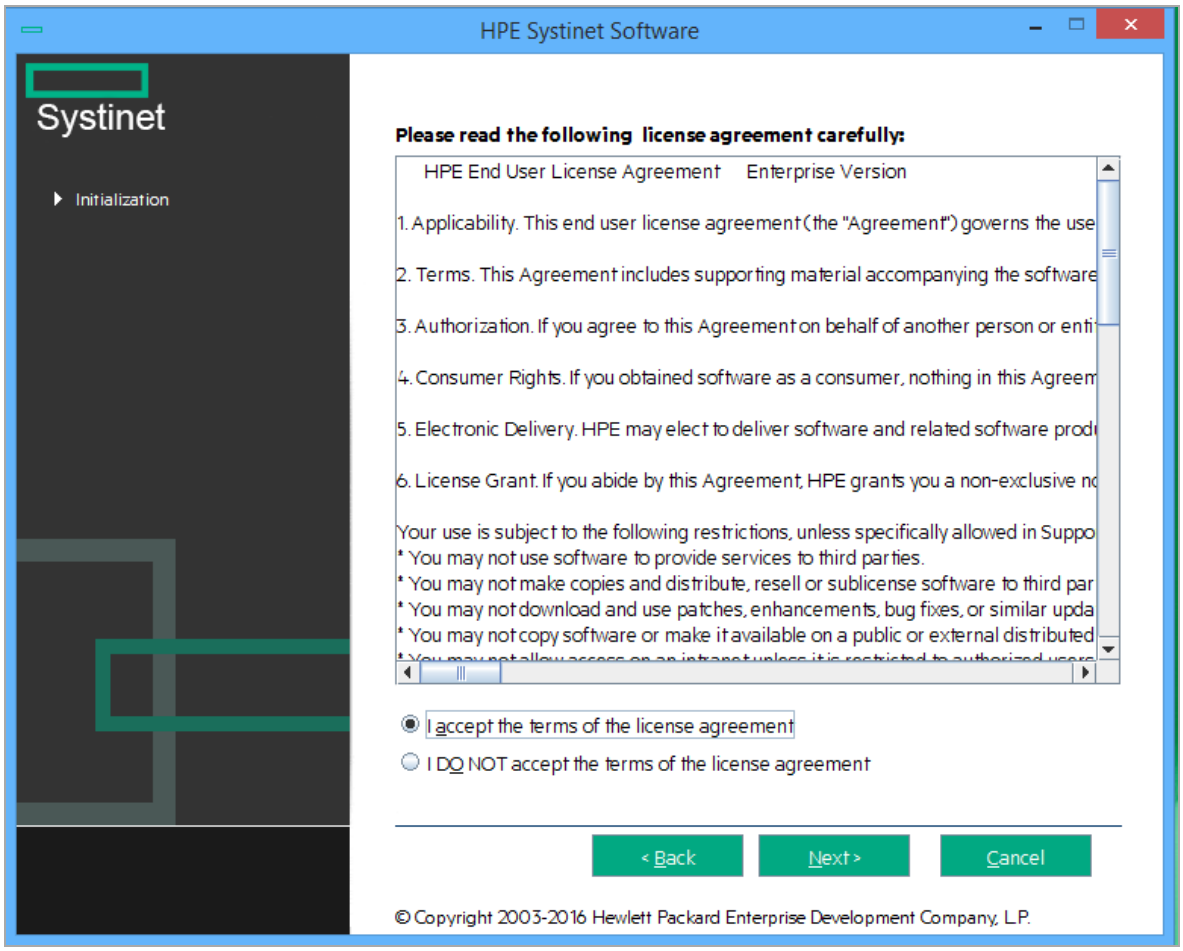
In the Welcome page, review the hardware and software requirements.



Click **Next** to continue to "Step 3 - License" below.

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 contains the license agreement in different languages including Japanese, Korean, Chinese, and Taiwanese.

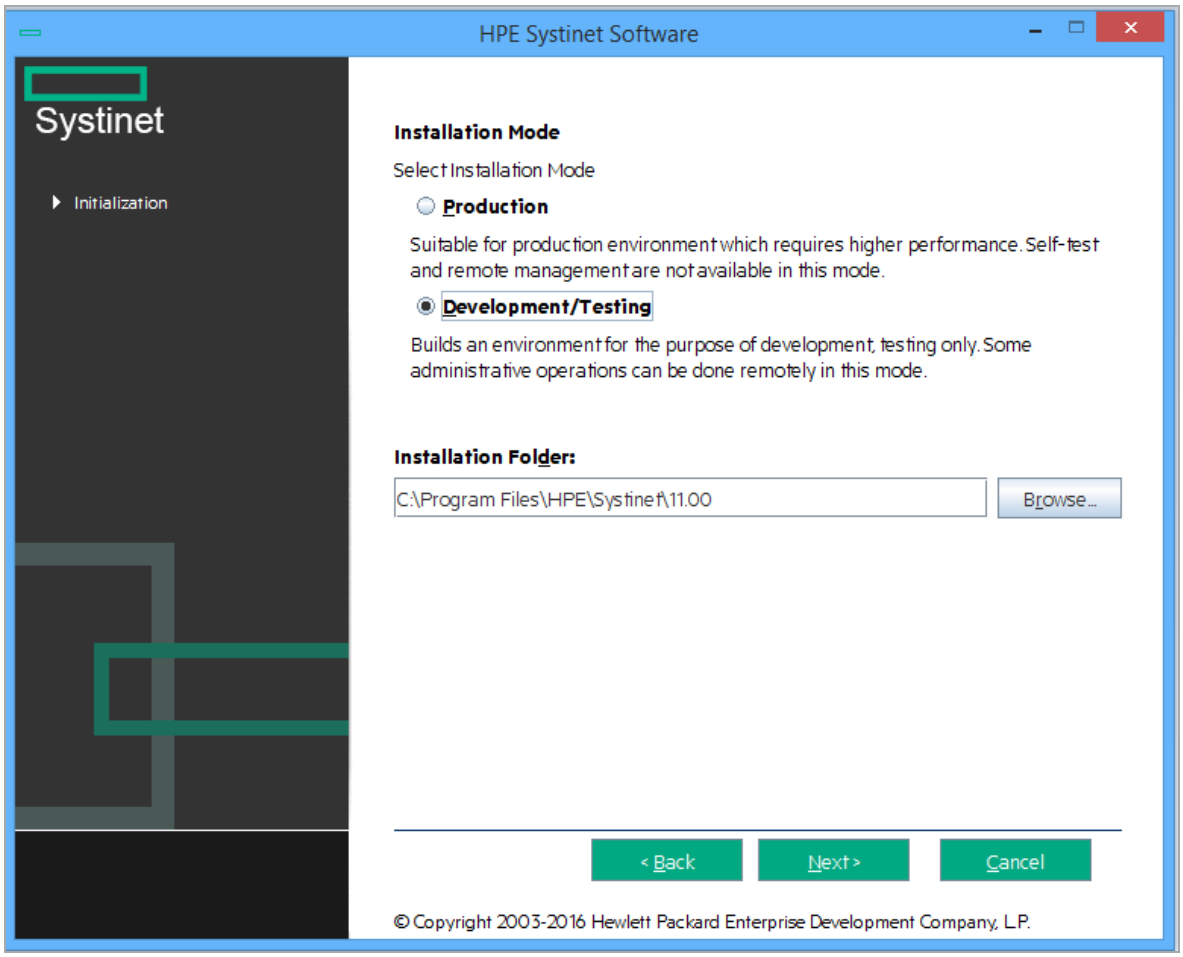
Select **I accept the terms of the license agreement**.

Click **Next** to continue to "Step 4 - Installation Folder" below.

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.



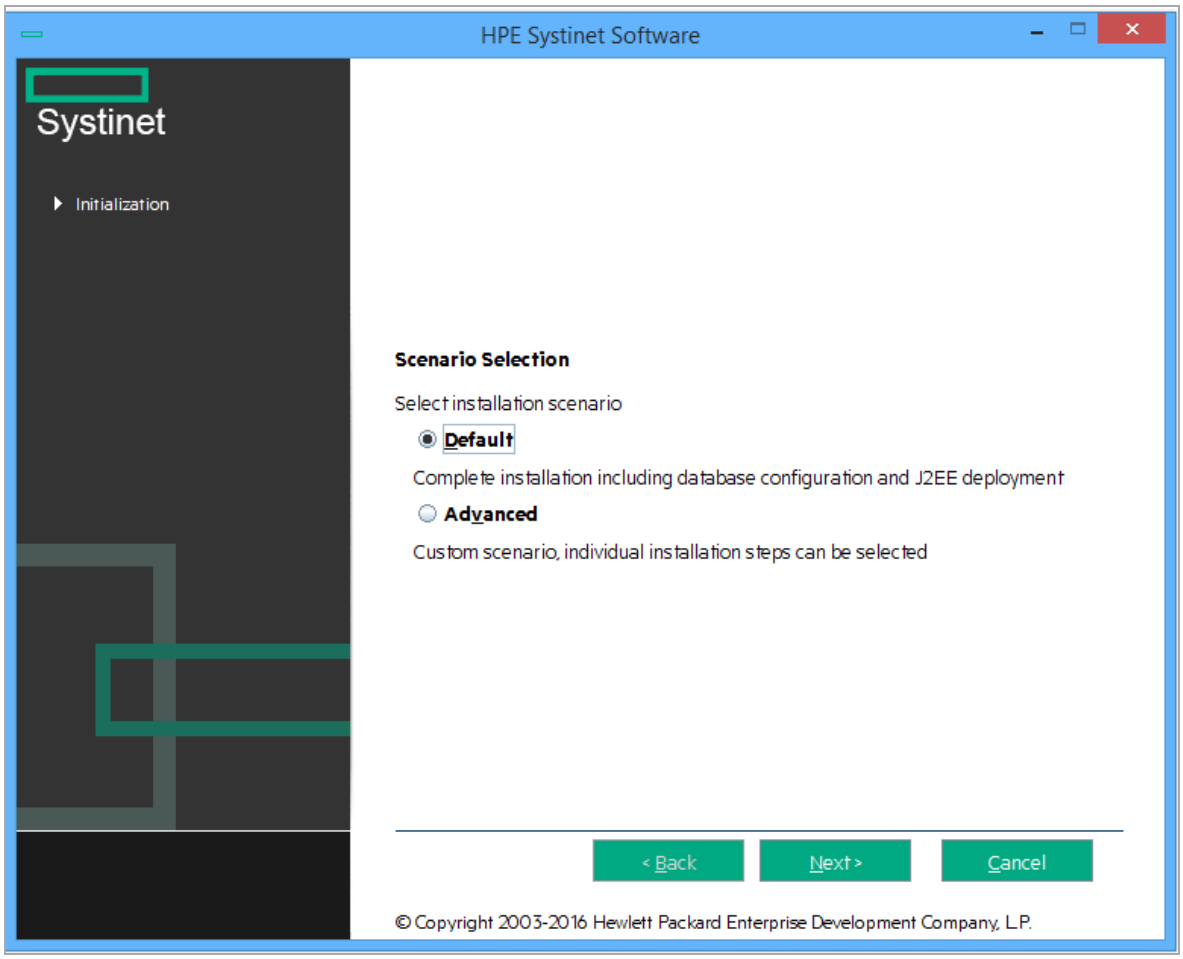
> **Note:** In this document, the installation location is referred to as `SYSTINET_HOME`.

> **Note:** To avoid error when installing HPE Systinet into a Windows system folder, disable User Access Control (UAC) in Windows Control Panel.

Click **Next** to unpack the distribution files to the chosen location and continue to "Step 5 - Scenario Selection" below.

Step 5 - Scenario Selection

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

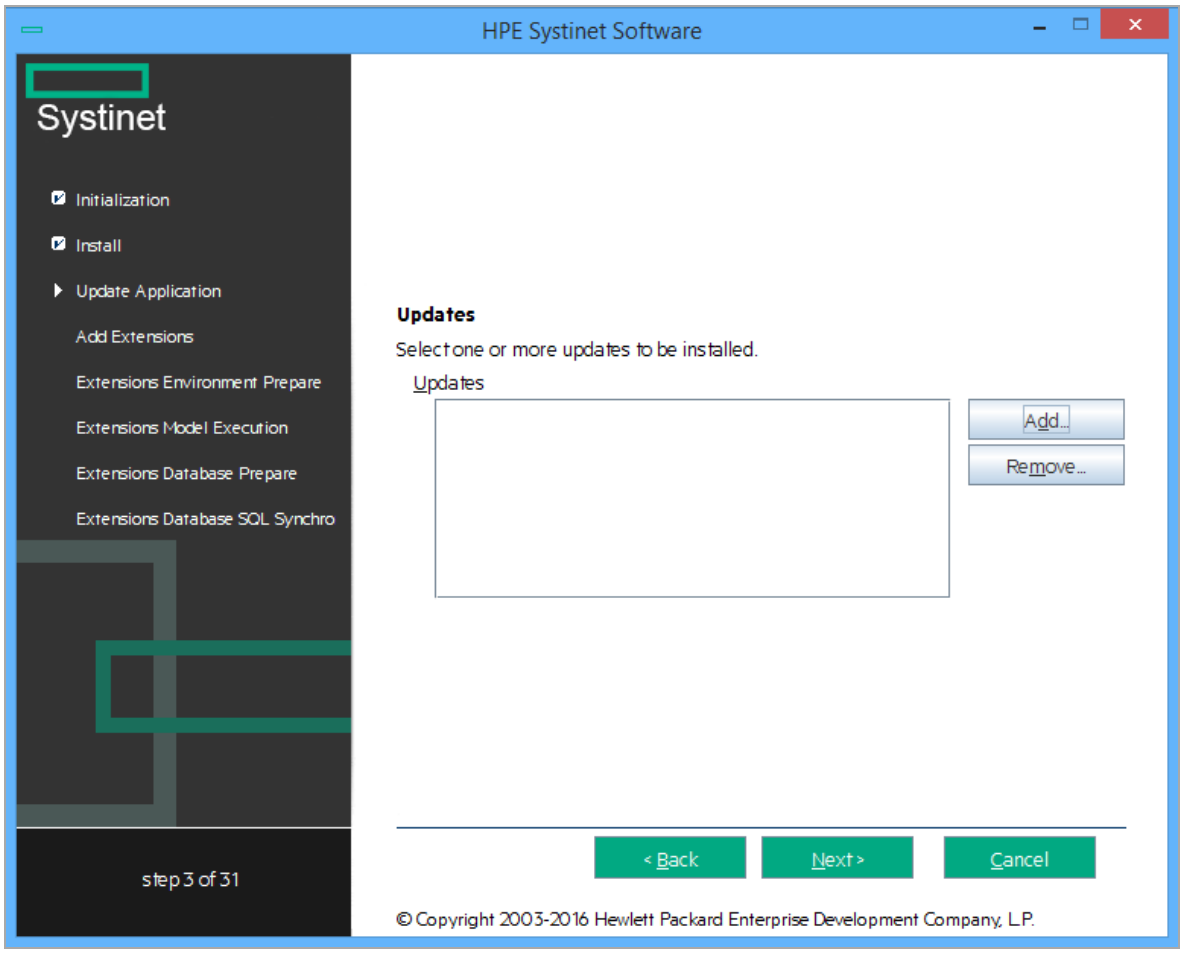


Note: The **Advanced** scenarios enable you to perform parts of the installation separately.

Click **Next** to validate the installation and continue to "Step 6 - Updates" below.

Step 6 - Updates

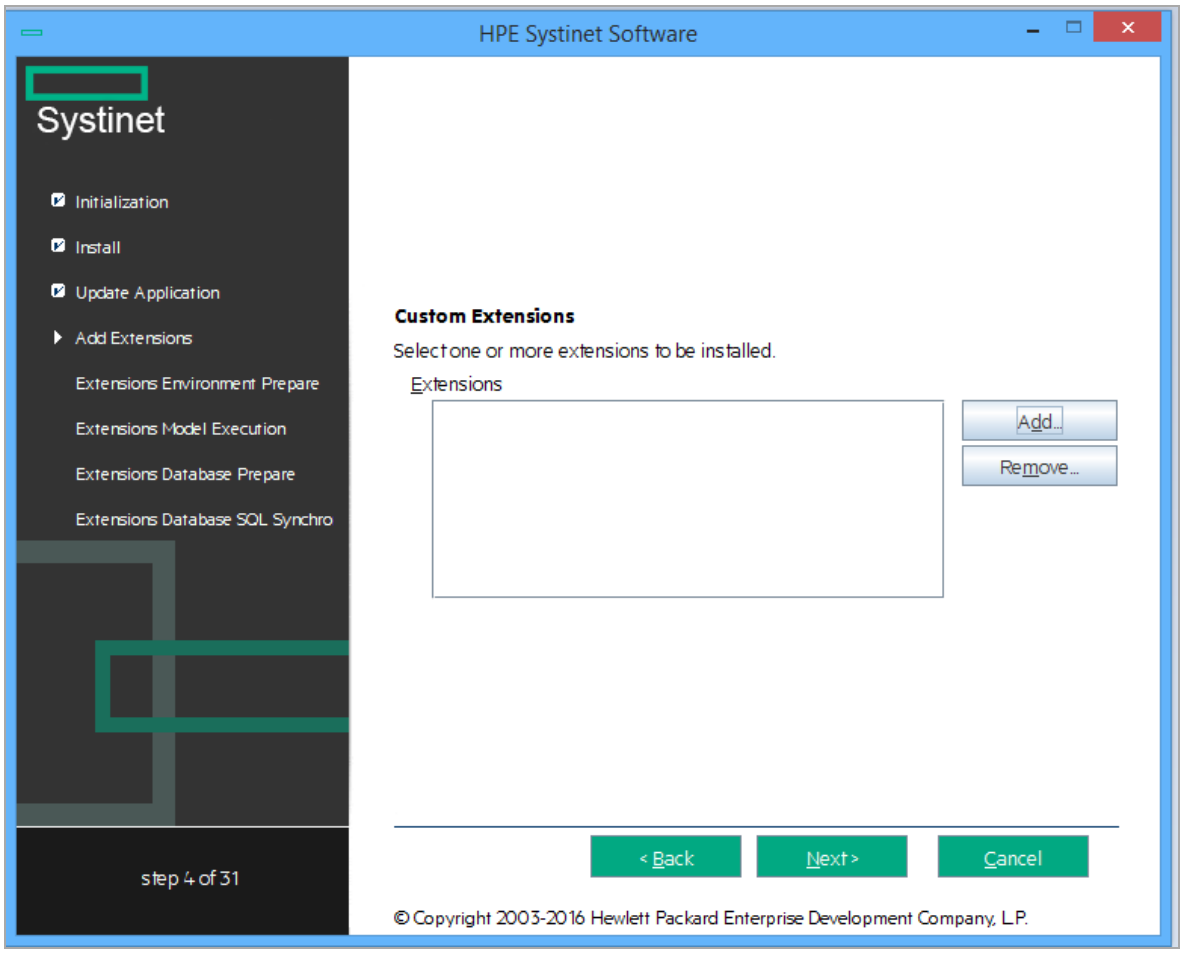
In the Updates page, use **Add** and **Remove** to select updates (such as patches) to apply during the installation.



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

Step 7 - Custom Extensions

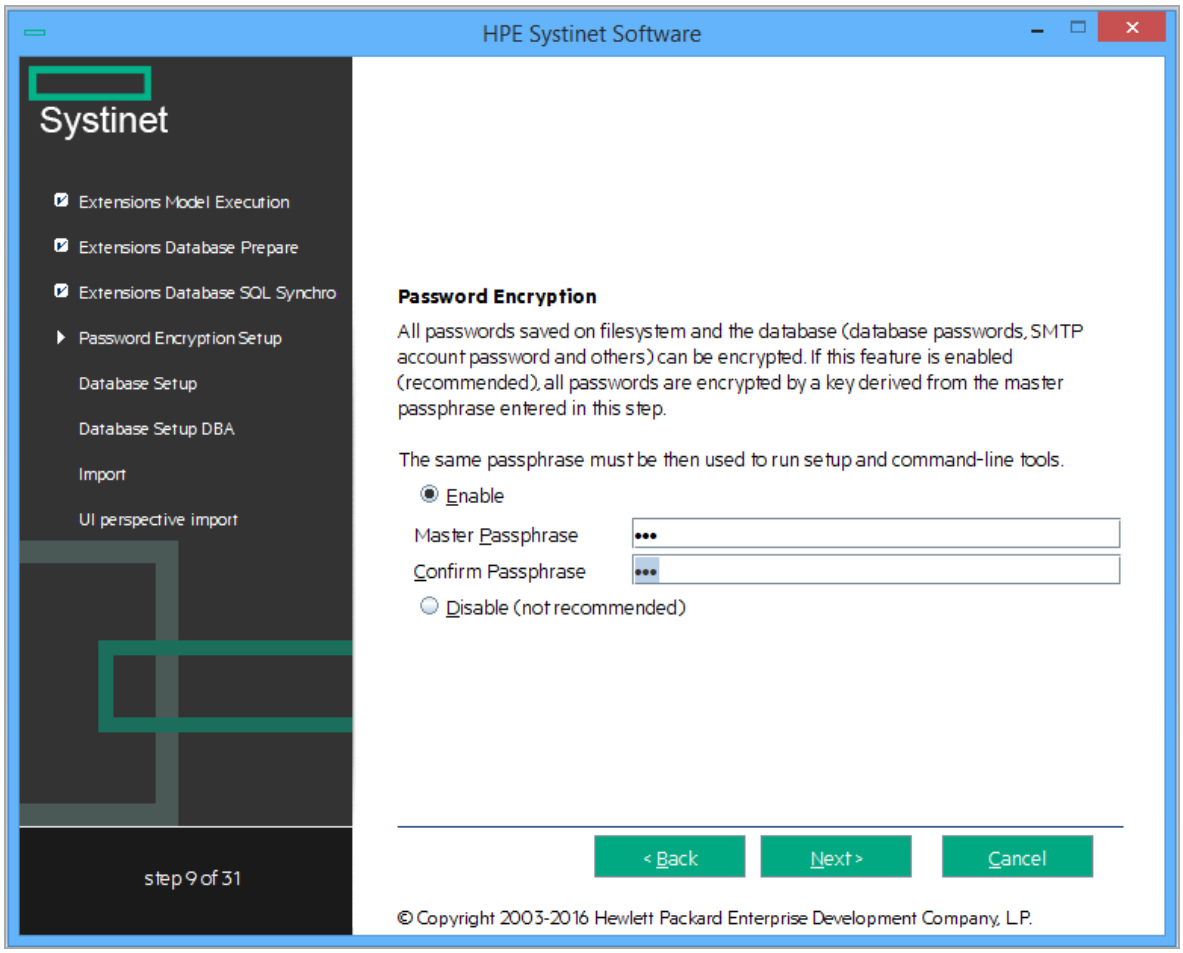
In the Custom Extensions page, use **Add** and **Remove** to select existing extensions that will extend the functionality of HPE Systinet. The selected extensions will be applied during the installation.



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

Step 8 - Password Encryption

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



Do one of the following:

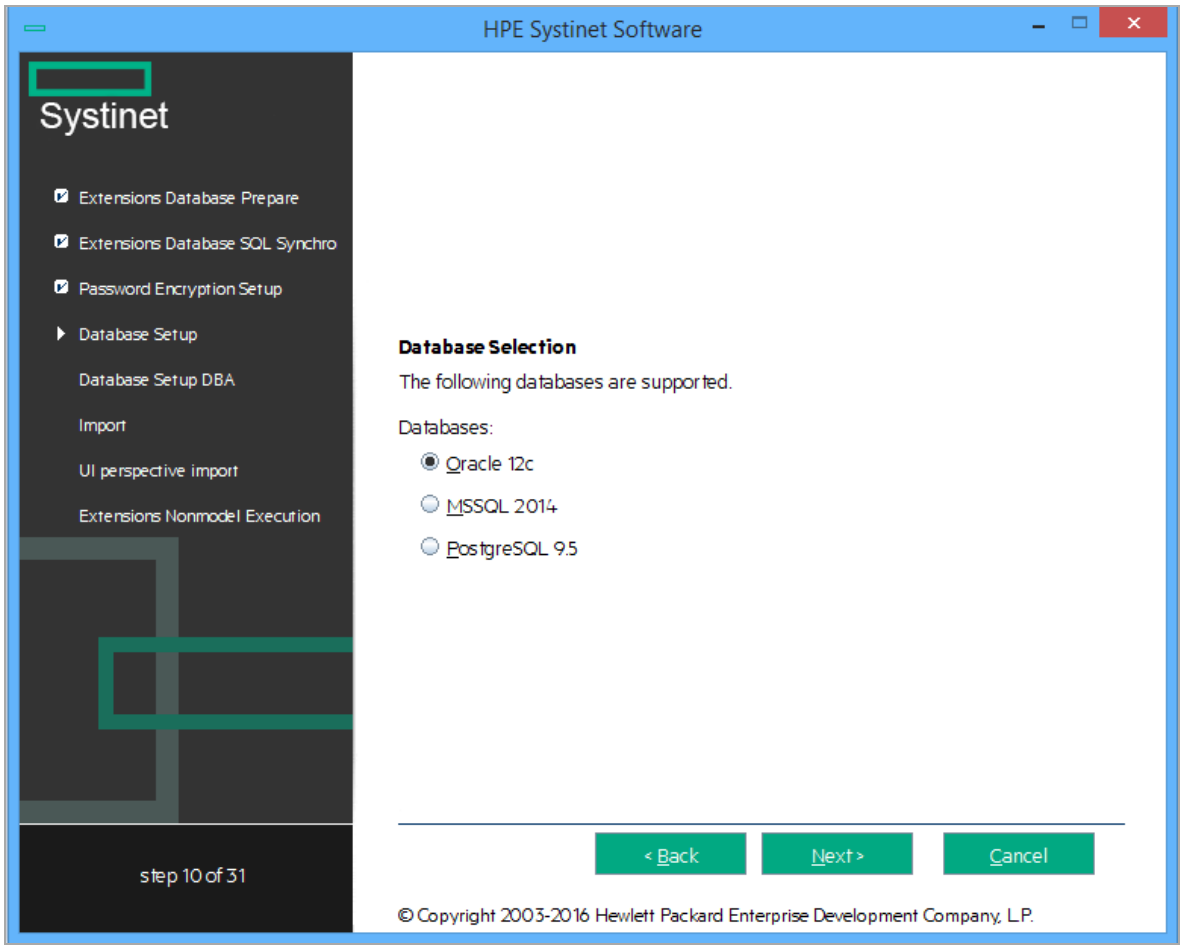
- For production or sensitive installations, select **Enable** and type the **Master Passphrase** and **Confirm Passphrase**.
- For demo installations, select **Disable**.

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

Click **Next** to continue to "Step 9 - Database Selection" on the next page.

Step 9 - Database Selection

In the Database Selection Page, select one of the following database types to use:



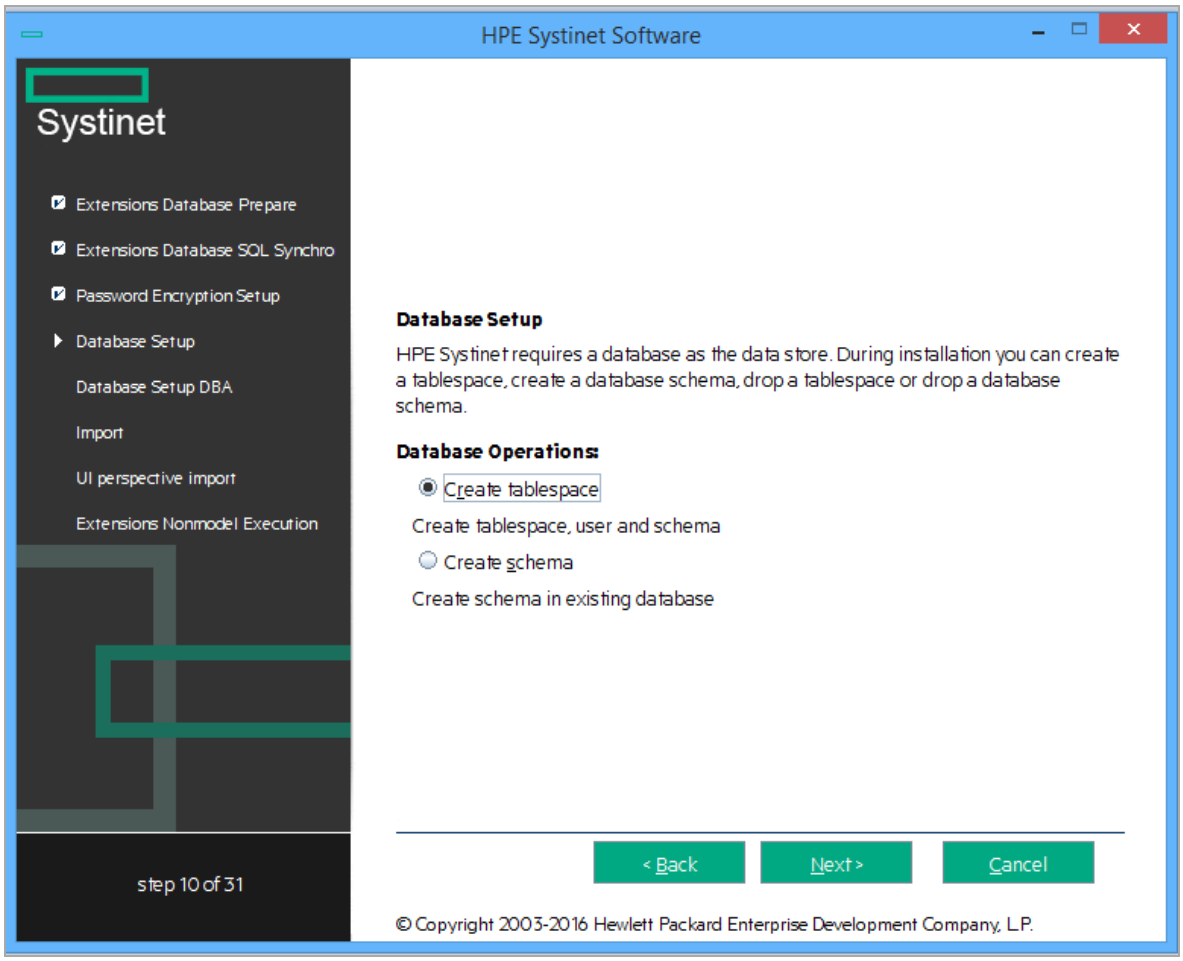
- **Oracle 12c**
- **MSSQL 2014**
- **PostgreSQL 9.5**

> **Note:** HPE Systinet supports PostgreSQL database in Development Mode only.

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

Step 10 - Database Setup

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



If you choose Oracle, available options are:

- **Create Tablespace**
- **Create Schema**

If you choose MSSQL, available options are:

- **Create Database**
- **Create Schema**

If you choose Postgre SQL, available options is:

- **Create Database**

Select the appropriate option according to your database administrator.

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

Continue to "Step 11 - Database Parameters" on the next page.

Step 11 - Database Parameters

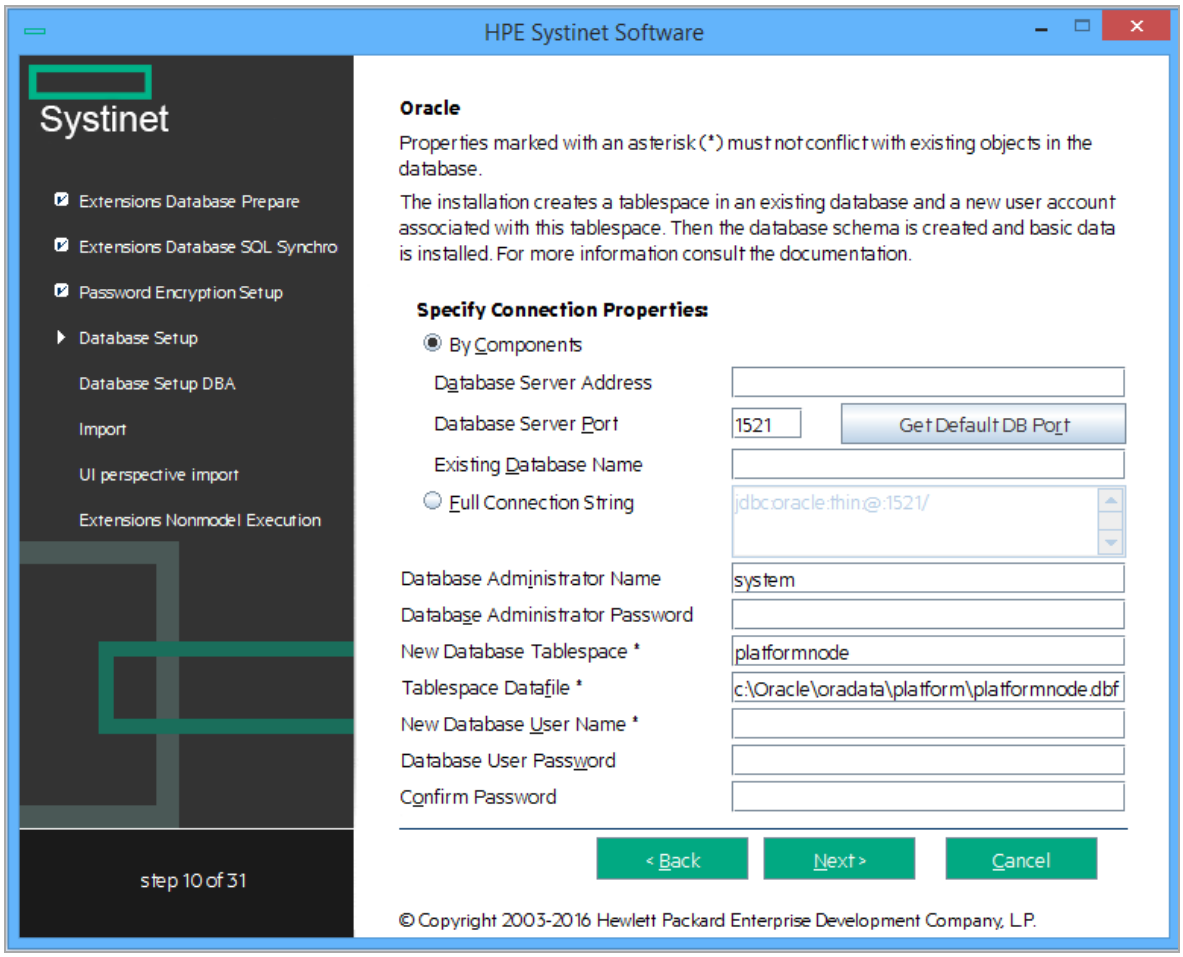
The required database parameters vary depending on your database type and setup type.

For details, see the appropriate section:

- "Oracle Create Tablespace" below
- "Oracle Create Schema" on page 47
- "MSSQL Create Database" on page 49
- "MSSQL Create Schema" on page 50
- "PostgreSQL Create Database" on page 52

Oracle Create Tablespace

In the Oracle tablespace page, 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 an alternative option to inputting the individual connection parameters.
Database Administrator	User name and password of the administrator of the	

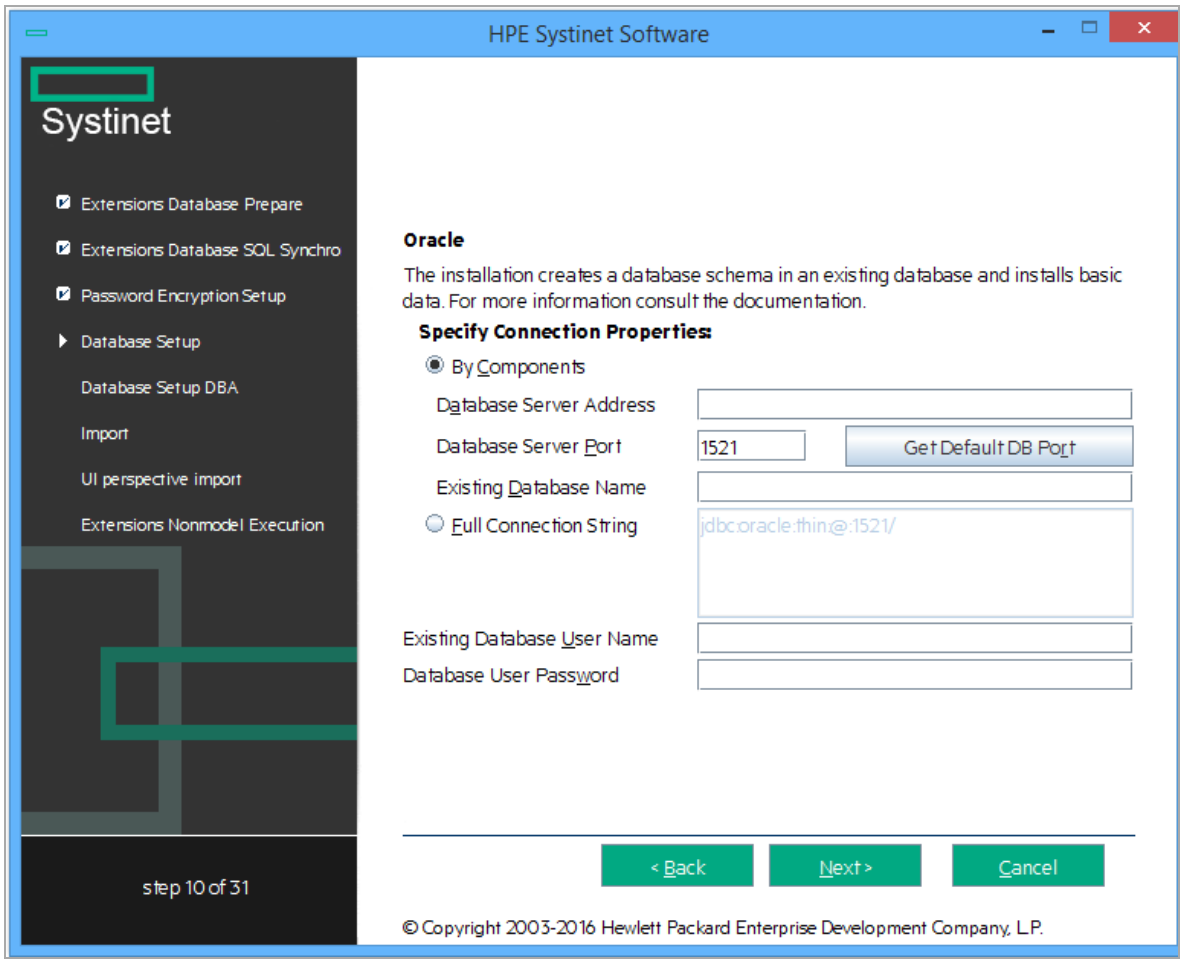
Oracle Create Tablespace Parameters, continued

Parameter	Description	Notes
Name	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 53.

Oracle Create Schema

In the create a new Oracle schema page, set the following parameters:



Oracle Create Schema Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform` the hostname is `orahost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform` the port number is `1521`.
Existing Database Name	Name of the database.	For example, in the database connection string `jdbc:oracle:thin:@orahost:1521/platform` the database name is `platform`.
Full Connection String	Full connection string to the database.	Select this as an alternative option to inputting the individual connection parameters.
Existing Database	User name and password to connect to the database.	

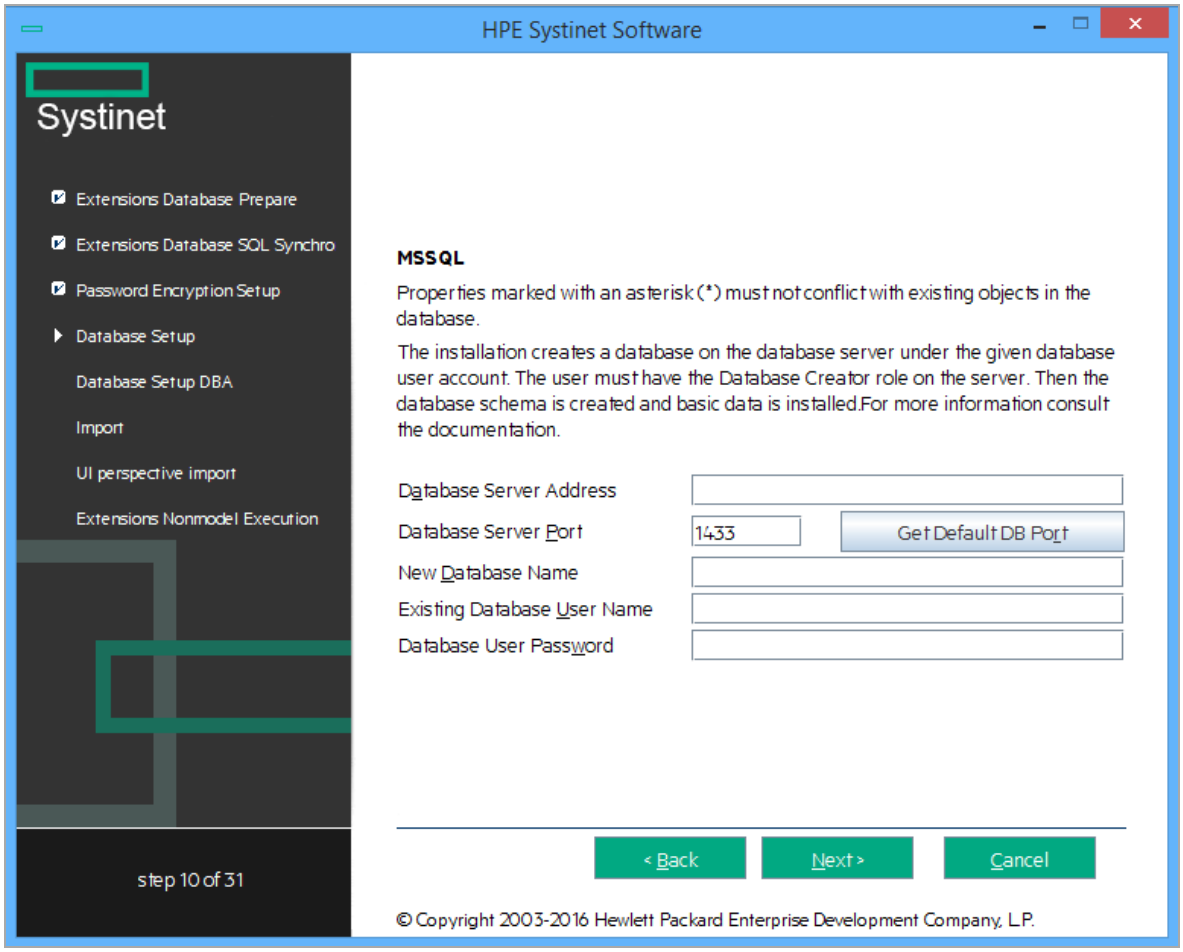
Oracle Create Schema Parameters, continued

Parameter	Description	Notes
User Name		
Database User Password		

Click **Next** to continue to "Step 12 - JDBC Drivers" on page 53.

MSSQL Create Database

In the create a new MSSQL database page, set the following parameters:



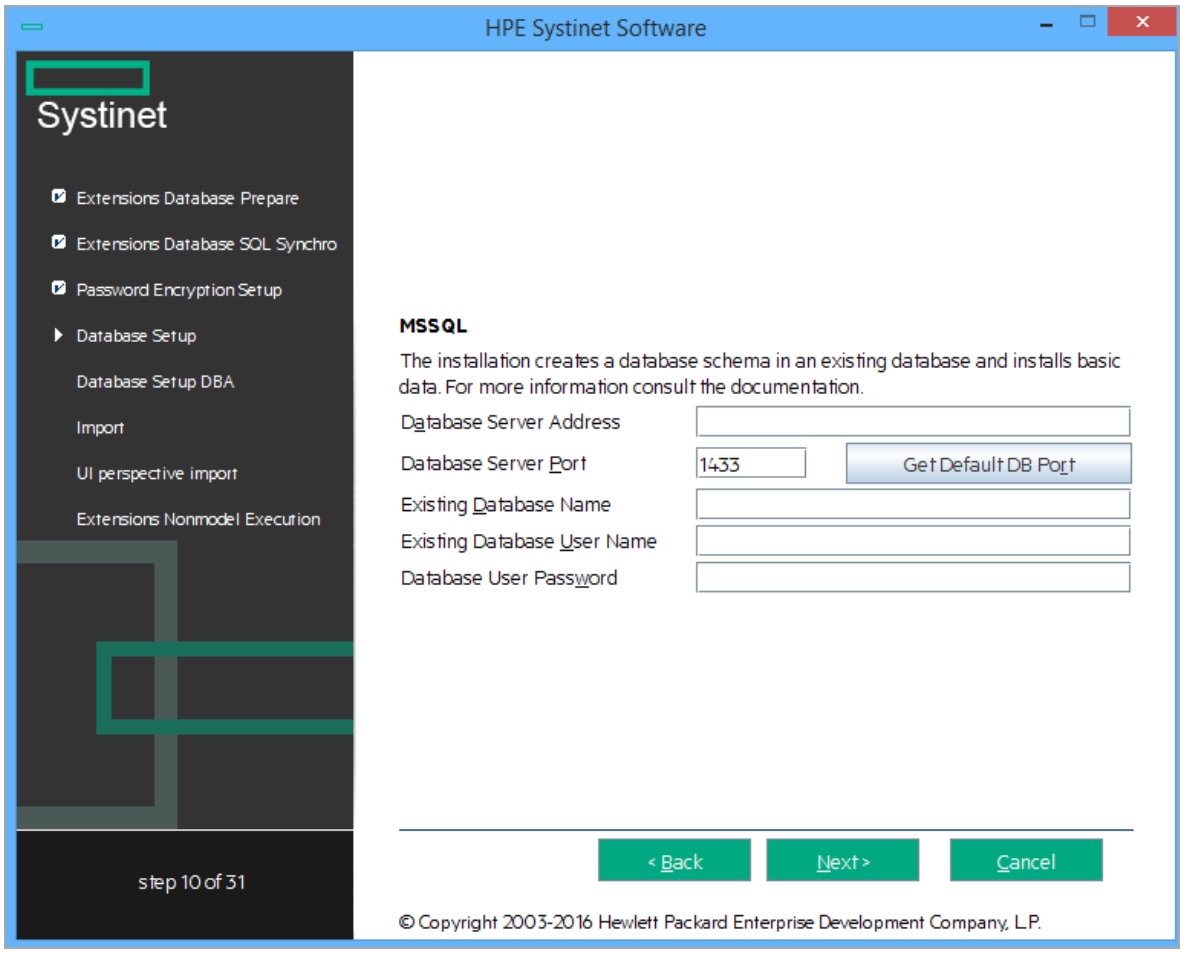
MSSQL Create Database Parameters

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.	
Database User Password		

Click **Next** to continue to "Step 12 - JDBC Drivers" on page 53.

MSSQL Create Schema

In the create a new MSSQL schema page, set the following parameters:



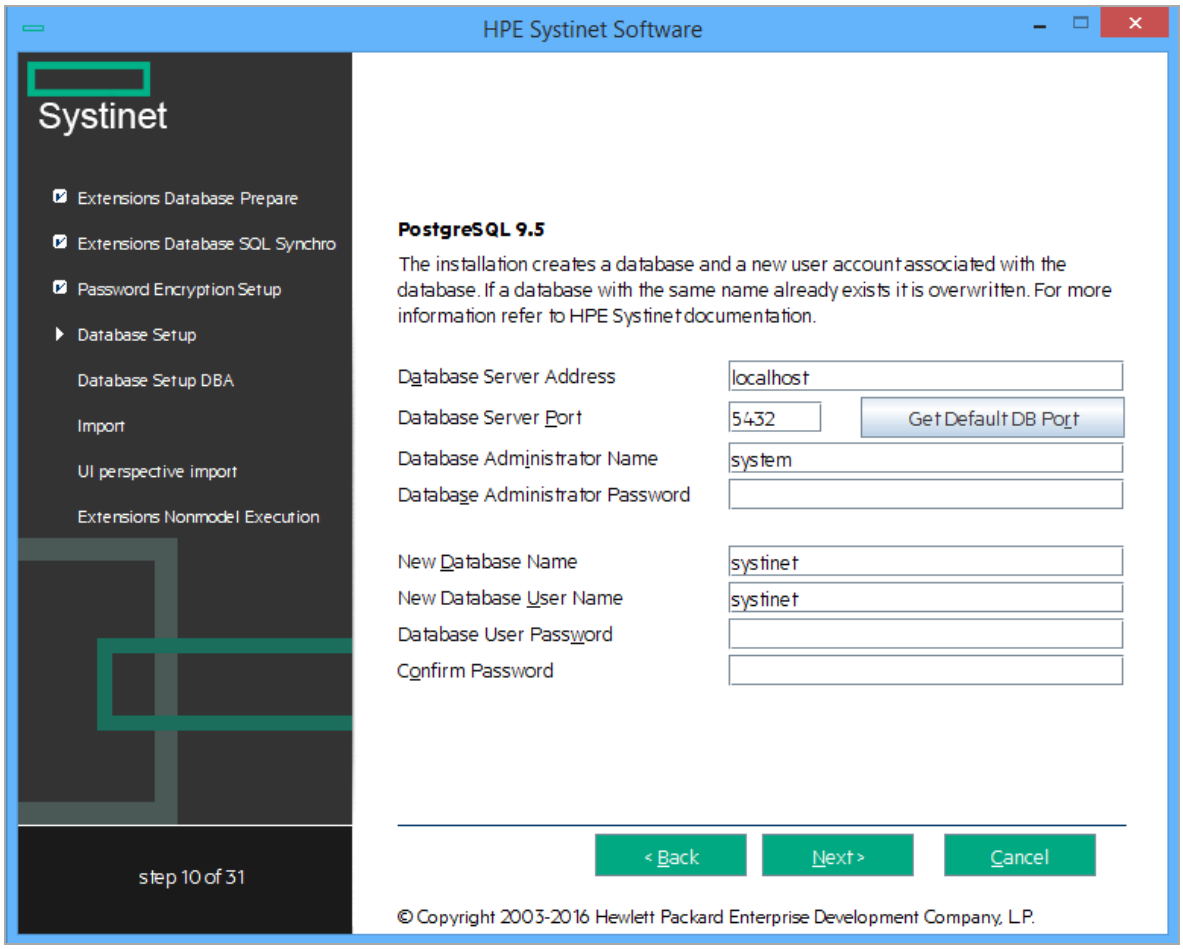
MSSQL Create Schema Parameters

Parameter	Description	Notes
Database Server Address	Hostname or IP address where the database server is accessible.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform` the hostname is `sqlhost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform` the port number is `1433`.
Existing Database Name	Name of the database.	For example, in the database connection string `jdbc:sqlserver://sqlhost:1433:platform` the database name is `platform`.
Existing Database User Name	For the Create Schema option the user must have schema creation rights.	
Database User Password		

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

PostgreSQL Create Database

In the create a new PostgreSQL database page, set the following parameters:



PostgreSQL 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:postgresql://postgrehost:port/em` the hostname is `postgrehost`.
Database Server Port	Connection port for the database.	For example, in the database connection string `jdbc:postgresql://postgrehost:5432/em` the port number is `5432`.

PostgreSQL Create Database Parameters, continued

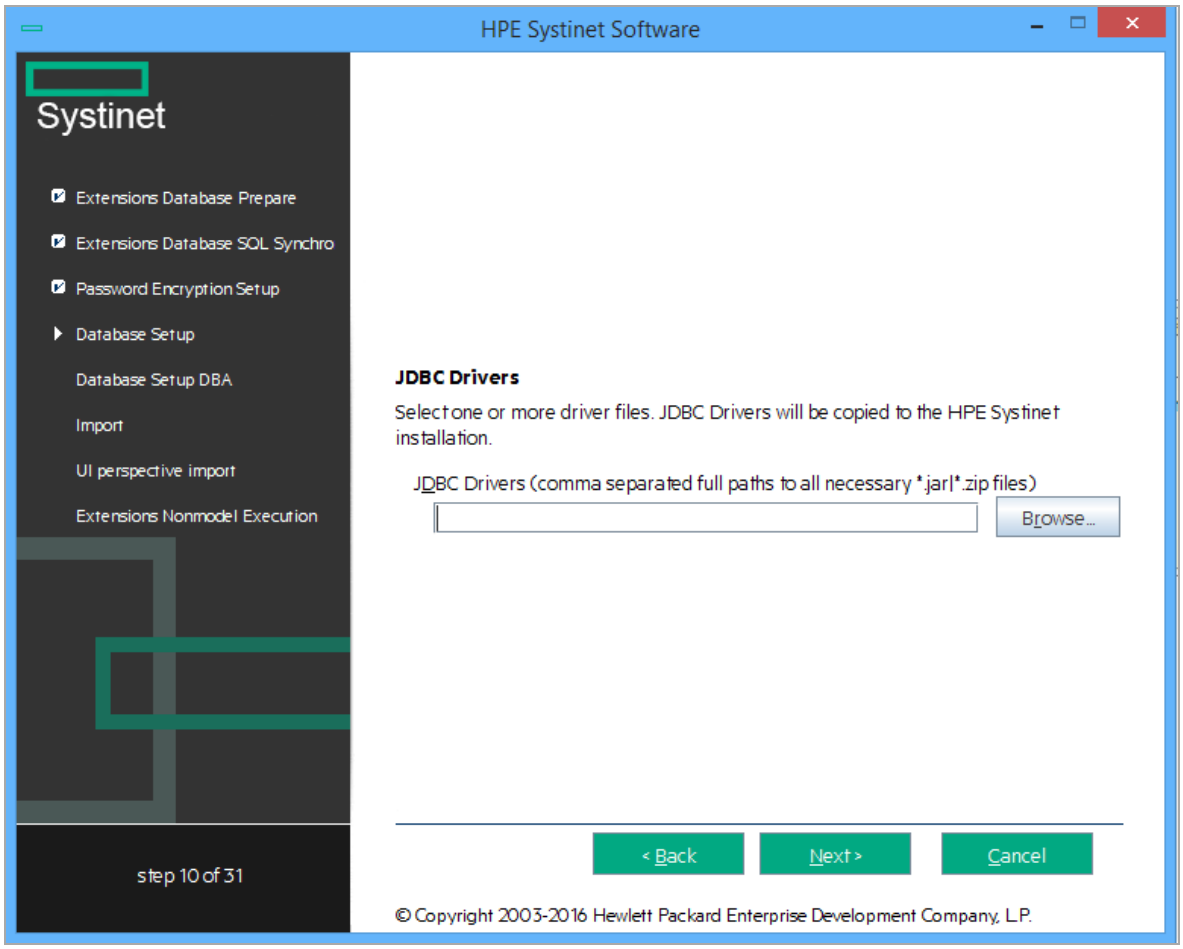
Parameter	Description	Notes
Database Administrator Name	For the Create Database option the user must have super user, role creator and database creator roles.	
Database Administrator Password		
New Database Name	Name of the database.	For example, in the database connection string `jdbc:postgresql://postgrehost:5432/em` the database name is `systinet`.
New Database User Name	For the Create Database option, a new database user is created and granted ownership of the database.	
Database User Password		
Confirm Password		

PostgreSQL JDBC driver is provided in the installation package itself, hence not required to specify during installation.

Click **Next** to continue to "Step 13 - Repository Import" on page 55.

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	12.1.0.1.0	ojdbc7.jar, orai18n.jar	12.1.0.1.0	oracle.jdbc.driver.OracleDriver

Supported MSSQL Drivers

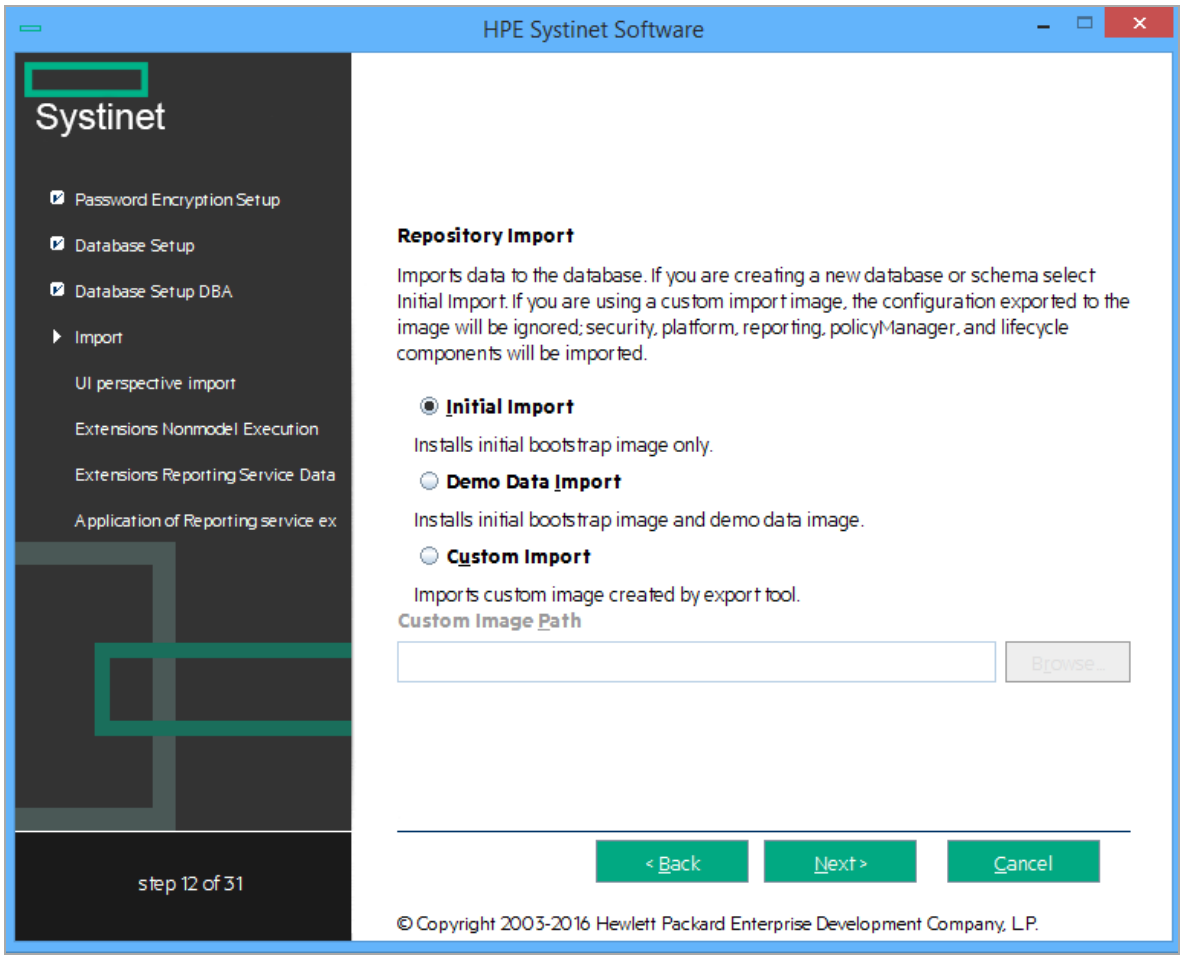
Database	DB Version	Driver Packages	Driver Version	Driver Class
Microsoft SQL Server	2014	sqljdbc4.jar	4.0	com.microsoft.sqlserver.jdbc.SQLServerDriver

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

Continue to "Step 13 - Repository Import" on the next page.

Step 13 - Repository Import

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

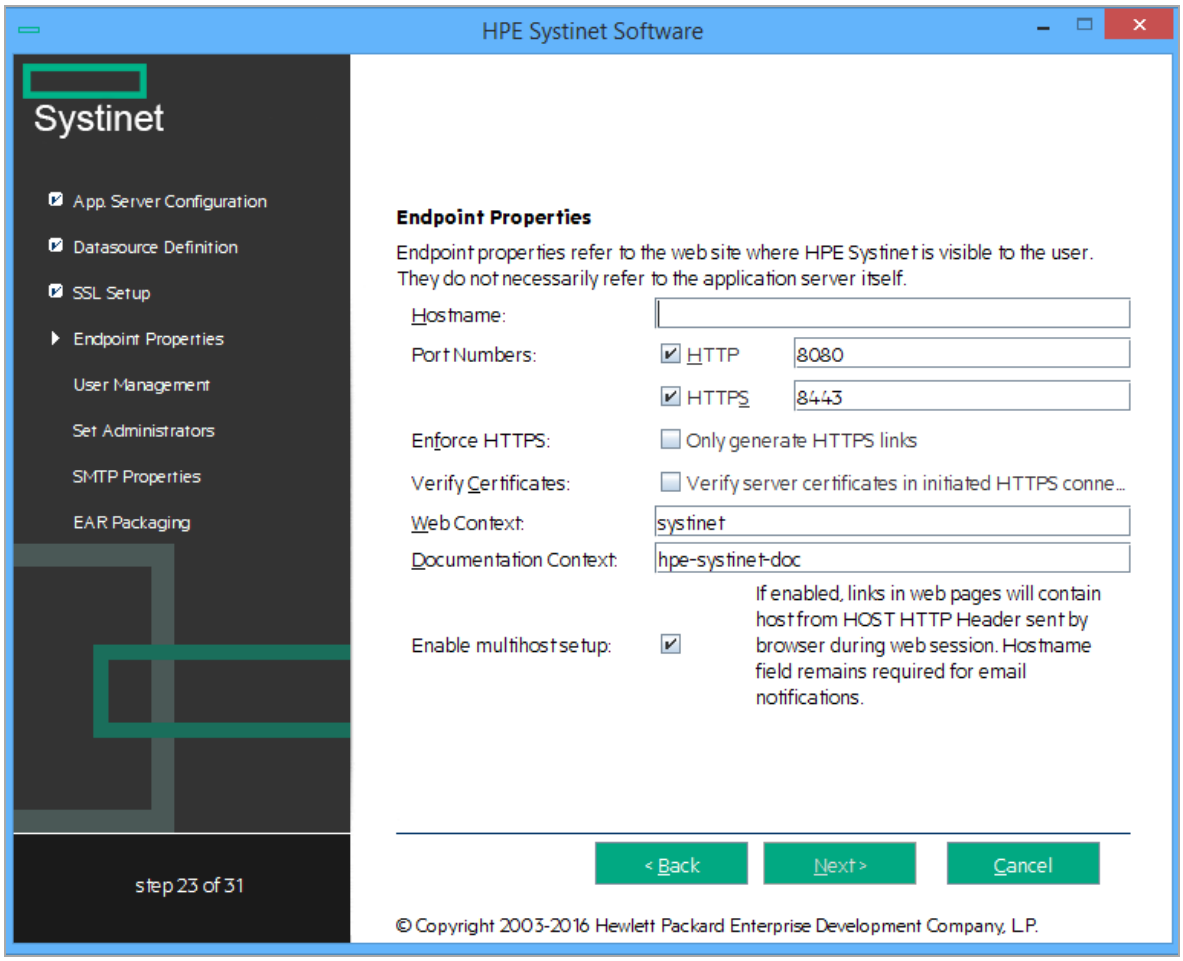
  > **Note:** The compliance status of artifacts included in the demo data does not reflect their initial status as the import does not contain any policy validation data. Regenerate the validation data manually or allow the automatic validation task to regenerate it.

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

Click **Next** to validate the data image and continue to "Step 14 - Endpoint Properties" on the next page.

Step 14 - Endpoint Properties

In the Endpoint Properties page, specify the endpoint properties:



1. Enter the **Hostname**.
   - For integration with CA Single Sign On, set the endpoint to the proxy server integrated with CA Single Sign On.
   - 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:** 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.

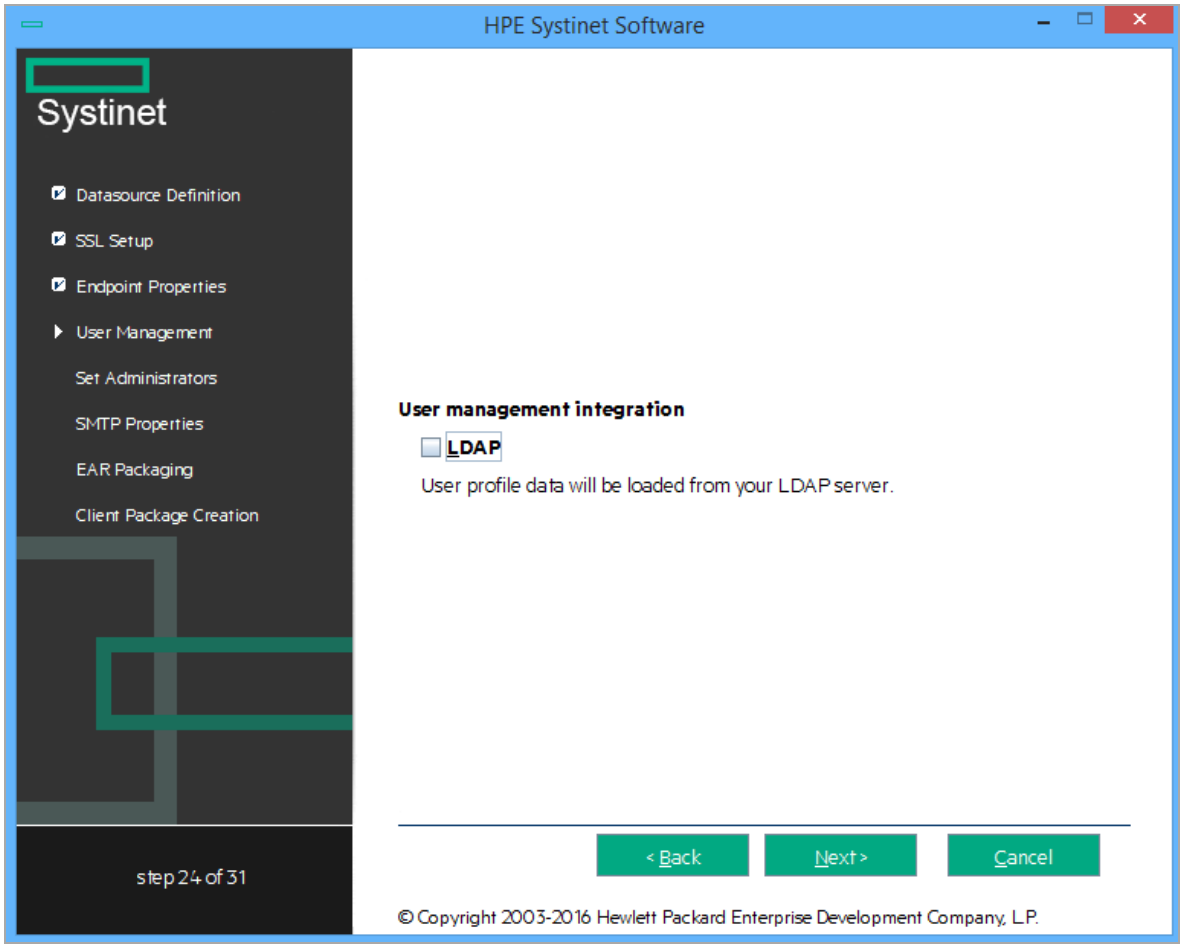
4. (Optional) Select **Verify Certificates** if you want the server certificates to be verified in initiated HTTPS connections.
5. Use the default **Web Context**: **systinet**.
6. Use the default **Documentation Context**: **hpe-systinet-doc**.
7. (Optional) Select **Enable multihost setup** to use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

   Refer "How to Configure HPE Systinet with a Proxy Server" on page 31.

Click **Next** to continue to "Step 15 - User Management Integration" below.

Step 15 - User Management Integration

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



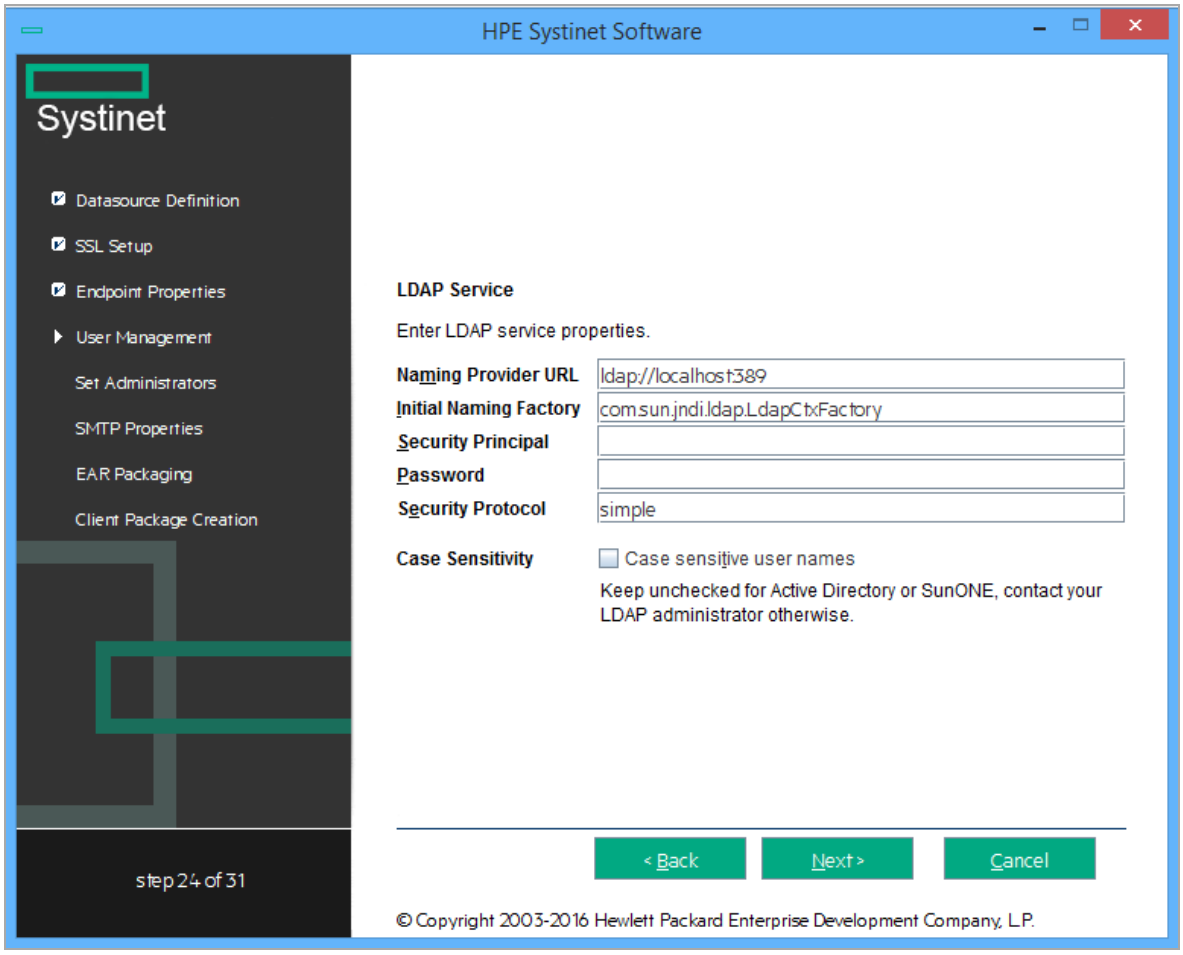
- Select **LDAP** if you want to integrate with an LDAP server account store.
- Do not select **LDAP** if you want to store accounts in your database.

If you selected LDAP, click **Next** to continue to "LDAP Service Properties" below.

If you did not select LDAP, click **Next** to continue to "Step 16 - System Email Configuration" on page 65.

LDAP Service Properties

In the LDAP Service page, set the following LDAP connection parameters, credentials, and case-sensitivity properties:



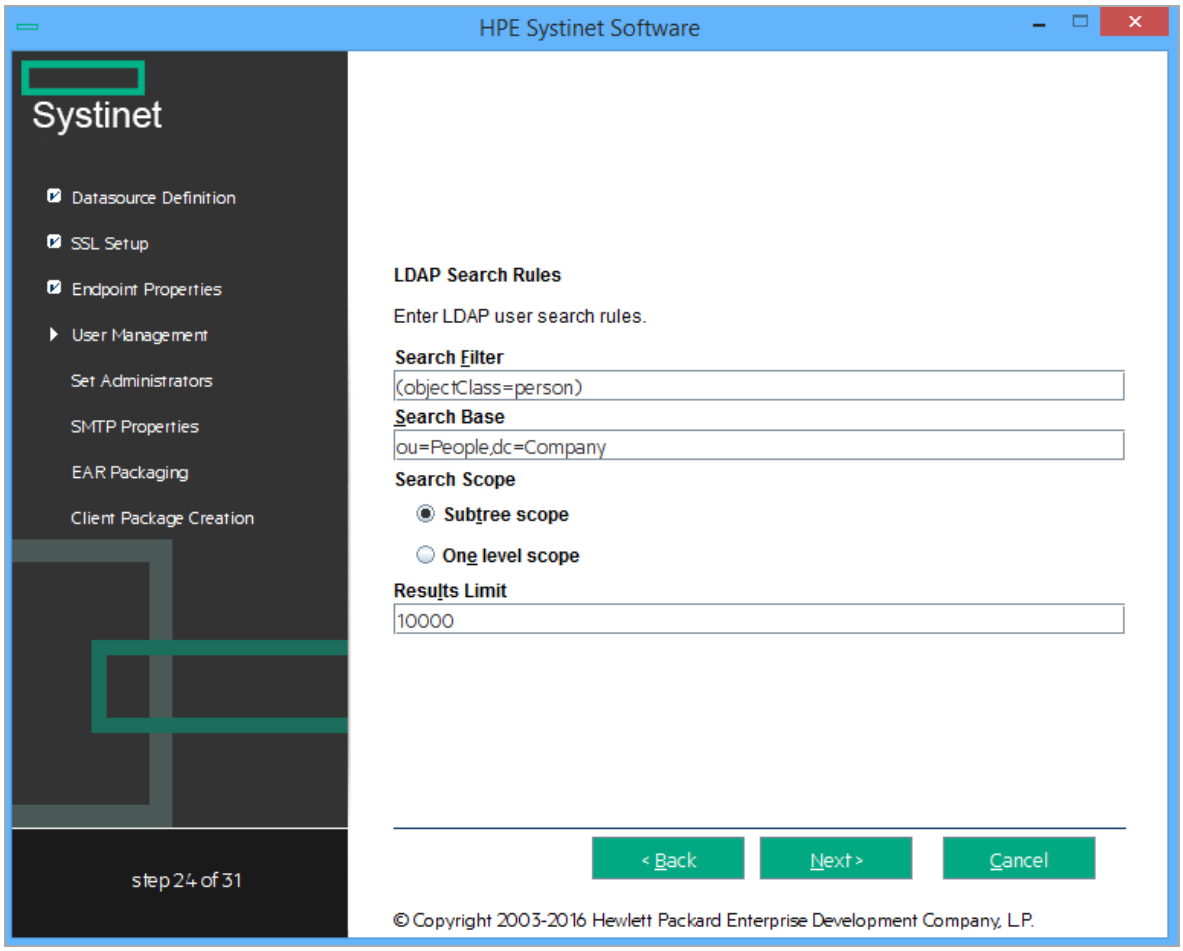
LDAP Service Properties

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.
Security Protocol	Keep the default.
Case Sensitivity	When checked, sets all user names to be case sensitive. The default for HPE Systinet logins is case-insensitive. **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 search rule properties:



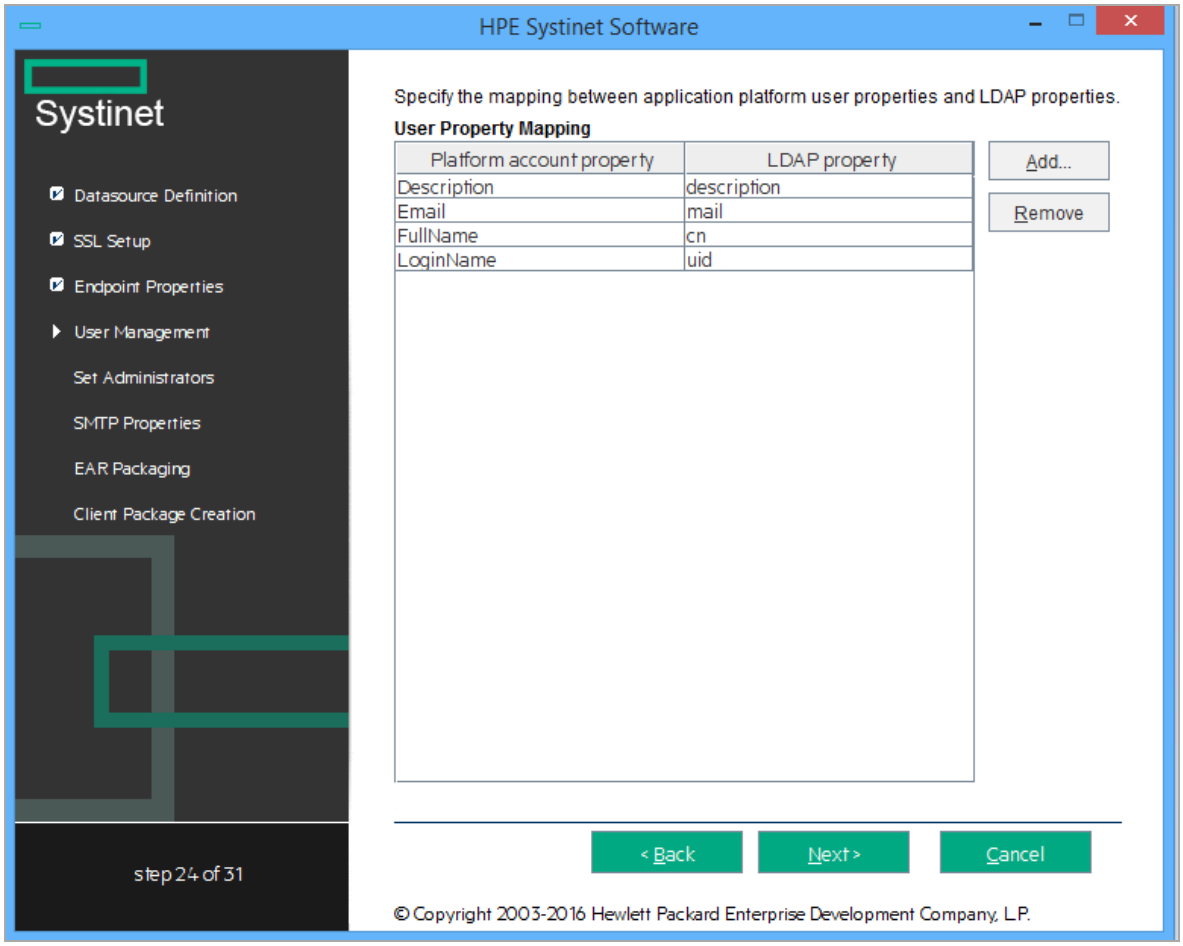
LDAP Search Rules Properties

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	• Subtree Scope: The search base and all its sub-nodes are searched. • 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.
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" on the next page.

LDAP User Properties Mapping

In the User Property Mapping page, use **Add** and **Remove** to set the user 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:

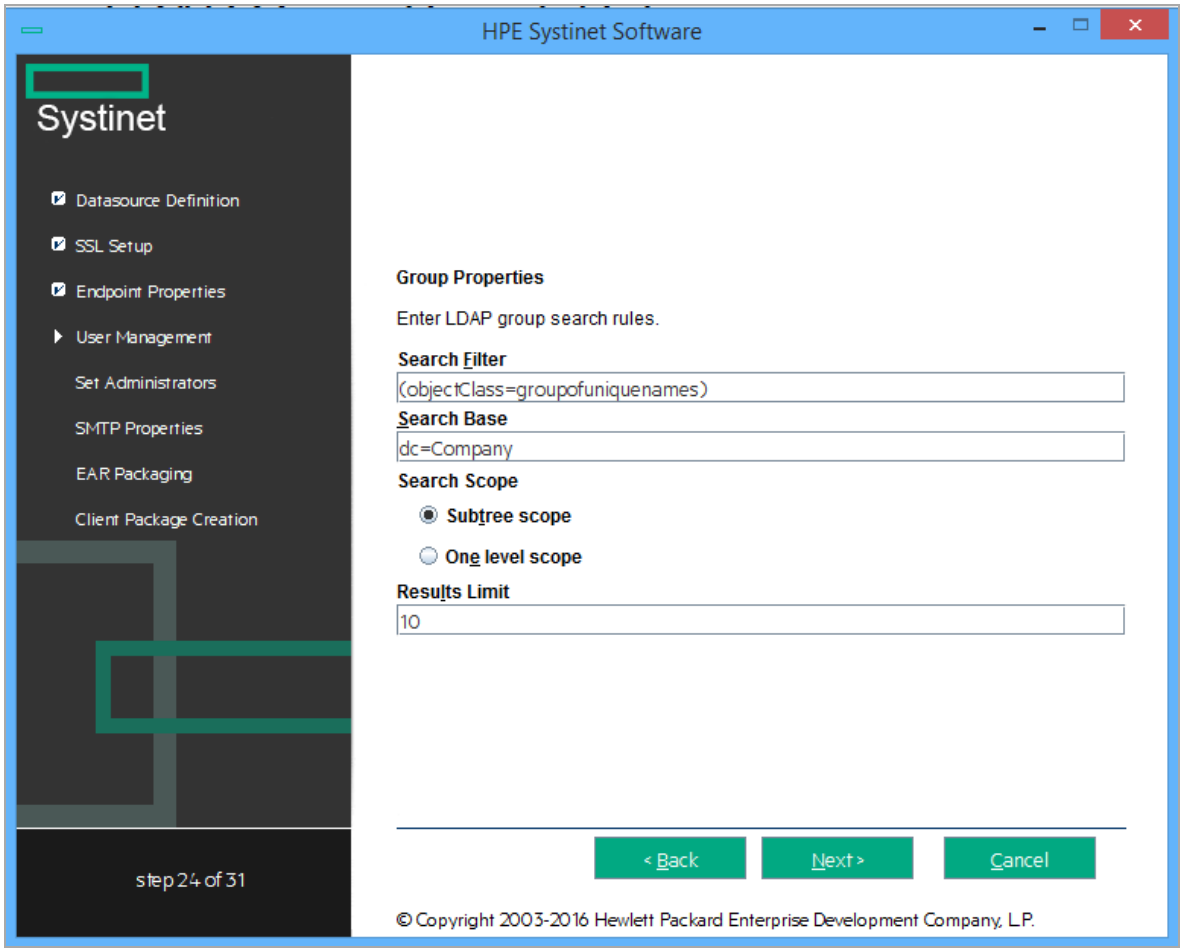
```
java.lang.String Email
java.lang.String Description
java.lang.String LanguageCode
java.lang.String Phone
java.lang.String AlternatePhone
java.lang.String Address
java.lang.String City
java.lang.String Country
```

> **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" below.

LDAP Group Search Rules

In the Group Properties page, enter the following group search rules properties:



LDAP Group 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.

LDAP Group Search Rules Properties, continued

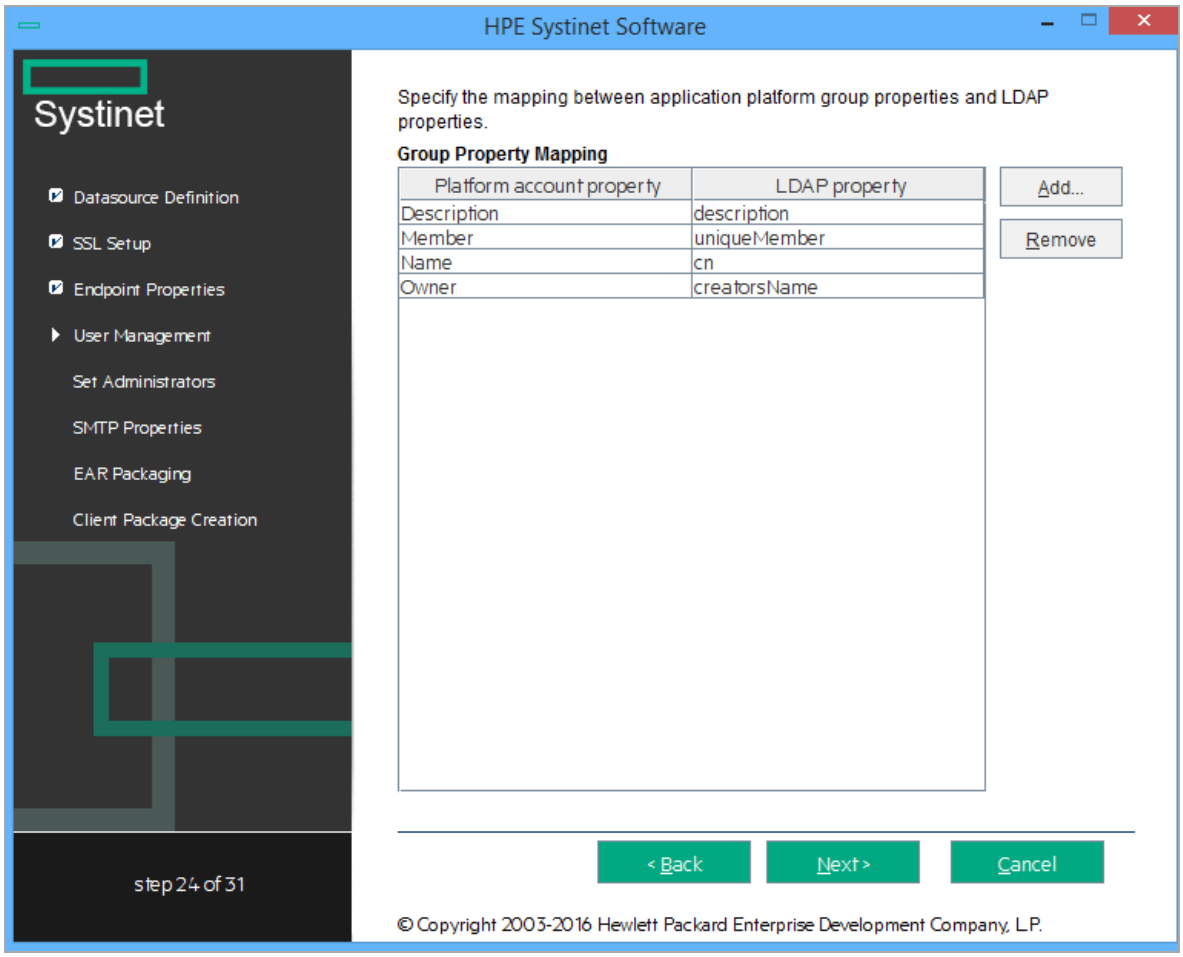
Property	Description
Search Scope	• Subtree Scope: The search base and all its sub-nodes are searched. • One-level Scope: Only direct sub-nodes of the search base (entries one level below the search base) are searched. The base entry is not included in the scope.
Results Limit	Number of items returned 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 group property mappings. between application user properties and LDAP properties.

The properties to map are: **Description**, **Member**, **Name**, and **Owner**.



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:

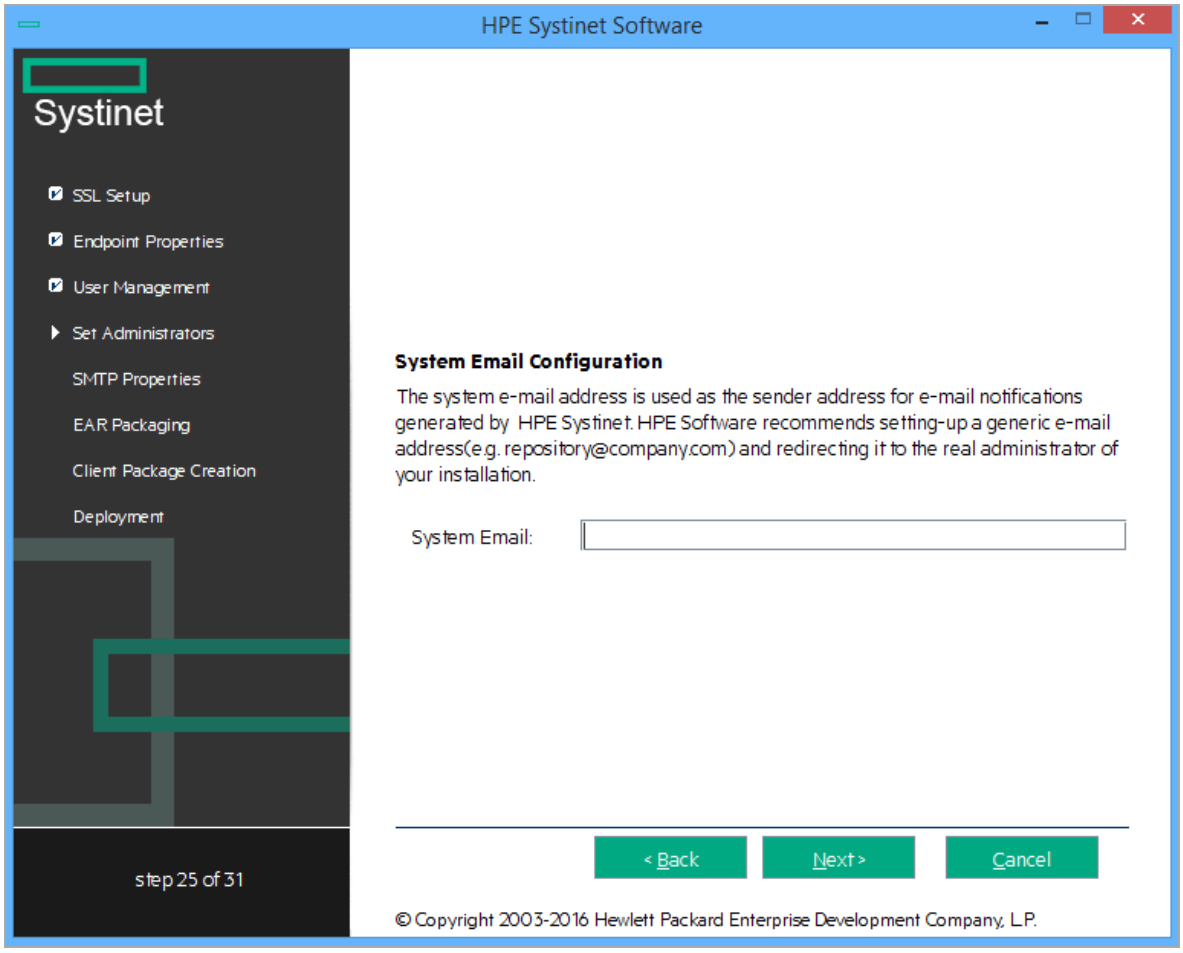
```
java.lang.string Owner
java.lang.String Description
```

> **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 16 - System Email Configuration" on the next page.

Step 16 - System Email Configuration

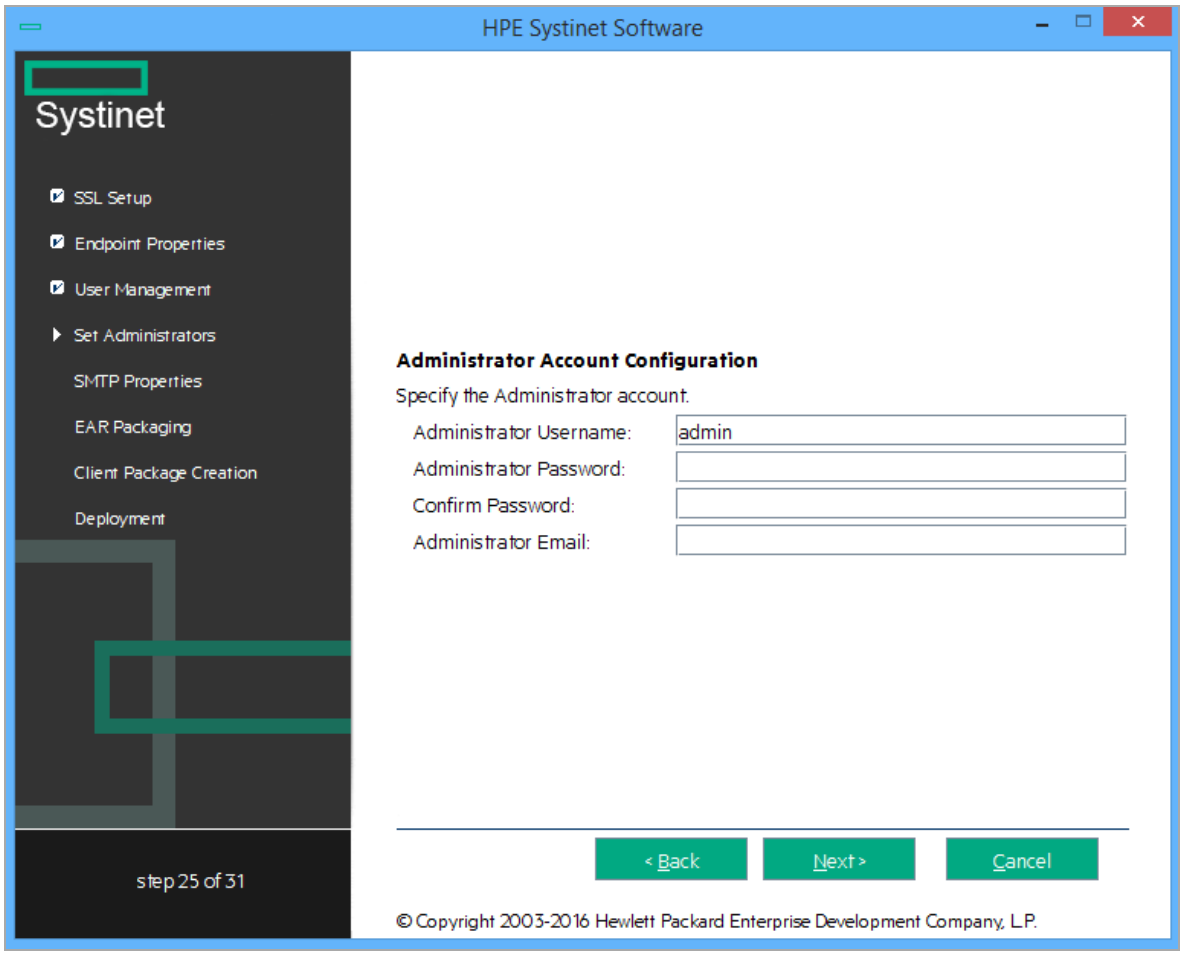
Enter the system mail account to be used as the source of automatic notification mails and system messages.



Click **Next** to continue to "Step 17 - Administrator Account Configuration" below.

Step 17 - Administrator Account Configuration

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



1. Enter the **Administrator Username**.

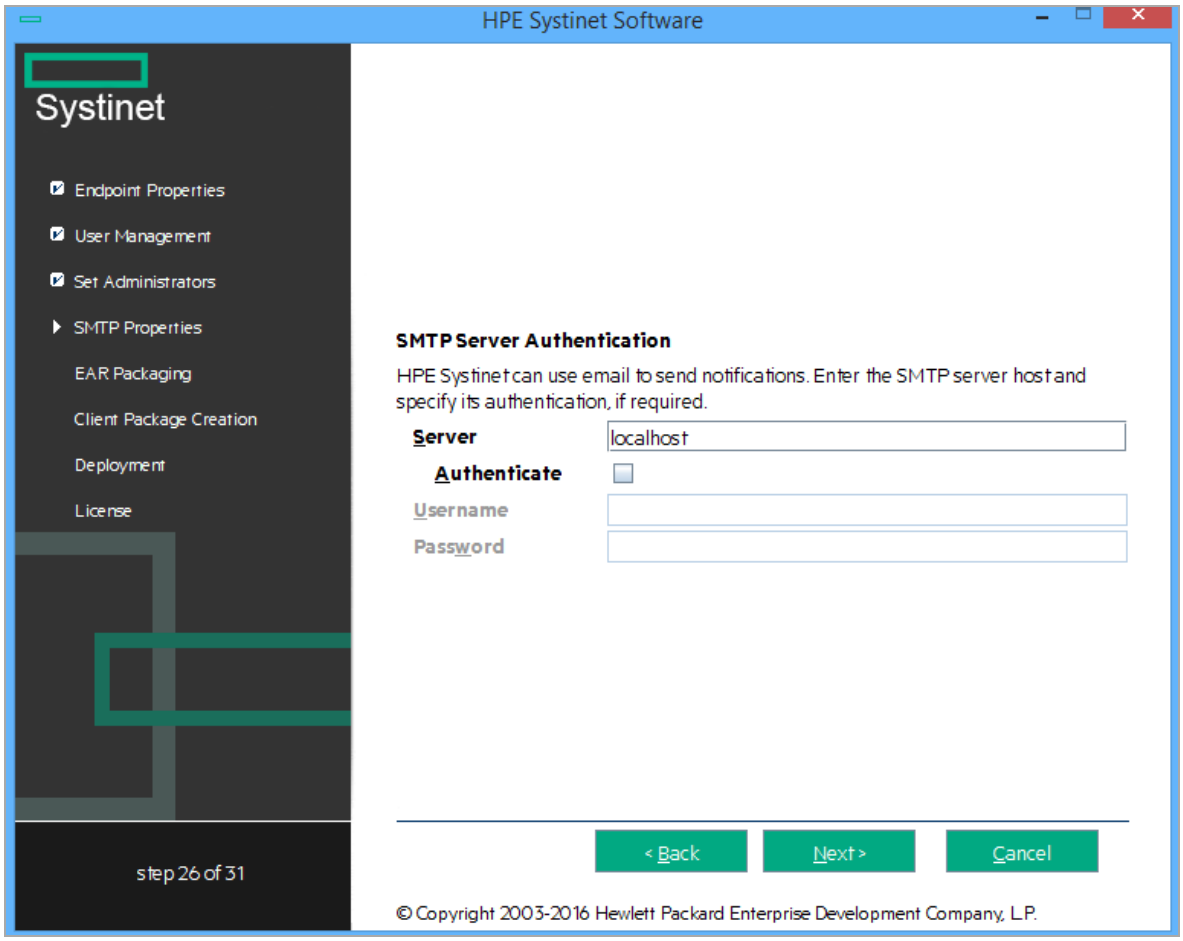
> **Note:** The administrator login name must be valid for the selected application server instance. The user with the specified name becomes an HPE Systinet administrator. For JBoss the specified administrator account is automatically created.

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

Click **Next** to continue to "Step 18 - SMTP Server Authentication" below.

Step 18 - SMTP Server Authentication

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

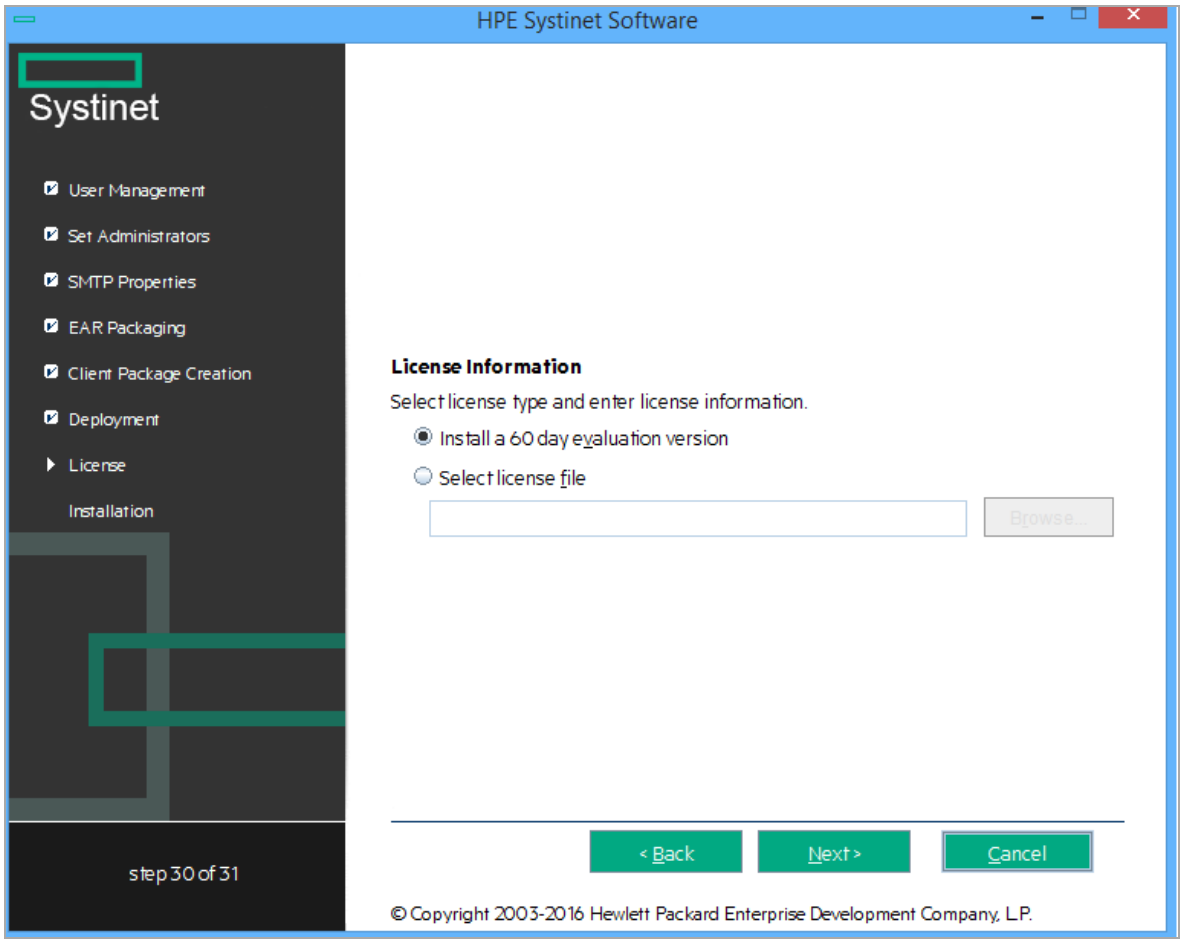


To authenticate, select **Authenticate** and enter the SMTP server credentials.

Click **Next** to create the client package and continue to "Step 19 - License Information" below.

Step 19 - License Information

In the License Information page set which license to use.



Do one of the following:

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

> **Note:** The administrator can change the license at a later date. For details, see *License Management* in *HPE Systinet Administration Guide*.

Click **Next** to continue to "Step 20 - Confirmation" below.

Step 20 - Confirmation

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

Continue to "Step 21 - Installation Progress" on the next page.

Step 21 - Installation Progress

The Installation Progress page tracks 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.

Chapter 8: Advanced HPE Systinet Installation

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 HPE Systinet in console mode to the specified location. Normally used in conjunction with **-u**.

- **-s, --save-config *FILE***

  Execute the HPE Systinet Installation, but save the configuration to the specified file instead of installing HPE 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`.

You can also find them by running **java -jar hpe-systinet-10.04.jar --help**.

HPE Systinet supports the following installation scenarios for production environment:

Manual Database Deployment

The automatic database setup may not be suitable for production environment. In that case, HPE Systinet can be installed manually by a database administrator (database decoupled mode) as follows:

1. Execute the command `java -jar hpe-systinet-10.04.jar -a` to create database scripts.
2. Copy all files from `SYSTINET_HOME/sql` to database server and run `all.sql`.
3. Execute the command `SYSTINET_HOME/setup.bat|.sh -c` to finish the Systinet installation.

> **Note:** The manual database deployment is not supported for installing Systinet with PostgreSQL database.

Silent Installation

Installation through HPE Systinet installer wizard may not be suitable for production environment. In such a scenario and also when Graphical User Interface (GUI) is not available, you can perform a silent installation as follows:

1. Execute the command `java -jar hpe-systinet-10.04.jar -s my-env-properties.xml` to create a silent mode properties file. Enter all the required information as you would while running HPE Systinet Installer Wizard.

   Upon completion there will be a `my-env-properties.xml` file created in the working directory.
2. Copy the `.jar` file along with the `my-env-properties.xml` file on the server, where the silent mode installation is to take place.
3. Edit the `my-env-properties.xml` file to match your target environment.
4. Execute the command **`java -jar hpe-systinet-10.04.jar -u my-env-properties.xml -i <SYSTINET_HOME>`** (No GUI required) to start the silent installation.

> **Note:** You may need to change the value `shared.as.jboss.location` in the `my-env-properties.xml` file to match the new **SYSTINET_HOME** directory. The **SYSTINET_HOME** directory must be empty.

Chapter 9: Configuration

After installation, deployment environments may require additional configuration.

For details, see the following sections:

Set Up CA Single Sign On Integration

You can configure HPE 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 CA Single Sign On 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 **CA Single Sign On Setup**, and click **Next**.
4. In the CA Single Sign On Setup page, select **Enable CA Single Sign On 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 HPE Systinet EAR file as described in the appropriate sections for each application server.

Enable Full-Text Search in HPE Systinet

You can enable full-text search in HPE Systinet as follows:

- "Enable Full-Text Search in MSSQL" below
- "Enable Full-Text Search in Oracle" on page 75

> **Note:** The full-text search is not applicable for PostgreSQL.

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 HPE 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 HPE recommends creating a new one for independent management purposes.

For more details, see http://msdn2.microsoft.com/en-us/library/ms189520.aspx.

3. Do one of the following:
   - To create a full-text index that is synchronized immediately after any data changes, execute the following command:

```
sqlcmd -U <user> -P <password> -d <database>
CREATE FULLTEXT INDEX ON ry_resource(
  m_extensions TYPE COLUMN m_extensions_fe LANGUAGE 0x0,
  data TYPE COLUMN data_fe LANGUAGE 0x0)
KEY INDEX pk_resource ON ry_resource_ftsc WITH CHANGE_TRACKING AUTO
go
```

   - To create a full-text index that is synchronized manually, execute the following command:

```
sqlcmd -U <user> -P <password> -d <database>
CREATE FULLTEXT INDEX ON ry_resource(
  m_extensions TYPE COLUMN m_extensions_fe LANGUAGE 0x0,
  data TYPE COLUMN data_fe LANGUAGE 0x0)
KEY INDEX pk_resource ON ry_resource_ftsc WITH CHANGE_TRACKING OFF, NO
POPULATION
go
```

   For more details, see http://msdn2.microsoft.com/en-us/library/ms187317.aspx.

   > **Note:** For specific language configuration, see https://msdn.microsoft.com/en-us/library/ms142507(v=sql.120).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 https://msdn.microsoft.com/en-us/library/ms176076(v=sql.110).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 be obtained by the following SQL command:

```
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 (FTS), you must create indexes and schedule their update. Use the Oracle **sqlplus** console. Connect to the database using the same credentials used during installation.

> **Caution:** FTS does not work for Oracle XE.

The procedure in commands is shown below 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 the 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://docs.oracle.com/cd/B28359_01/server.111/b28310/indexes003.htm#ADMIN11722.

> **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 HPE Systinet users with the stoplist, and a warning not to use these terms in full-text searches.

An example of commands to set up a stoplist on Oracle is shown in the following example:

Creating an Oracle Indexing Stoplist

```
call CTX_DDL.CREATE_STOPLIST('MyStoplist');
call CTX_DDL.ADD_STOPWORD('MyStoplist', 'a');
... Add a word that should not be indexed. Repeat the command for each word to be
excluded.

-- Include the DROP INDEX commands only if an index already exists.
DROP INDEX idx_ry_resource_meta;
DROP INDEX idx_ry_resource_data;
CREATE INDEX idx_ry_resource_meta on ry_resource(m_extensions) indextype is
ctxsys.context parameters
  ('filter ctxsys.null_filter section group CTXSYS.NULL_SECTION_GROUP STOPLIST
MyStoplist
    SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL') ;
CREATE INDEX idx_ry_resource_data on ry_resource(data) indextype is ctxsys.context
parameters
  ('filter ctxsys.null_filter section group CTXSYS.NULL_SECTION_GROUP STOPLIST
MyStoplist
    SYNC (EVERY "TRUNC(SYSDATE)+1") TRANSACTIONAL');
```

Create a custom LEXER preference:

By default, Oracle uses BASIC_LEXER preference to index whitespace delimited languages such as English, French, German, and Spanish. However, you can create a custom LEXER preference by using Oracle Text LEXER type to specify the language of the text to be indexed.

Below is an example of commands to create a custom LEXER which defines '_' as printjoins:

1. Drop the existing FTS indexes:

   ```
   DROP INDEX idx_ry_resource_meta;

   DROP INDEX idx_ry_resource_data;
   ```

2. Create a custom LEXER based on the BASIC_LEXER type:

   ```
   begin

   ctx_ddl.create_preference('custom_lexer','BASIC_LEXER');

   ctx_ddl.set_attribute('custom_lexer','printjoins','_');

   end;
   ```

3. Re-create the FTS indexes with the created custom_lexer:

   ```
   CREATE INDEX idx_ry_resource_meta ON ry_resource(m_extensions)

   INDEXTYPE IS CTXSYS.CONTEXT PARAMETERS

   ('lexer custom_lexer 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

('lexer custom_lexer FILTER CTXSYS.AUTO_FILTER');
```

For more details, refer to Oracle Text documentation.

Configure LDAP over SSL/TLS

You can configure LDAP over SSL (or TLS) with a directory server of your choice. HPE recommends that you first install HPE 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 HPE Systinet with an LDAP account provider.

HPE Systinet must not be running.

- **LDAP over SSL Without Client Authentication**

  In this case, only LDAP server authentication is required. This is the default configuration.

  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.url` property matches the name in the directory server certificate's subject common name (CN part of certificate's Subject). Otherwise you get an exception during startup of HPE Systinet. It informs you of a hostname verification error. The stacktrace contains the hostname that you must use.

- **LDAP over SSL With Mutual Authentication**

  HPE 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.

Configure HPE Systinet to Access Integration Server via HTTPS

To connect the HPE Systinet server with the integration servers using the HTTPS protocol, you need to import the certificate of that server into HPE Systinet truststore.

To import the certificate of integration server into HPE Systinet:

1. Access the integration server URL (HTTPS protocol) via web browser. The web browser asks for import of the server certificate.
2. Export the certificate from the web browser (for example: export the certificate into bsm.cert).
3. Run the following command:

   ```
   keytool -import -alias myBSMServer -file bsm.cert -keystore SYSTINET_
   HOME/conf/client.truststore
   ```

4. Restart Systinet server.
5. Login to Systinet as administrator and create an integration server using HTTPS protocol.

Configure Transaction Timeout

A typical JTA transaction might be started by EJBs or a JMS session in Systinet. So, if the duration of these transactions exceeds the specified timeout setting, the transaction service rolls back the transactions automatically.

For long running tasks, you can increase the transaction timeout by modifying the application server configuration at `SYSTINET_HOME/jboss/standalone/configuration/standalone-full.xml` (the default is 300 seconds).

```
<subsystem xmlns="urn:jboss:domain:transactions:1.5">
    <core-environment>
        <process-id>
            <uuid/>
        </process-id>
    </core-environment>
    <recovery-environment socket-binding="txn-recovery-environment" status-
socket-binding="txn-status-manager"/>
    <coordinator-environment default-timeout="1200"/>
</subsystem>
```

Chapter 10: Applying Custom Extensions

HPE Systinet 10.04 contains significant changes to the architecture model. If you have customized extensions from earlier versions, follow the steps below to apply them to HPE Systinet 10.04.

To Apply Custom Assertion Extension:

1. Install HPE Systinet Workbench 10.04.
2. Create a new assertion project from existing extension.
3. Build the new assertion extension.
4. Apply the new assertion extension to HPE Systinet 10.04.

For details, see the *Assertion Editor Guide*.

To Apply Custom Taxonomy Extension:

1. Install HPE Systinet Workbench 10.04.
2. Create a new taxonomy project from existing extension.
3. Build the new taxonomy extension.
4. Apply the new taxonomy extension to HPE Systinet 10.04.

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 HPE Systinet 10.04. In the event of a conflict the old system taxonomy takes precedence.

To Apply Custom Model Extension:

1. Install HPE Systinet Workbench 10.04.
2. Create a new extension project from existing extension.
3. Build the new extension.
4. Apply the new extension to HPE Systinet 10.04.

For details, see the *Customization Editor Guide*.

> **Caution:** Custom Java code in old extensions must be reviewed.

To Apply Custom Report Extension:

1. Install HPE Systinet Workbench 10.04.
2. Create a new report project from existing extension.
3. Build the new report extension.
4. Apply the new report extension to HPE Systinet 10.04.

For details, see the *Report Editor Guide*.

Chapter 11: Starting HPE Systinet

After deployment, you must start HPE Systinet and apply final configuration as follows:

Starting HPE Systinet

To start HPE Systinet execute the following command : `SYSTINET_HOME/bin/serverstart.sh|.bat`

To access HPE Systinet UI, open the following URL in browser: `http(s)://host:port/context`

Enable Full-Text Search in HPE Systinet

To be able to use full-text searching it must be enabled in the HPE Systinet UI.

To enable FTS, see *Configuration Management > How to Manage Basic Configuration Options* in *HPE SystinetAdministration Guide*.

> **Note:** The full-text search is not applicable for PostgreSQL.

Turn on HPE Systinet Self-Test

The self-test is disabled by default.

To turn on, see *Configuration Management > Self-Test* in *HPE Systinet Administration Guide*.

Installing HPE Systinet License

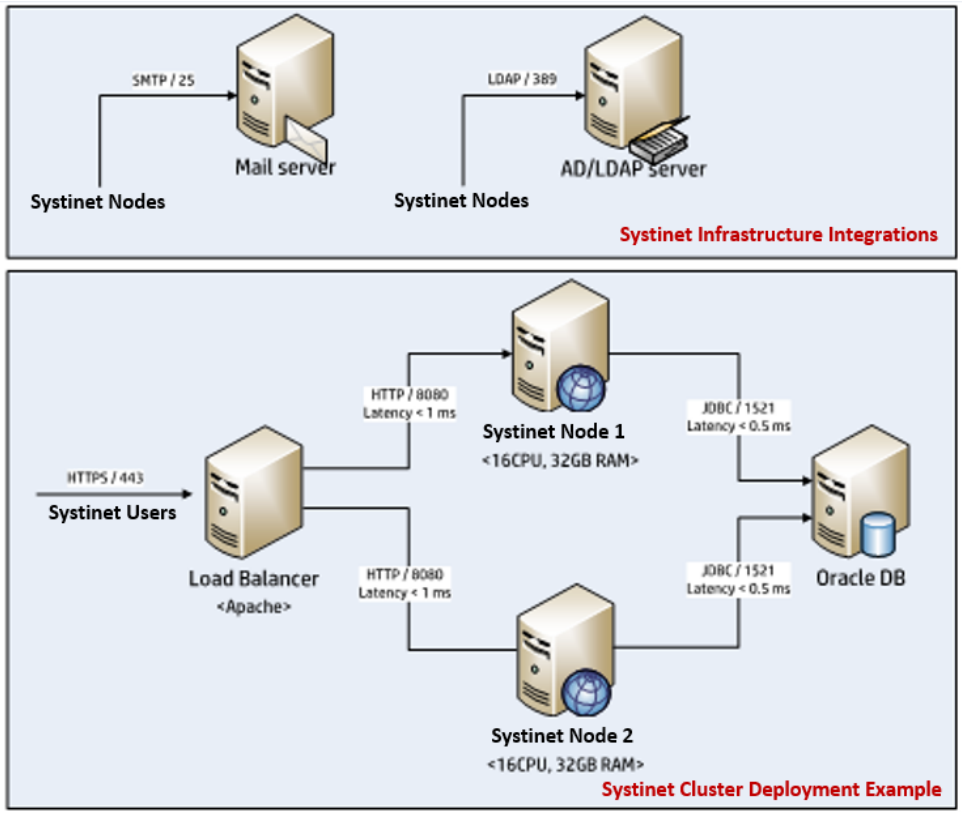
By default HPE Systinet includes a 60 day instant-on license.

To install or renew HPE Systinet license, see "License Management" in *HPE Systinet Administration Guide*.

Chapter 12: Setting JBOSS Clustering

This section guides you to setup HPE Systinet in JBoss Cluster environment. A diagrammatic representation is given below of how the set up looks once configured. The number of JBoss Servers (clustered node) can be changed.

JBoss Cluster deployment with two JBoss servers and the load balancer



Prerequisites

- Physical machines or VMs
- Systinet installation file
- HP JBoss 6.4.0 GA or JBoss AS 7.1.1
- mod_cluster 1.2.0 or newer

See " Install and Configure for JBoss Cluster" on the next page for the complete set up steps.

Install and Configure for JBoss Cluster

To start the JBoss Cluster setup for Systinet follow the instructions given below :

Primary Node: Install & Configure Systinet on JBoss EAP 6.4.0 GA or JBoss AS 7.1.1 (Other JBoss nodes are created based on the primary node)

1. Install Systinet following the steps given initially in this guide. If installed already, then just change the endpoints and ports by running the setup tool. When installing Systinet ensure the following:
   - The hostname is the hostname of the Load Balancer and not of installed the Systinet/JBoss
   - The HTTP port is "80" (listen port of Load Balancer)
   - The HTTPS port is "443" (secure port of Load Balancer)
   - Enable Jboss cluster properties
2. In Systinet, make following change to `configuration-properties.xml`:

```
<!--- Let Jboss generate standalone-full-ha.xml instead of standalone-
full.xml -->
    <property name="shared.as.jboss.configuration" value="standalone-full-
ha"/>
    <property name="install.jboss7.apacheProxy.setup" value="true"/>
    <property name="install.jboss7.web.instance-id" value="node1"/>
    <property name="install.jboss7.web.ajp.install" value="true"/>
    <!--- Load balancer name in the configuration of Load Balancer server
            'ManagerBalancerName mycluster' (httpd.conf), default value is
'mycluster'
     --/>
    <property name="install.jboss7.modcluster.balancer" value="mycluster"/>
    <property name="install.jboss7.modcluster.advertise" value="false"/>
    <!--- Load balancer address (IP:PORT ) , default port is '6666' --/>
    <property name="install.jboss7.modcluster.proxy-list"
value="127.0.0.1:6666"/>
    <property name="install.jboss7.modcluster.connector" value="ajp"/>
```

3. Build `start_cluster_node.bat` (Windows) or `start_cluster_node.sh` (Linux).
   - Copy the file `serverstart.sh/serverstart.bat` in *SYSTINET_HOME/bin*and rename to *`start_cluster_node.bat/start_cluster_node.sh`*.
   - Open the file `start_cluster_node.bat/start_cluster_node.sh`
   - Replace the line *CALL "%~dp0.\env.bat" (Window) or . "`dirname "${0}"`"/env.sh (Linux)* with the commands in the file `SYSTINET_HOME/bin/env.bat or env.sh`

> **Note:** Doing this removes the dependency of the file on `env.bat/env.sh`. Now, `start_cluster_node.bat/start_cluster_node.sh` can be copied anywhere.

- Change the command to start JBoss server.

  On Windows, change:

  ```
  CALL "%JBOSS_HOME%\bin\standalone.bat" -Djboss.bind.address=0.0.0.0 --server-config=standalone-full.xml -Djboss.server.log.dir="%SOA_LOG_DIR%" %*
  ```

  To

  ```
  CALL "%JBOSS_HOME%\bin\standalone.bat" -server-config= standalone-full-ha.xml -b node_ip -Djboss.server.log.dir="%SOA_LOG_DIR%" %*
  ```

  On Linux, change:

  ```
  exec "${JBOSS_HOME}"/bin/standalone.sh -Djboss.bind.address=0.0.0.0 -server-config=standalone-full.xml -Djboss.server.log.dir="${SOA_LOG_DIR}" "$@"
  ```

  To

  ```
  exec "${JBOSS_HOME}"/bin/standalone.sh -server-config= standalone-full-ha.xml -b node_ip -Djboss.server.log.dir="${SOA_LOG_DIR}" "$@"
  ```

  > **Note:** + node_ip is the IP address of the JBoss clustered node.

Installation JBoss clustered nodes

4. Build another JBoss clustered node.
   - Copy *JBOSS_HOME* folder and `start_cluster_node.bat/start_cluster_node.sh` from primary node to the target clustered node
   - If the path of *JBOSS_HOME* is changed in the new node, you must update *JBOSS_HOME* variable in the file `start_cluster_node.bat/start_cluster_node.sh`
   - Update node IP address (-b) to IP address of the new node.
   - If the new clustered node is on the same physical/virtual machine, you must add the parameter "*-Djboss.socket.binding.port-offset*" to change port number of the new JBoss instance.

     For example:

- *Djboss.socket.binding.port-offset=100 for second node*
- *Djboss.socket.binding.port-offset=200 for third node*

◦ Open the file *JBOSS_HOME/standalone/configuration/standalone-full-ha.xml* and change the instance-id in the tag:

```
<subsystem xmlns="urn:jboss:domain:web:2.2" default-virtual-server="default-host"
native="false" instance-id="node2">
```

◦ Delete the following folders (if there) to avoid warning message about duplicate node ID and others.

- *JBOSS_HOME/standalone/data*
- *JBOSS_HOME/standalone/log*
- *JBOSS_HOME/standalone/tmp*

5. Repeat step 4 if you want to setup more than two JBoss clustered nodes.

Installation & configuration apache + mod_cluster (Load Balancer)

6. This instructs you to install apache + mod_cluster on Linux. For other OS, search for the required information on the respective OS sites and execute accordingly.

   For Linux:

   ◦ Download *mod_cluster 1.2.0 final* for Linux at http://downloads.jboss.org/mod_cluster//1.2.0.Final/mod_cluster-1.2.0.Final-linux2-x64-ssl.tar.gz.

   For Windows 64 bit:

   ◦ Go to http://downloads.jboss.org/mod_cluster//1.2.6.Final/windows/mod_cluster-1.2.6.Final-windows-x86-ssl.zip and unzip it to *LB_HOME* folder.

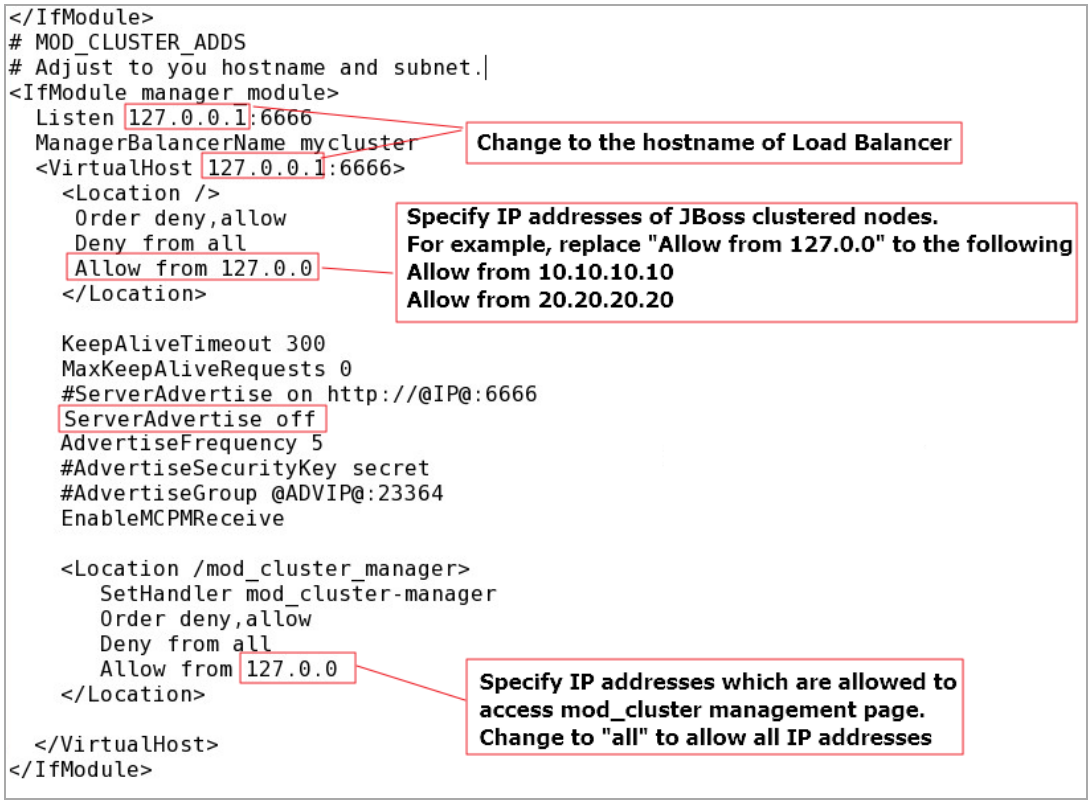
7. Configure the file *httpd.conf* of mod_cluster

   ◦ Copy *httpd.conf.in* from *LB_HOME/conf/default* to *LB_HOME/conf* and rename it to *httpd.conf*.

   ◦ Open the file, uncomment Servername, set it to the hostname of the Load Balancer. Keep the port as 80.

   > **Note:** If you change this Server name and port, you have to change endpoint of Systinet. Refer Step 1.

- Modify *mod_cluster* part as in the image below.




```
</IfModule>
# MOD_CLUSTER_ADDS
# Adjust to you hostname and subnet.
<IfModule manager_module>
  Listen 127.0.0.1:6666
  ManagerBalancerName mycluster
  <VirtualHost 127.0.0.1:6666>
    <Location />
     Order deny,allow
     Deny from all
     Allow from 127.0.0.0
    </Location>

    KeepAliveTimeout 300
    MaxKeepAliveRequests 0
    #ServerAdvertise on http://@IP@:6666
    ServerAdvertise off
    AdvertiseFrequency 5
    #AdvertiseSecurityKey secret
    #AdvertiseGroup @ADVIP@:23364
    EnableMCPMReceive

    <Location /mod_cluster_manager>
       SetHandler mod_cluster-manager
       Order deny,allow
       Deny from all
       Allow from 127.0.0
    </Location>

  </VirtualHost>
</IfModule>
```

Starting and Stopping Systinet on Jboss Cluster nodes

8. To start and stop Systinet on Jboss Cluster nodes, simply run the created file *start_cluster_node.bat/start_cluster_node.sh*
9. To stop Systinet on JBoss clustered nodes, run the command below:
   - *JBOSS_HOME/bin/jboss-cli.sh –connect command=:shutdown $** (Linux)
   - *JBOSS_HOME\bin\jboss-cli.bat --connect command=:shutdown %** (Windows)

Starting and Stopping mod_cluster (Load Balancer)

10. To start Load Balancer:
    - On Linux:

      cd /opt/jboss/httpd/sbin

      ./apachectl start

- On Windows:

  LB_HOME/bin/httpd.exe

11. To stop Load Balancer:

    Run the following commands:

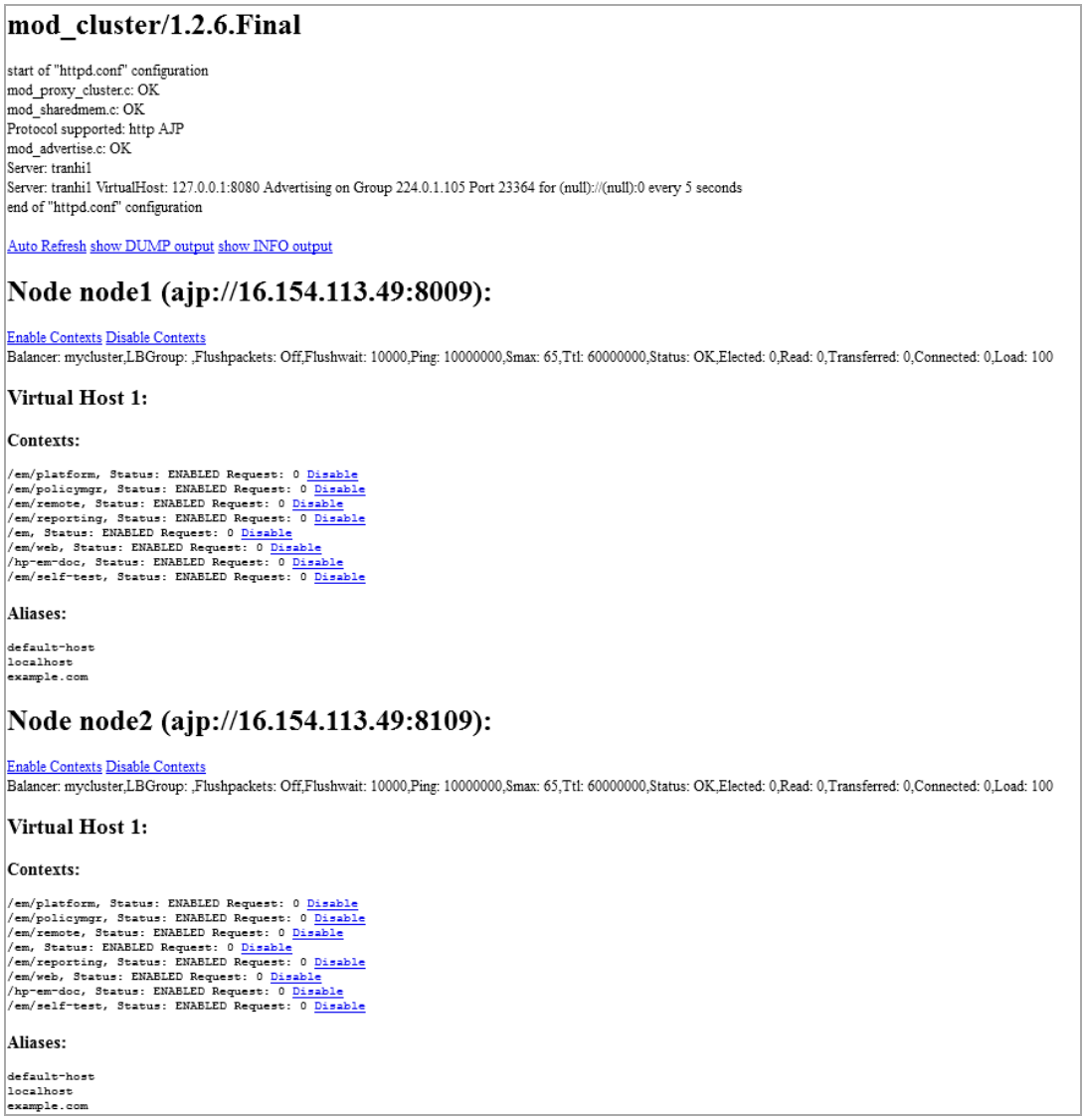
    - *cd /opt/jboss/httpd/sbin*
    - *./apachectl stop*

Verification and Testing High Availability

12. Verification :
    - Start all JBoss clustered nodes and the Load Balancer.
    - Open the web browser and access Systinet at http://load-balancer-hostname/EM_Context.
    - Open the web browser and access the *mod_cluster* management page http://load-balancer-hostname:6666/mod_cluster_manager.

      > **Note:** Chrome considers 6666 to be an unsafe port. Hence, if you are using this port, either use another web browser, or read the article how-to-fix-err-unsafe-port-error-on-chrome to fix it.

You will see the following result:



mod_cluster/1.2.6.Final

start of "httpd.conf" configuration
mod_proxy_cluster.c: OK
mod_sharedmem.c: OK
Protocol supported: http AJP
mod_advertise.c: OK
Server: tranhi1
Server: tranhi1 VirtualHost: 127.0.0.1:8080 Advertising on Group 224.0.1.105 Port 23364 for (null)://(null):0 every 5 seconds
end of "httpd.conf" configuration

Auto Refresh show DUMP output show INFO output

Node node1 (ajp://16.154.113.49:8009):

Enable Contexts Disable Contexts
Balancer: mycluster,LBGroup: ,Flushpackets: Off,Flushwait: 10000,Ping: 10000000,Smax: 65,Ttl: 60000000,Status: OK,Elected: 0,Read: 0,Transferred: 0,Connected: 0,Load: 100

Virtual Host 1:

Contexts:

/em/platform, Status: ENABLED Request: 0 Disable
/em/policymgr, Status: ENABLED Request: 0 Disable
/em/remote, Status: ENABLED Request: 0 Disable
/em/reporting, Status: ENABLED Request: 0 Disable
/em, Status: ENABLED Request: 0 Disable
/em/web, Status: ENABLED Request: 0 Disable
/hp-em-doc, Status: ENABLED Request: 0 Disable
/em/self-test, Status: ENABLED Request: 0 Disable

Aliases:

default-host
localhost
example.com

Node node2 (ajp://16.154.113.49:8109):

Enable Contexts Disable Contexts
Balancer: mycluster,LBGroup: ,Flushpackets: Off,Flushwait: 10000,Ping: 10000000,Smax: 65,Ttl: 60000000,Status: OK,Elected: 0,Read: 0,Transferred: 0,Connected: 0,Load: 100

Virtual Host 1:

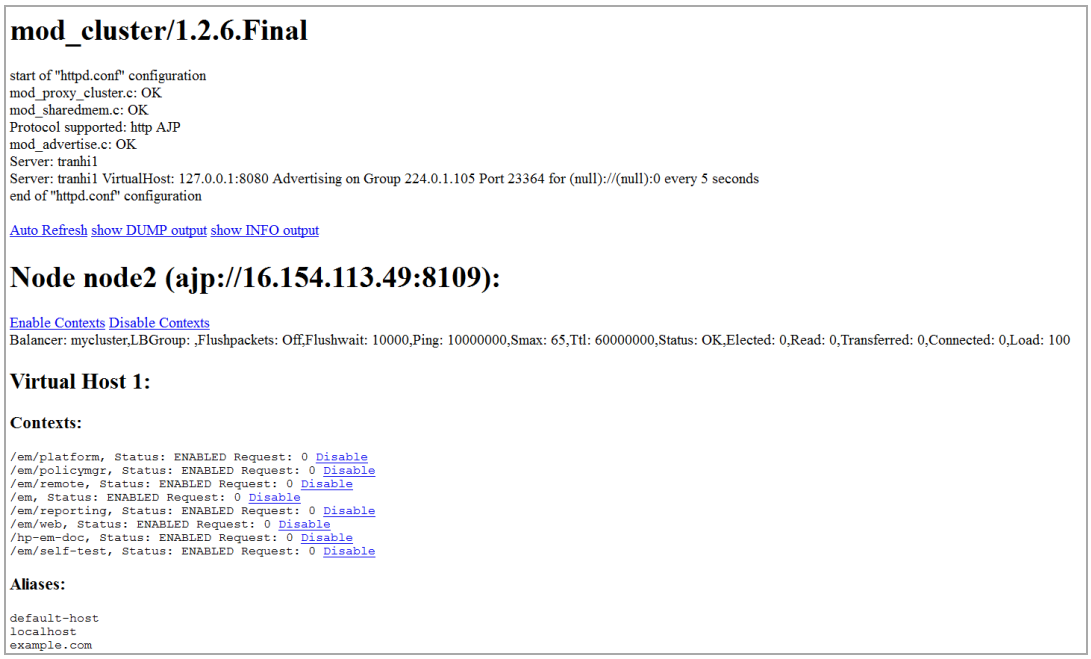
Contexts:

/em/platform, Status: ENABLED Request: 0 Disable
/em/policymgr, Status: ENABLED Request: 0 Disable
/em/remote, Status: ENABLED Request: 0 Disable
/em, Status: ENABLED Request: 0 Disable
/em/reporting, Status: ENABLED Request: 0 Disable
/em/web, Status: ENABLED Request: 0 Disable
/hp-em-doc, Status: ENABLED Request: 0 Disable
/em/self-test, Status: ENABLED Request: 0 Disable

Aliases:

default-host
localhost
example.com

13. Testing High Availability
    - Stop JBoss clustered node 1.
    - Open the web browser and access Systinet at http://load-balancer-hostname/EM_Context. Systinet server must be available as other clustered nodes are running.
    - Open the web browser and access the mod_cluster management page to check running nodes. You will see the following result:



mod_cluster/1.2.6.Final

start of "httpd.conf" configuration
mod_proxy_cluster.c: OK
mod_sharedmem.c: OK
Protocol supported: http AJP
mod_advertise.c: OK
Server: tranhi1
Server: tranhi1 VirtualHost: 127.0.0.1:8080 Advertising on Group 224.0.1.105 Port 23364 for (null)://(null):0 every 5 seconds
end of "httpd.conf" configuration

Auto Refresh show DUMP output show INFO output

Node node2 (ajp://16.154.113.49:8109):

Enable Contexts Disable Contexts
Balancer: mycluster,LBGroup: ,Flushpackets: Off,Flushwait: 10000,Ping: 10000000,Smax: 65,Ttl: 60000000,Status: OK,Elected: 0,Read: 0,Transferred: 0,Connected: 0,Load: 100

Virtual Host 1:

Contexts:

/em/platform, Status: ENABLED Request: 0 Disable
/em/policymgr, Status: ENABLED Request: 0 Disable
/em/remote, Status: ENABLED Request: 0 Disable
/em, Status: ENABLED Request: 0 Disable
/em/reporting, Status: ENABLED Request: 0 Disable
/em/web, Status: ENABLED Request: 0 Disable
/hp-em-doc, Status: ENABLED Request: 0 Disable
/em/self-test, Status: ENABLED Request: 0 Disable

Aliases:

default-host
localhost
example.com

- Stop other clustered nodes and conduct further tests if required.