Service Manager

Software Version: 9.50

For the supported Windows® and Linux® operating systems

Installation Guide

Document Release Date: November 2016

Software Release Date: October 2016

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

© 1994 - 2016 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.

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

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For a complete list of open source and third party acknowledgements, visit the HPE Software Support Online web site and search for the product manual called HPE Service Manager Open Source and Third Party License Agreements.

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 HPE Passport and to sign in. To register for an HPE Passport ID, click **Register for HPE Passport** on the HPE Software Support site or click **Create an Account** on the HPE 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 HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register for HPE Passport** on the HPE Support site or click **Create an Account** on the HPE 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

Introduction

This guide provides instructions on how to install and set up Service Manager from scratch.

If you are upgrading from an existing implementation of Service Manager, see the *Service Manager Upgrade Guide*, which is available in both HTML format from the Service Manager Help Center and PDF format from the HPE Software Support Online website.

Deployment architecture

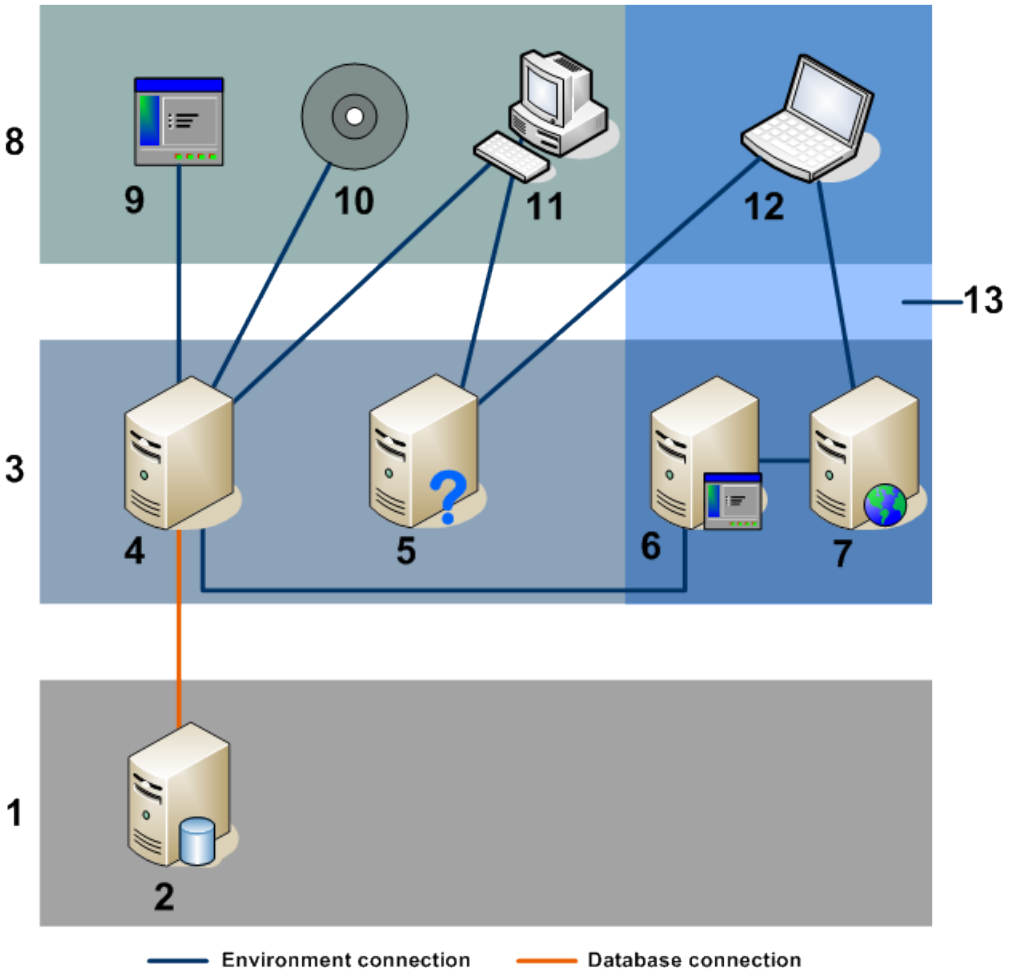
You can install Service Manager in a production environment or in non-production environments: development, test, and reporting environments. HPE recommends that you perform the installation in a development environment and then convert or push the installation to your production environment.

- Production environment: The production environment enables you to deploy your customizations and provide services to your user base. Most production environments run 24 hours a day and 7 days a week, support many simultaneous users, and process large numbers of transactions and requests. In a production environment, you typically install the components of Service Manager on dedicated servers to maximize system performance.
- Development environment: A development environment enables you to evaluate application features and customize your installation prior to deployment in a production environment. In a development environment, you typically install all Service Manager components on one test system with a limited number of users and data.
- Test environment: A test environment is an installation that mirrors your production environment where you can safely test performance, upgrades, and backup and restore procedures. In a test environment, you typically install Service Manager in the same configuration as your production environment.
- Reporting environment: A reporting environment is an installation that mirrors the data from your production environment that you use to generate and view reports. In a reporting environment, you typically install Service Manager to synchronize data with your production environment but limit the number of users that access the system.

Service Manager environment overview diagram

The Service Manager environment overview diagram describes the components of a Service Manager installation. The Service Manager table below provides a description for each component and lists whether the component is required or optional.

> **Note:** This diagram does not include the following Service Manager components: Solr Search Engine, Smart Analytics, Service Manager Collaboration, and HPE Identity Manager (IdM). Refer to their specific installation sections for their deployment architectures.



Item	Name	Required?	Description
1	**Database Tier**	Required	Consists of one or more supported RDBMS servers. Your Service Manager application data must reside in an external RDBMS.
2	RDBMS	Required	A relational database management system for storing Service Manager applications and data. Requires a 1 GB network connection to the Service Manager Server.
3	**Server Tier**	Required	Contains servers that provide or process data for clients. The server tier includes the Service Manager server, which runs the Service Manager applications and manages the connections between the client and web tiers to the database tier.
4	HPE Service Manager Server	Required	Manages connections between clients and the database tier.

Item	Name	Required?	Description
5	Help Server	Optional	A pre-configured web server that enables end users to access documentation from the Windows and web clients as well as directly from a web browser.
6	Web Applications Server	Optional	Offers Java applications and content for web clients.
7	Web Server	Optional	Provides HTTP or HTTPS content to web clients.
8	**Client Tier**	Required	Contains the applications and methods available for connecting to Service Manager.
9	Web Applications	Optional	Applications that can connect to or communicate with Service Manager through a web services API.
10	HPE Products	Optional	The suite of applications that can connect to or communicate with the Service Manager server. Temporary licenses are integrated with the Service Manager server. For a complete and up-to-date list of HPE integrations, see the Service Manager Compatibility Matrix on the HPE Software Integration Portal.
11	Windows Client	Required	Intended for Service Manager administrators or implementers. The Windows Client must be installed on a Windows workstation and requires a separate installation on each system that you want to connect to Service Manager. Each installation consumes a license. You must install at least one Windows Client, depending on the number of administrators and power users. The Windows Client enables you to design forms and work with the dbdict, capabilities that are not available to the Web client user. Requires a 100 MB network connection to Service Manager (SOAP over HTTP or HTTPS).
12	Web Client	Optional	Recommended for end users. A web client enables users to connect to the Service Manager server using a web browser, without needing to install any additional software on the user's system. You can install a web client once and then any number of web users can access Service Manager from a single URL without consuming a license. Service Manager provides three end user portals: Employee Self-Service (ESS), Service Request Catalog (SRC), and Service Manager Service Portal. You can select one of them according to your needs. You must install the web tier, SRC, or Service Manager Service Portal to support web clients. A web client can run on non-Windows platforms.

Item	Name	Required?	Description
			Note: There are scaling issues to consider: one web application server can only handle so many concurrent users before you need additional servers to handle the load.
13	Web Tier	Optional	Web application server and web server combinations that enable users to connect via a web browser. Third-party server software that provides the HTTP or HTTPS content to Service Manager web clients. Some web application servers also include built-in or bundled web servers.

Components

A Service Manager installation may include the following components:

- Core components
  - Server
  - Windows Client

    Install at least one Windows Client for the system administrator or group of power users. The Windows Client provides some system administration functionalities that are not available from the Web Tier client.
  - Web Tier

    The Web Tier client provides several views: Power User, Employee Self-Service (ESS), Accessible, and Self-Service Accessible.
  - Database
  - Applications
- Other components
  - Language Packs: A language pack is required when users need to use a localized version of Service Manager.
  - Smart Analytics or Solr Search Engine

    To enable Knowledge Management search, install either of them. If you have purchased Smart Analytics, do not use the Solr Search Engine. Additionally, once Smart Analytics is enabled, you can no longer use the Solr Search Engine.
  - Service Request Catalog (SRC) or Service Manager Service Portal

SRC or Service Manager Service Portal can be used as a replacement for the ESS user portal. Both of them are a user portal through which users can submit support requests, order catalog items, search knowledge, and complete surveys.

- Collaboration

  Collaboration is an instant messaging solution combining IT Collaboration and End User Chat.

- HPE Identity Manager (IdM) service

  The IdM service is required only if you want to enable SAML Single Sign-On for Service Manager.

JRE support

As of version 9.50, Service Manager (SM) adds the support of Open Java Development Kit (OpenJDK) for all SM components that require a JRE or JDK to work.

Important: Out-of-box, an OpenJDK JRE is bundled with the Windows Server, Windows Client, and Service Manager Service Portal so that you do not have to manually install a JRE for them. For the other components, including the Linux Server installation package, you need to manually install either an OpenJDK JRE or Oracle JRE.

You have the option to use either Oracle JDK or OpenJDK with Service Manager. For the supported versions of Oracle JRE and OpenJDK JRE, see the *Service Manager Support Matrix*.

JRE bitness

For the Server (both Windows and Linux) and Windows Client: use 32-bit JRE.

For the rest of the components: use a JRE with the same bitness as the operating system.

How to use OpenJDK with Service Manager

Use OpenJDK with SM components as described in the following table.

Caution: Service Manager does not support enabling FIPS mode with OpenJDK. If you want to enable FIPS mode for Service Manager, use Oracle or IBM JDK as needed. For more information, see the "Configure Java for FIPS mode" topic in the Service Manager Help Center.

Component(s)	How to use OpenJDK
• Windows Server	An OpenJDK jre folder is already bundled with the components. No installation is required.

Component(s)	How to use OpenJDK
• Windows Client	
Linux Server	**Important:** For Red Hat Linux 7.1, the 32-bit OpenJDK cannot be installed by the yum command. You need to upgrade to version 7.2 or higher or use Oracle JDK. 1. Make sure your Linux host has Internet access. 2. Go to the SM Server installation directory, run the "`installOpenJDK.sh -i4sm`" command as a superuser (such as root). Running this script will install OpenJDK and the related 32-bit dependent libraries. This script will also install a “fontconfig” rpm that is required for exporting reports generated by the Service Manager Reports functionality. **Note:** If your Linux host has no Internet access, you can use 32-bit Oracle JDK. Alternatively, do the following to use OpenJDK: a. Install 32-bit OpenJDK by yourself. b. Update the JAVA_HOME environment variable to make it point to the OpenJDK jre directory. c. From the SM Server's RUN directory, run "`setupLink.sh jre`" as the owner of the Service Manager installation directory. This will create a symbolic link for the OpenJDK JRE.
• Web tier • SRC • Mobility Client	**Note:** If the web tier or Mobility Client is deployed on WebSphere, IBM JDK must be used instead. 1. Install an appropriate version of OpenJDK on the Tomcat host. You can download it from https://zulu.org/. 2. On the Tomcat host, update the JAVA_HOME variable to make it point to the OpenJDK.
Solr Search Engine	1. Install an appropriate version of OpenJDK according to the operating system bitness of the Tomcat host. You can download it from https://zulu.org/. 2. Update the JAVA_HOME variable on the Tomcat host to make it point to the OpenJDK.

How to use Oracle JDK with Service Manager

Note: Before you proceed, make sure that Oracle JDK or JRE is already installed on the corresponding system (SM Server, Windows Client, and so on).

Use Oracle JDK as described in the following table.

Component	How to use Oracle JDK
Windows Server	1. Rename the <SM Server installation path>\RUN\jre folder to create a backup copy. 2. Download an appropriate version of 32-bit Oracle JRE from the Oracle website. 3. Copy the Oracle jre folder to the SM Server's RUN folder.
Windows Client	1. Rename the Client's jre folder to create a backup copy. For example: C:\Program Files (x86)\HPE\Service Manager 9.50\Client\jre.bak 2. Download an appropriate version of Oracle JRE from the Oracle website. 3. Copy the Oracle jre folder to the <Service Manager installation path>\Client folder.
Linux Server	1. If there is an existing jre link or jre folder in the Server's RUN directory, remove it. 2. Update the JAVA_HOME environment variable to make it point to the Oracle JRE. 3. From the Server's RUN directory, run the "setupLinks.sh jre" command as the owner of the Service Manager installation directory. This will create a symbolic link for the Oracle JRE.
Web tier SRC Mobility Client	**Note:** If these components are deployed on WebSphere, you must use IBM JDK instead. 1. Install an appropriate version of Oracle JRE according to the operating system bitness of the Tomcat host. 2. Update the JAVA_HOME variable on the Tomcat host to make it point to the Oracle JRE.
Solr Search Engine	1. Install an appropriate version of Oracle JRE according to the operating system bitness of the Tomcat host. 2. Update the JAVA_HOME variable on the Solr Search Engine host to make it point to the Oracle JDK.

Recommended installation order

For new installations, the following order is recommended:

1. Prepare an RDBMS. For details, see "Prepare your RDBMS" on page 24.
2. Install the Service Manager Server, and load the applications and demo data. For details, see "Install the Service Manager Server" on page 35.
3. Install the Service Manager Windows Client. For details, see "Install the Service Manager Windows Client" on page 51.
4. Install the web tier. For details, see "Install the Service Manager web tier" on page 63.
5. Install the Service Manager language packs. For details, see "Install language packs" on page 76.

   > **Note:** The language packs are intended for new installations only. If you have already an old language pack installed on top of an existing installation, you must upgrade your applications by running the Upgrade Utility. The Upgrade Utility will upgrade both the applications and language packs at the same time.

6. Install other components as needed, including Service Manager Service Portal or SRC, Smart Analytics or Solr Search Engine, Mobile Applications Client, and Collaboration. For detailed steps, click the appropriate links under the **Install** node of the Service Manager Help Center.

For existing implementations, the following order is recommended:

1. Upgrade your RDBMS if needed.
2. Install the new Service Manager Server without loading the applications and demo data, and restore your old server configurations. For details, see "Install the Service Manager Server" on page 35.
3. Install the new Service Manager Windows Client. For details, see "Install the Service Manager Windows Client" on page 51.
4. Install the new Service Manager web tier, and restore your old configurations. For details, see "Install the Service Manager web tier" on page 63.
5. (Optional) Upgrade your applications to the new version. For more information, click the **Upgrade** node of the Service Manager Help Center.

   > **Note:** This will also upgrade the old language packs that are installed in your system.

> **Tip:** While it is possible to upgrade only the Service Manager Server and Clients to the new version, many of the new features are not supported by the old applications. To get the benefit of all the new features, you must upgrade to the latest Service Manager applications as well.

6. Install the new version of other components as needed, and restore their old configurations if any.

Support matrix

Before you proceed to the installation of Service Manager, visit the HPE Support Matrices website for the latest support matrix information for Service Manager.

The support matrix document describes the hardware and software requirements and the compatibility information of Service Manager components.

Download the Service Manager installation files

The Service Manager installation files are released as the packages described in the following table.

Package	Components
SM9.50-1.zip	• Server • Windows Client • Web Tier • Mobility Client • Service Request Catalog (SRC) • Service Manager Service Portal • Solr Search Engine and KM Import Utility • Application Upgrade Utility • Redistributables (open source and third-party license files) • Help Center • Documentation (in PDF format)
SM9.50-2.zip	• Smart Analytics • Collaboration • HPE Identity Manager (IdM) service • Crystal Reports
SM9.50-LaguagePack.zip	Service Manager language packs

Before you proceed, download the installation packages. For details, contact your HPE representative.

Prepare your RDBMS

The following recommendations assume the implementation of conventional database tuning and performance measures. Actual results may vary on a system-by-system basis, based on the tuning expertise available and hardware and software selections. These recommendations are intended only as a guide and should not be implemented on a production system without extensive testing.

A fully qualified database administrator should assist with this preparation.

> **Note:** HPE recommends that the Service Manager server be within reasonable proximity to the RDBMS. Utilizing a RDBMS for use with Service Manager Server over a WAN link is not recommended and will have negative impact on overall product performance.

Follow the instructions in this section to prepare your Relational Database Management System (RDBMS) prior to installing the Service Manager data.

> **Note:** Currently, only SQL Server and Oracle databases are supported for Service Manager.

Prepare a SQL Server database

To prepare a SQL Server database, follow these steps:

1. Meet general space requirements:

   Place all Service Manager data in one or more dedicated table spaces within a single SQL Server instance. These table spaces must contain Service Manager data only. Multiple instances consume more system resources than a single-instance solution.

   Allocate at least 1 GB of data space for a test system. The amount of space necessary for a production system depends on the amount of data that you need to store and your specific implementation.

2. Set the sorting of characters for localized systems and set the case sensitivity of the database.

   Service Manager supports both case-sensitive and case-insensitive Microsoft SQL server. To use Service Manager in case-insensitive mode, you must select a case-insensitive collation on the SQL Server before installing Service Manager. You can specify the desired case-sensitivity for sort order during the creation of the database. Set the SQL Server database to the desired collation when you create it. Service Manager automatically detects the settings.

- To run in case-sensitive mode, pick a collation that ends with _BIN, such as Latin1_General_BIN.
- To run in case-insensitive mode, pick a collation that ends with _CI_AS, such as Latin1_General_CI_AS.

MS SQL Server collation support

HPE Service Manager supports two types of collations :

- Those ending in some form of _BIN (binary)
- Those ending in some form of _CI_AS (case-insensitive, accent sensitive)

_BIN is used for case-sensitive collation, meaning both, comparisons (WHERE NAME="ADMINISTRATOR") and sorting (ORDER BY NAME) are case-sensitive. Collations ending in _CS_AS claim to be case-sensitive, but that only applies to comparisons. For sorting, they use a "dictionary order," which is essentially case-insensitive.

_CI_AS is the supported case-insensitive collation. It uses case-insensitive comparisons (WHERE NAME="AdMinIstrator") and case-insensitive sorting. Do not use _CI_AI since Service Manager has no concept of accent insensitivity.

The sort order becomes important in the case of a combined SQL/IR search. In that case, IR has to match its own results with the results returned by SQL, and for that it assumes binary or case-insensitive sorted order.

Note that such queries might take place even if you do not know about them. For example in the Service Catalog, when ordering, a user enters an IR query, but the RAD appends a long non-IR query to it. This results in a mixed query.

The other aspect of the collation is the code page. The code page defines the code page of VARCHAR columns, NVARCHAR are always in UTF-16. "General" refers to the American default Windows code page, Win 1252.

Service Manager supports the following SQL Server code pages:

Code page	Description
874	MS cp874 Thai
932	MS cp932 Japanese
936	MS cp936 Simplified Chinese
949	MS cp949 Korean
950	MS cp950 Traditional Chinese

Code page	Description
1250	MS cp1250 Central European
1251	MS cp1251 Russian, Bulgarian, Serbian
1252	MS cp1252 Latin/Western European
1253	MS cp1253 modern Greek
1254	MS cp1254 Turkish
1255	MS cp1255 Hebrew
1256	MS cp1256 Arabic
1257	MS cp1257 Estonian, Latvian, Lithuanian
1258	MS cp12578 Vietnamese

You can generate the list of all the code pages supported by Service Manager with the command, `sm -reportlanguages`. Only those code pages that start with "mswin" are used in the context of SQL Server.

If you are using an unsupported code page, you will see this warning in the log file: `W SQL Server uses a code page <nnn> unsupported by HPE Service Manager which retrieved codepage <nnnn>`.

> **Note:**
> If you have selected the **Use Unicode Data Type** option when configuring the Service Manager server, unicode sorting is used instead of collation sorting. For more information about the **Use Unicode Data Type** option, see "Install and configure the Service Manager Server " on page 41.

3. Create server connections. Every Service Manager thread, foreground, or background, requires a connection to your RDBMS. Service Manager background processors require 17 connections to run. Make sure that you allocate enough connections for all of your users. For additional information, refer to your RDBMS vendor documentation.
4. Create a login ID and password for Service Manager to use to connect to your database.

   Create a login ID and password for Service Manager to use to connect to your SQL Server database.

   The login must have CREATE/ALTER/DROP TABLE authority for the target database. The CREATE/ALTER/DROP TABLE authority is only required during installation and creation of new Service Manager tables, and only if you allow Service Manager to issue the DDL to create tables

and indexes. When Service Manager connects to your database using the login ID, tables are created in the default table space defined for that login ID.

> **Caution:** You must grant the DB account of the "sqllogin" SM parameter the privilege to create Stored Procedures and User Defined Functions.

5. Set up a connection to Service Manager:

   Service Manager connects to the database through your RDBMS client. To set up the connection between the Service Manager application server and your RDBMS, know the name of the database and the login ID and password required to connect to the database server that you created above. The Service Manager initialization file, sm.ini, must be present in the Service Manager server RUN directory.

   Set up connectivity to your SQL Server database

   Follow these connectivity rules when you set up the connection to your SQL Server:

   - Make sure that the database name you enter in the configuration tool corresponds to the ODBC Driver system data source.
   - Configure the ODBC Driver data source as a System DSN. Set it up to use the following settings:
     - SQL server authentication
     - ANSI quoted identifiers
     - ANSI nulls, paddings, and warnings
   - Do not create the system DSN by using a 64-bit ODBC administrator. When Service Manager is installed on a 64-bit Windows system, create the System DSN entry for the ODBC Driver by launching odbcad32.exe from: C:\WINDOWS\SysWOW64.

   > **Note:** As of version 9.50, HPE Service Manager supports SQL Server AlwaysOn for SQL Server 2012 and later versions. AlwaysOn is a high availability solution for SQL Server databases. To support SQL Server AlwaysOn, Service Manager Server introduces the sqlalwayson:1 parameter and the SQMSSQLAO.ODBC.DLL file. To use this functionality, you must install Microsoft ODBC Driver 11 for SQL Server (or a later version) and configure a System DSN with this ODBC driver. For more information, see the "Support of SQL Server AlwaysOn" topic in the Help Center.

6. Set time zones for reporting:

   If you plan to report on Service Manager data using your RDBMS tools, set the sqltz parameter in the sm.ini file. This is an optional parameter that the Service Manager server uses to control the

storing of date and time values in the RDBMS. This parameter defines the time zone to use as a base for all date and time values. The time zone is specified as the name of the time zone record in the Service Manager tzfile table. The default time zone is Greenwich/Universal (GMT). For more information about using the sqltz parameter, see the System Configuration Parameters topic in the Service Manager Help.

> **Caution:** If you use different time zone settings, the dates contained in reports made by your RDBMS utility may be inaccurate.

7. Set the Truncate Log On Checkpoint option for the target database on your SQL server. During initial system load, Service Manager places a high insert transaction load on your SQL server. Set the Truncate Log On Checkpoint option to prevent the transaction log from growing too large.
8. Create your SQL Server database with a code page that supports the character set of most of your data. To support multiple character sets, you can use Unicode data type (NVARCHAR, NCHAR, or NVARCHAR(MAX). For information about how to use the Unicode data type, see the *Configure the Service Manager Server* section below.

> **Caution:** If you choose a Western European code page, the system cannot store Eastern European or Asian characters in columns defined as VCHAR, CHAR, or TEXT data type. If you must store characters from different languages, consider using the Unicode data type, that is, NVARCHAR, NCHAR, or NVARCHAR(MAX).

Prepare an Oracle database

Oracle Transparent Application Failover (TAF) enables database clients to switch the connection to surviving nodes in an Oracle Real Application Cluster (RAC) without re-establishing the database connection or setting up necessary session properties in the event of a failure of an instance.

All supported Service Manager server versions perform similar session recovery operations within the application. When Service Manager detects a connection failure, it attempts to reestablish the connection, set up necessary session properties, and repeat the failed transactions. Service Manager retries the connection for one minute. If the database is in an Oracle RAC configuration, this should allow time for failover and reconnection to another available instance.

Since similar failover functionality is available within Service Manager, the product has not been modified to run in an Oracle TAF configuration.

> **Caution:** Using Service Manager in combination with Oracle TAF could cause connectivity issues. Do not run Service Manager in an Oracle TAF configuration.

To prepare an Oracle database, follow these steps:

1. Meet general space requirements:

   Place all Service Manager data in a dedicated table space within a single Oracle instance. This table space must contain Service Manager data only. Multiple instances consume more system resources than a single-instance solution.

   Allocate at least 1 GB of data space for a test system. The amount of space necessary for a production system depends on the amount of data that you need to store and your specific implementation.

2. Set the sorting of characters for localized systems.

   > **Note:** Setting the sorting of characters in Service Manager is dependent on the settings defined within the back-end database or client connections to these databases. Please check with your company's Database Administrator when setting up your Service Manager database to ensure you have the correct settings for the native language(s) that will be used within Service Manager.

   Database vendors provide different options for these settings and continue to add/modify settings for languages around the world. Refer to the technical documentation provided by the database vendor for more information and recommendations on the correct localization settings. For additional information, search the vendor documentation for the following terms.

   - Globalization Support
   - Oracle client installation globalization

3. Create server connections. Every Service Manager thread, foreground, or background, requires a connection to your RDBMS. Service Manager background processors require 17 connections to run. Make sure that you allocate enough connections for all of your users. For additional information, refer to your RDBMS vendor documentation.

4. Create a login ID and password for Service Manager to use to connect to your database.

   Create a login ID and password for Service Manager to use to connect to your Oracle server. When you log on to Service Manager, it creates a table in the default table space defined for that login ID. The login ID must have the following privileges:

   - Connect
   - Create, Alter, Drop a table
   - Create, Alter, Drop an index
   - Select on v_$parameter
   - Alter Session Privileges

You can provide these privileges to an Oracle user by using the following oracle statements:

```
create user <smadmin> identified by <smadmin> default
tablespace <users> quota unlimited on <users>;
grant connect, resource, select on v_$parameter to <smadmin>;
```

- CREATE/ALTER/DROP TABLE privileges are only required during installation and creation of new Service Manager tables if you allow Service Manager to issue the DDL to create tables and indexes.
- You must grant the DB account of the "sqllogin" SM parameter the privilege to create Stored Procedures and User Defined Functions.

5. Set the case sensitivity of the database.

   Service Manager supports case-insensitivity for Oracle 11.2.0.3 and later. For earlier versions of Oracle, Service Manager requires a case-sensitive database. Click the appropriate task below for instructions on setting case-sensitivity.

   Set case-sensitivity on a new Oracle database

   a. While creating a new Oracle instance, choose **All Initialization Parameters** and modify the parameters.

   b. Set the case-sensitivity for the NLS_SORT and NLS_COMP parameters:

      - For a case-sensitive database, set NLS_SORT and NLS_COMP to **BINARY**.
      - For a case-insensitive database, set NLS_SORT to **BINARY**_CI and set NLS_COMP to **LINGUISTIC**.

   c. In Service Manager, run the following SQL statement to verify that the parameters are in effect:

      ```
      select parameter, value from nls_instance_parameters;
      ```

   d. Make sure that the values for NLS_SORT and NLS_COMP match your selection in Step b.

   Change an existing case-sensitive Oracle database with Service Manager data to be case-insensitive

   a. Back up all Service Manager data.x

   b. Run the following command:

      ```
      sm -system_unload -system_directory:<path to where you want to store the
      Service Manager data unload files>
      ```

   c. Log in to Oracle as a sys admin user, and issue the following statements to set NLS_SORT to

BINARY_CI and NLS_COMP to **LINGUISTIC**:

```
alter system set NLS_SORT=BINARY_CI SCOPE=SPFILE;
alter system set NLS_COMP=LINGUISTI CSCOPE=SPFILE;
create pfile from spfile;
```

d. Shut down and restart the Oracle instance.

> **Note:** If you are running Oracle on parallel servers, be sure to replicate the parameter file to all instances of Oracle.

e. Drop all Service Manager tables.

f. In Service Manager, run the following SQL statement to verify that the parameters are in effect:

```
select parameter, value from nls_instance_parameters;
```

g. Make sure that the values for NLS_SORT and NLS_COMP match your selection in Step b.

h. Remove groupname, sqldebug, and any other debugging parameters from the sm.ini file, and then run the following command:

```
sm -system_load -system_directory:<path to the Service Manager data unload files>
```

i. Validate the case-insensitive unique indexes.

During the initial system load, Service Manager creates a set of case-insensitive indexes for each table, based on the keys in that table. When the sqldebug:1 parameter is in the sm.ini file, Service Manager logs these indexes the first time it reads a table. You can review the settings created for each table by viewing the sm.log file.

The case-insensitive unique indexes should be as Oracle function-based indexes where the Column Expression is `NLSSORT("<field name>",'nls_sort=''BINARY_CI''')`.

Follow these steps to verify that the case-insensitive unique indexes are created with the correct column expression:

i. Set sqldebug:1 in the sm.ini file, located in the <SM_install_location>\Server\RUN directory.

ii. Start Service Manager.

iii. Check the sm.log file in the <SM_install_location>\Server\logs directory. The following entry in the log file indicates that the Oracle instance is set to case-insensitive and that you connected to it successfully:

```
RTE I Oracle server settings for language, territory and character set:
AMERICAN_AMERICA.AL32UTF8 (AL16UTF16)
RTE I OCI Client settings for language, territory and character set:
AMERICAN_AMERICA.AL32UTF8 (UTF16)
....
RTE I Oracle instance setting for NLS_SORT is set to BINARY_CI
RTE I Oracle instance setting for NLS_COMP is set to LINGUISTIC
...
RTE I Oracle session is set up in CASE INSENSITIVE mode
```

The following information in the log file indicates that the Dbdict table has an index, DBDICTM1C989DE64, with a key called "NAME", which is case-insensitive:

```
RTE D Table Name: DBDICTM1

RTE D Schema Name                    Index Name
RTE D ------------------------------ ------------------------------
RTE D SMDB                           DBDICTM1C989DE64
RTE D ------------------------------ ------------------------------
```

(Lines continue)

```
Type Column Name                    Column Expression
---- ------------------------------ ----------------------------------------
U    SYS_NC00003$                   NLSSORT("NAME",'nls_sort=''BINARY_CI''')
---- ------------------------------ ----------------------------------------
```

6. Set up a connection to Service Manager:

   Service Manager connects to the database through your RDBMS client. To set up the connection between the Service Manager application server and your RDBMS, know the name of the database and the login ID and password required to connect to the database server that you created above. The Service Manager initialization file, sm.ini, must be present in the Service Manager server RUN directory.

   To set up connectivity to your Oracle database, follow these steps:

   a. Install the Oracle client on your Service Manager server machine.

      > **Note:** Service Managerrequires a 32-bit Oracle Client library, which can be found in the Oracle 64-bit Client installation directory or Oracle 32-bit Instant Client directory. Visit the Oracle site to download the proper Oracle client for the platform where you plan to run the Service Manager server.

   b. Configure a connection to the Oracle server in the tnsnames.ora file. Define the database name.

- On UNIX systems, the tnsnames.ora file is located in $ORACLE_HOME/network/admin or can be specified using the TNS_ADMIN environment variable.
- On Windows systems the tnsnames.ora file is located in the Oracle Home [%ORACLE_HOME%/network/admin] directory.

c. For Oracle 11.1 or above only, disable ADR tracing by turning off the diag_adr_enabled parameter in the sqlnet.ora file: diag_adr_enabled=OFF. ADR tracing is enabled by default.

> **Note:** An Oracle bug ("Multi Threaded OCI Client Dumps Core After Reconnecting To Database") is triggered when ADR tracing is enabled. Once this bug is triggered, the Service Manager server will crash every time when setting up a connection to the Oracle server.

d. Specify the name of the Oracle database connection in the sqldb parameter in the sm.ini file. You can do this after you install the Service Manager Server by running the Configuration tool and specifying the database name you provided in the tnsnames.ora file.

7. Set time zones for reporting:

   If you plan to report on Service Manager data using your RDBMS tools, set the sqltz parameter in the sm.ini file. This is an optional parameter that the Service Manager server uses to control the storing of date and time values in the RDBMS. This parameter defines the time zone to use as a base for all date and time values. The time zone is specified as the name of the time zone record in the Service Manager tzfile table. The default time zone is Greenwich/Universal (GMT). For more information about using the sqltz parameter, see the System Configuration Parameters topic in the Service Manager Help.

   > **Caution:** If you use different time zone settings, the dates contained in reports made by your RDBMS utility may be inaccurate.

8. Set Oracle table spaces. Most tables on an Oracle server hold less than 50 KB of data. Service Manager sets the initial storage space size when creating the SQL tables. When manually creating a new Oracle instance, follow these guidelines:
   - Create the database with a block size of 8 KB or a multiple thereof.
   - Create a separate table space for the Service Manager data, and make this the default table space for the Service Manager user.
   - Set the TEMPORARY table space for the Service Manager user to an appropriate temporary table space.
9. Set your UNIX environment variable for Oracle:

a. Find the path to your Oracle client's 32-bit shared libraries.

b. Set the UNIX environment variable as shown in the following examples. In these examples, the path to the Oracle client shared libraries is set relative to the Oracle environment variable $ORACLE_HOME.

- C shell: `setenv LD_LIBRARY_PATH $LD_LIBRARY_PATH:$ORACLE_HOME/lib32`
- Korn shell: `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib32`

> **Note:** For Linux, you must set the LD_LIBRARY_PATH variable.

10. Create your Oracle database with a UTF-8 code page. All data passed from Service Manager to the Oracle client is encoded in UTF-8; using a UTF-8-based Oracle database reduces the overhead of converting data and prevents the loss of special characters.

Install the Service Manager Server

This section provides instructions on how to install and configure the Service Manager Server.

Generate and install your Service Manager licenses

The Service Manager installer automatically copies AutoPassJ libraries as part of the server installation. AutoPass validates your license and determines what product features are enabled. Follow the steps in this section to obtain your permanent licenses.

1. Go to the HPE Software Licensing website.
2. Log on to **HPE Passport**.
3. Follow the instructions provided on the website to obtain license keys for your product.
4. Save the license key file to your system. Install license key(s) directly from a license key file. Do not manually transcribe and edit them from the activation certificate. Copy each license key file to the appropriate target system.

   As part of the process of obtaining a perpetual AutoPass license, a .dat file or several .dat files were sent to the email address that you provided. These files contain the licensing data required to use the applicable Service Manager modules. After you receive these files, follow these steps to move them to the Service Manager Server:

   a. Rename the .dat file to a .txt file so that you can open it with a text editor. For example, rename J8888X1624204.dat to J8888X1624204.txt.

   b. Create a text file named **LicFile.txt** and place it in the <*Service Manager server installation path*>/RUN/ directory.

c. Copy the license data from the license .txt file that you created in step **a** and paste it in the LicFile.txt file that you created.

> **Note:** Create the LicFile.txt file only once. If you request any additional licenses, append those licenses to the end of this file.

> **Tip:** You can run the "sm -updatelicense" command to load a new license .txt file into the existing one.

> **Note:** Make sure the LicFile.txt file is not read-only. The AutoPass jar files were updated in Service Manager version 9.50. Because of this code change, after upgrading to version 9.50 or later from an earlier version, the first time when you start the Service Manager Server, the Server will attempt to change the content of the license file to XML format. If the license file is read-only, the Service Manager Server will fail to start.

5. If you plan to run your system in a horizontally-scaled environment, copy LicFile.txt to the <*Service Manager server installation path*>\RUN\ folder on all hosts running in the horizontal group. In addition, provide the **grouplicenseip** parameter for each host. The **grouplicenseip** value should match the IP address that you provided when obtaining the license key.

> **Note:** If you have horizontal scaling implementation setup as a high availability failover cluster, you must request a permanent Service Manager license for both the virtual and the physical IP addresses of the host. Otherwise the Service Manager Server will fail to start.

Temporary licenses

You can use the following command line option to install a 60-day temporary license to evaluate, test, or develop your Service Manager system: `sm -instantOn`.

You can install a temporary license once per system. The license is valid for 60 days. Within this 60-day period, you must obtain a perpetual license key or a trial evaluation extension to continue using the product. During the last 10 days of the evaluation period, every user who logs in to the system will see a license expiration warning message. To remove the warning message, a system administrator must follow the steps above to obtain perpetual license files.

> **Note:** If you have not purchased all modules and want to consider adding modules for review during the Instant-On process, contact your HPE account manager.

Next, make sure you meet the Service Manager server installation requirements. See "Meet the Service Manager Server requirements" on the next page.

Meet the Service Manager Server requirements

Before you install the Service Manager Server, you should meet the following requirements.

For information about the supported operating systems and databases, refer to the *Service Manager Support Matrix* on the HPE Support matrices web site.

Meet the requirements for a Windows system

1. Make sure that you have a compatible operating system with the current updates.
2. The Service Manager Server requires the following database resources.

Requirement	Resources needed
RDBMS server	◦ Oracle database ◦ MS SQL Server
RDBMS client	◦ Oracle client ◦ Windows ODBC DSN defined for SQL Server

3. Have 1 GB RAM minimum. For production purposes, RAM is based on the expected user load.

   > **Note:** To avoid potential out-of-memory issues, we recommend that you run the `ulimit -d unlimited` command to set the heap size to unlimited before starting the Service Manager Server.

4. Create a local administrator account on the Windows server.
5. Have 1 GB of disk space.
6. Have a valid TCP/IP port that is greater than 1024.
7. Specify the appropriate number of processes. The system starts one process for each sm command line in the sm.cfg file. By default, each process is limited to 50 concurrent user sessions. The system assigns each user session or background process a dedicated thread.

   > **Note:** If you start background processes by using the sm system start command in the sm.cfg file, then the sm processes own the background process threads. If you start the background processes from a user session inside Service Manager, then the thread controller

> process that owns the user session also owns the background process threads.

8. Specify the amount of shared memory that you want the system to allocate. A server uses approximately 50 MB of base shared memory and requires an additional 5 MB of shared memory for every 50 users. You can specify the amount of shared memory the system allocates by using the shared_memory parameter in the sm.ini file.
9. For an Oracle database, update your system's PATH variable to include the path to the 32-bit versions of your RDBMS client. Refer to your operating system documentation for information on setting variables.

   For a Microsoft SQL Server database, configure ODBC DSN.

Meet the requirements for a Linux system

1. Make sure that you have a compatible operating system with the current updates.
2. The Service Manager Server requires the following database resources.

Requirement	Resources needed
RDBMS server	◦ Oracle database
RDBMS client	◦ Oracle database client

3. Have 1 GB of disk space.
4. Have a valid TCP/IP port that is greater than 1024.
5. Specify the appropriate number of processes. The system starts one process for each sm command line in the sm.cfg file. By default, each process is limited to 50 concurrent user sessions. The system assigns each user session or background process a dedicated thread.

   > **Note:** If you start background processes by using the sm system start command in the sm.cfg file, then the sm processes own the background process threads. If you start the background processes from a user session inside Service Manager, then the thread controller process that owns the user session also owns the background process threads.

6. Create a separate user ID that owns Service Manager. Service Manager will not run from a root account. You only need root access to modify the system kernel, and mount the Service Manager DVD.

7. Run the installation script from an ANSI terminal to avoid rendering errors. Non-ANSI terminals such as hpterm may produce unreadable results.
8. Update your system's LD_LIBRARY_PATH variable to include the path to the 32-bit versions of your RDBMS client. Refer to your operating system documentation for information on setting variables.
9. Adjust kernel resources. A server uses approximately 50 MB of base shared memory and requires an additional 5 MB of shared memory for every 50 users. You can specify the amount of shared memory the system allocates by using the shared_memory parameter in the sm.ini file.

   The following kernel resource requirements are the minimum values required to run a Service Manager server. If you run other programs that require kernel resources on the same system as Service Manager, then add the Service Manager kernel resource requirements to the existing resources. For example, if the existing system requires 100 MB in kernel resources, and Service Manager requires an additional 50 MB, then update the kernel resources to 150 MB.

   To configure kernel IPC parameters:

   The default shared memory limit (both SHMMAX and SHMALL) is 32 MB, but you can change it from the proc file system without restarting the system. For example, to specify 128 MB:

   ```
   # echo 134217728 >/proc/sys/kernel/shmall
   # echo 134217728 >/proc/sys/kernel/shmmax
   ```

   You can use sysctl.conf to control these parameters. Add the following to the /etc/sysctl.conf file:

   ```
   kernel.shmall = 134217728
   kernel.shmmax = 134217728
   ```

   sysctl.conf is usually processed at startup but can be called later.

   - Modify the kernel parameters as needed:
     - shmmax: This parameter enables you to allocate shared memory. A server uses approximately 50 MB of base shared memory and requires an additional 5 MB of shared memory for every 50 users. Allocate more shared memory than what you specify in the sm.ini file.
     - shmmni: This kernel parameter enables you to set the maximum number of shared memory segments system-wide.

     > **Note:** Service Manager uses 12 semaphores, regardless of the number of users logged on to the system.

   - Make sure that the upper limit (ulimit -n size) for file descriptors is at least 1024.

- Adjust the UDP buffer size to 20MB or higher. For better performance, if there is enough memory available on the server, choose a value larger than 20MB. Linux may generate warnings if the UDP buffer sizing set in the configuration files surpasses kernel limits. For example, a warning might look like the following:

  ```
  23966( 23966) 08/11/2009 15:38:33 receive buffer of socket
  java.net.DatagramSocket@c9d92c was set to 20MB, but the OS only allocated
  131.07KB. This might lead to performance problems. Please set your max
  receive buffer in the OS correctly (e.g. net.core.rmem_max on Linux)
  ```

  A superuser can change 0 kernel limits to enhance performance of UDP communication. To retrieve the UDP buffer sizing setting, use the `sysctl -w net.core.rmem_max` command. To change the setting, use the `sysctl -w net.core.rmem_max=8388608` command.

10. Disable the Linux security feature, exec-shield-randomize (for RedHat Enterprise Linux) or kernel.randomize_va_space (for SuSe Linux). The out-of-box smstart script sends you an error message and does not start the server if exec-shield-randomize or kernel.randomize_va_space is on. If you use your own script instead of smstart, be aware that the server can start if the security feature is turned on, but it will stop later.

    Take RedHat Enterprise Linux for example. The /proc/sys/kernel/exec-shield-randomize file controls whether Exec-Shield randomizes VM mapping. You can turn off exec-shield-randomize by using any of the following options:

    - Use the following command:

      ```
      echo 0 >/proc/sys/kernel/exec-shield-randomize
      ```

      The default value for /proc/sys/kernel/exec-shield-randomize is 1.

    - Include the following line in the /etc/sysctl.conf file:

      ```
      kernel.exec-shield-randomize=0
      ```

    - Include the following line in the /etc/grub.conf file:

      ```
      exec-shield=0
      ```

11. Make sure that the user running the installation script has permission to create new directories in the chosen installation path.

12. For 64-bit Linux, install the required libraries to support 32-bit Java on a 64-bit system by running the following command as “root”:

    > **Tip:** This step is required only when you are using an Oracle jre.

    ```
    yum -y install glibc.i686
    ```

You may need to update /etc/yum.repos.d with the working links for the required package if necessary.

> **Caution:** If the required 32-bit libraries are missing from the system, an "Unsupported java version" error will occur later when you configure or start the server by running the `configure` or `smstart` script. As a result, you will not be able to configure or start the server.

Next, install and configure the Service Manager Server. See "Install the Service Manager Server" on page 35.

Install and configure the Service Manager Server

Install Service Manager in a development environment and then convert or push the installation to your production environment.

> **Tip:** If you are upgrading from an earlier version of the Service Manager Server, see the *Service Manager Upgrade Guide*.

Install the Windows Server

To install the Service Manager9.50 Server on a Windows system, complete the following tasks.

Task 1. Install the new Service Manager Server

To install the Service Manager Server, follow these steps:

1. Log on to the Windows server as a user with local administrator privileges.
2. Extract the SM9.50-1.zip file into the appropriate drive of the server.
3. Navigate to the **Installation\Server** folder, and double-click **setupserver-9.50.exe**.
4. Click **Next** to read and accept the licensing agreement.
5. Select the **I accept the terms of the License Agreement** option. The Next button becomes active.
6. Click **Next** to accept the default installation folder: C:\Program Files (x86)\HPE\Service Manager 9.50\Server, or click **Choose** to choose a different installation location.

> **Caution:** Do not install the server over existing versions of ServiceCenter or Service Manager. Install in a new folder. The Service Manager server folder name cannot contain parentheses or use non-ASCII characters. The server cannot start if installed in a folder with a non-compliant folder name.

> **Note:** If you have two different versions of the Service Manager Server (for example, the 9.21 server and 9.50 server) installed on the same server host, you will not be able to start both of them at the same time - your attempt to start the second server will fail with an error in the server log that indicates the program that created the shared memory is incompatible with the current program. This is because the two servers are different binaries, which cannot be attached to the same shared memory.

7. Click **Next** to prepare the installation process. The summary information page opens.
8. Click **Install** to copy the installation files.
9. When the installation is complete, click **Next**.
10. Select the **Run the Server Configuration Utility after installation** option to open the configure server tool at the end of the installation.

    > **Note:** You can skip this step and configure the Service Manager server manually by editing the RUN\sm.ini initialization file in a text editor.

11. Click **Done** to exit the installation wizard. The server installation is complete, and the Configuring Service Manager Server wizard opens. Follow the steps in the next section to configure the server.

Task 2. Configure the Service Manager Server

You can customize your server installation by modifying the Service Manager initialization file (sm.ini).

You can define the processes that the system starts automatically and the system's startup parameters from the Service Manager configuration file (sm.cfg), which determines how the system starts when started from a service.

If you select the **Run the Server Configuration Utility after installation** option, the configuration tool starts automatically during your installation.

When you install the server for the first time, the default settings are configured for the sample database. While this tool is intended to configure new or test implementations running the out-of-box sample data, you can use it whenever you want to change the settings in your system's sm.ini file. Refer to the Service Manager Help for a complete list of the parameters stored in the sm.ini file.

> **Caution:** The configuration utility overwrites your current sm.ini settings. You should back-up your system's sm.ini file prior to running the configuration utility to prevent any accidental data loss or loss of service.

To configure the Service Manager server, follow these steps:

1. Run the Server Configuration Utility, configure.bat, located in the <*Service Manager installation path*>\Server directory.
2. Specify the listener ports:
   - HTTP Port (system): The communications port on which you want Service Manager to listen to client connection requests. The default port is 13080.

   > **Note:** For a new server installation, the configuration wizard does not display the **Enable HTTPS Port** and **HTTPS Port** options, because SSL is not enabled by default (the sm.ini file contains the **sslconnector:0** parameter). If you have already set **sslconnector:1** in the sm.ini file and then rerun the configuration utility, the configuration wizard displays two HTTPS options so that you can reconfigure the HTTPS settings:
   >
   > - Enable HTTPS Port: Select this option to enable an HTTPS port.
   > - HTTPS Port: The communication port on which you want Service Manager to listen to secure client connection requests.
3. Specify the database type and connection information:
   - Database Type: The database that you want to use to store your data.
   - SQL Database Name:

     For Microsoft SQL Server, this is the ODBC DSN name. Note that Microsoft SQL Server is supported for a Windows platform only.

     For Oracle Database, this is the Network Service Name in tnsnames.ora.
   - SQL User: The user that Service Manager should connect to your database with.
   - SQL Password: The password for the user that Service Manager should use to connect to your database.
   - Use Unicode Data Type: Use this option if you need to support multiple languages that are not supported by one collation. Otherwise, use the right collation and do not select this option. This option may cause database performance downgrade because it creates a larger database size. For information about how to select SQL Server collations, refer to the SQL Server documentation.

     > **Caution:** Be aware that this operation is not reversible.
4. Click **Verify Connection** to confirm that Service Manager can connect to the database.
5. Upload the SM 9.50 demonstration data, if desired. All new Service Manager installations require this. Uploading the demonstration data also uploads the out-of-box 9.50 applications. If you are upgrading only the Service Manager client and server, you do not have to upload the data. The new

client and server can connect to your old system.

> **Note:** Before your system goes live, you need to purge the out-of-box demonstration data by running the **PurgeOutofBoxData** unload script. For details, see knowledge article KM718390.

> **Caution:** Do NOT upload the data into an existing production system. Instead, you need to perform an applications upgrade. For more information, see the *Service Manager Applications Upgrade Guide*.

> **Note:** If you selected the Unicode data type for SQL Server, the applications and demonstration data are uploaded as Unicode. Additionally, to indicate that your SQL Server database uses Unicode, the read-only **Use Unicode Data Type** flag is turned on in the **sqlserver** record of the **sqldbinfo** table.

Install the Linux Server

> **Note:** The following convention identifies variables that may change depending on your particular installation: `<variable>`. When you see a variable in brackets during the installation, replace the variable with information specific to your system. Do not type the brackets (< >) as part of the command.

To install the Service Manager9.50 Server on a Linux system, complete the following tasks.

Task 1. Install the new Service Manager Server

To install the Service Manager 9.50 Server, follow these steps:

1. Log on to the Linux server as a user with local administrator privileges.
2. Extract the SM9.50-1.zip file into the appropriate drive of the server.
3. Navigate to **Installation/Server** directory.
4. Run the **setupLinuxX64-9.50.bin** script.

   > **Note:** The setup scripts assume you will run them from an X-Windows environment. If you prefer to run the scripts from a console instead, add "-i console" to the command line. For example, `setupLinuxX64-9.50.bin –i console`.

5. Accept the license agreement.
6. At the installation script prompt, type the absolute installation directory where you want to install Service Manager, or accept the default one. Follow these rules:

- Do not install the server over existing versions of ServiceCenter or Service Manager. Install in a new folder.

  > **Note:** If you have two different versions of the Service Manager Server (for example, the 9.21 server and 9.50 server) installed on the same server host, you will not be able to start both of them at the same time - your attempt to start the second server will fail with an error in the server log that indicates the program that created the shared memory is incompatible with the current program. This is because the two server versions are different binaries, which cannot be attached to the same shared memory.

- The installer will ask you to confirm if the specified installation directory is correct. If you specify an invalid directory, the installer behaves unexpectedly.
- Do not use the "~" symbol when entering the path. InstallShield treats this as a regular character, and will create a directory with the name '~'.

The system takes several minutes to uncompress the files and complete the server installation.

7. Click **Finish** to exit the wizard.
8. If you want to use an OpenJDK jre, make sure your Linux host has Internet access and then run the "`installOpenJDK.sh -i4sm`" command as a superuser (such as root) in the server installation directory.

   If you want to use an Oracle jre, do the following:

   a. Update the JAVA_HOME environment variable to make it point to the Oracle jre.
   b. From the Server's RUN directory, run the "setupLinks.sh jre" command as the owner of the Service Manager installation directory. This will create a symbolic link for the Oracle jre.

   For more information, see the **JRE support** section in "Deployment architecture" on page 13.
9. To automatically configure the server, run the **configure** script in your <*Service Manager Server installation path*> directory to update the sm.ini file.

   > **Note:** You can also configure the Service Manager server by editing the sm.ini configuration file. Follow the instructions in the next task if you want to configure the server manually.

Task 2. Configure the Service Manager Server

You can customize your server installation by modifying the Service Manager initialization file (sm.ini).

You can define the processes the system starts automatically and the system's startup parameters from the Service Manager configuration file (sm.cfg), which determines how the system starts when started from the **smstart** script.

When you install the server for the first time, the default settings are configured for the sample database. While this tool is intended to configure new or test implementations running the out-of-box sample data, you can use it whenever you want to change the settings in your system's sm.ini file. Refer to the Service Manager Help for a complete list of the parameters stored in the sm.ini file.

> **Caution:** The configuration utility overwrites your current sm.ini settings. You should back-up your system's sm.ini file prior to running the configuration utility to prevent any accidental data loss or loss of service.

To configure the Service Manager server, follow these steps:

1. From a console, run the server configuration script, configure, located in the <*Service Manager installation path*>/Server directory:

   ```
   configure -consolemode
   ```

2. Specify the listener ports:
   - HTTP Port (system): The communications port on which you want Service Manager to listen to client connection requests. The default port is 13080.
   - Enable HTTPS Port: Select this option to enable an HTTPS port.
   - HTTPS Port: The communication port on which you want Service Manager to listen to secure client connection requests.

   > **Note:** For a new server installation, the configuration wizard does not display the **Enable HTTPS Port** and **HTTPS Port** options, because SSL is not enabled by default (the sm.ini file contains the **sslconnector:0** parameter). If you have already set **sslconnector:1** in the sm.ini file and then rerun the configuration utility, the configuration wizard displays these two HTTPS options so that you can reconfigure the HTTPS settings.

3. Specify the database type and connection information:
   - Database Type: The database that you want to use to store your data.
   - SQL Database Name:

     For Microsoft SQL Server, this is the ODBC DSN name.

     For Oracle Database, this is the Network Service Name in tnsnames.ora.
   - SQL User: The user that Service Manager should connect to your database with.
   - SQL Password: The password for the user that Service Manager should use to connect to your database.
4. Verify the connection to confirm that Service Manager can connect to the database by running the command **sm -sqlverifyconnection** in the Service Manager RUN directory.

5. Upload the SM 9.50 demonstration data, if desired. All new Service Manager installations require this. Uploading the demonstration data also uploads the out-of-box 9.50 applications. If you are upgrading only the Service Manager client and server, you do not have to upload the data. The new client and server can connect to your old system.

   > **Note:** Before your system goes live, you need to purge the out-of-box demonstration data by running the **PurgeOutofBoxData** unload script. For details, see knowledge article KM718390.

   > **Caution:** Do NOT upload the data into an existing production system. Instead, you need to perform an applications upgrade. For more information, see the **Upgrade** node of the Service Manager Help Center.

Now you have the Service Manager Server installed. Next, go to "Start the Service Manager Server" below if this is a new installation.

Start the Service Manager Server

Once the Service Manager Server is installed and is successfully connected to the database, you are ready to start it.

Start the Service Manager Server on Windows

Start the Service Manager server so that users can connect with client sessions. You can start the server from the Windows command prompt or from Windows services. Click a method below to view instructions for starting the server using that method.

Start the server from the Windows command prompt

1. Open the Windows command prompt on the Service Manager server. Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.
2. Change directories to the RUN folder of your Service Manager installation. For example, `C:\Program Files (x86)\HPE\Service Manager 9.50\Server\RUN`.

   > **Caution:** Before proceeding to the next step, check that the HPESM_pdf.txt file exists in this folder. Do not delete or modify this file; otherwise the server will fail to start. Additionally, if you have copied the HPSM7_pdf.txt or HPSM_pdf.txt file from the RUN folder of a previous server installation, you are recommended to delete it.

3. Type the following command:

```
sm -httpPort:13080 -httpsPort:13443
```

> **Tip:** You can omit the httpsPort parameter if SSL is not enabled in your Service Manager environment.

> **Note:** You can omit the httpPort and httpsPort parameters if you provide them in the Service Manager initialization file (sm.ini).

4. Press **Enter**.

> **Caution:** Leave the command prompt open while the Service Manager server runs. Closing the command prompt window stops Service Manager immediately without cleaning up any processes or releasing any record locks.

Start the server from Windows services

1. From the Windows Control Panel, click **Administrative Tools** > **Services** to open the Services applet.
2. In the Services list, click **HPEService Manager9.50 Server**.
3. Click **Start** to start the service.

   Windows displays a message that the Service Manager service is starting. After several seconds, the service starts and displays Started in the Status field. If the Service Manager service does not start, contact customer support with any error messages.

Start the Service Manager Server on Linux

Start the Service Manager server so that users can connect with client sessions.

> **Note:** You may encounter out-of-memory issues when the Service Manager server is highly loaded. To avoid the issues, we recommend that you run the `ulimit -d unlimited` command to set the heap size to unlimited before starting the Service Manager server.

1. Run the following command to go to the RUN directory of your Service Manager:

   ```
   cd <install path>/ServiceManager 9.50/RUN
   ```

> **Caution:** Before proceeding to the next step, check that the HPESM_pdf.txt file exists in this folder. Do not delete or modify this file; otherwise the server will fail to start. Additionally, if you have copied the HPSM7_pdf.txt or HPSM_pdf.txt file from the RUN folder of a previous server installation, you are recommended to delete it.

2. Type the following command, and then press Enter.

```
smstart
```

Now, the Service Manager server is started. Next, you must install either the Windows Client or the Web Tier to get a user interface for accessing the server. See "Install the Service Manager Windows Client" on page 51 and "Install the Service Manager web tier" on page 63.

> **Tip:** The Service Manager server supports several different implementation options to manage large numbers of client connections to the server. For information on how to manage your client connections, refer to the "Configuring installation and setup options" section of the online help.

Uninstall the Service Manager Server

Follow these instructions if you need to uninstall the Service Manager Server.

Uninstall the Windows Server

You can uninstall the server from Add/Remove Programs or using the Service Manager uninstaller. Click a task below to view instructions for uninstalling the server using that method.

Uninstall the server using Add/Remove Programs

1. Log in to the Windows server as a user with local administrator privileges.
2. Stop the Service Manager service.
3. From the Windows **Start** menu, click **Settings** > **Control Panel** > **Add/ Remove Programs**. The Add/Remove Programs dialog box opens.
4. Scroll to the Service Manager server program and click **Remove**. A message prompts you to verify that you want to remove the program.
5. Click **Yes**. The process takes several minutes. Additional messages indicate the progress of the uninstall. When you complete the uninstall, you return to the Add/Remove Programs dialog box.
6. Click **Close**.

Uninstall the server using the uninstaller

1. Log in to the Windows server as a user with local administrator privileges.
2. Run the following commands:

```
cd <install path>/Service Manager9.50/_uninstall

uninstaller.exe
```

Uninstall the Linux Server

1. Stop the Service Manager server.
2. Run the following commands to uninstall the server:

   ```
   cd <install path>/ServiceManager9.50/_uninstall

   uninstaller –i console
   ```

3. Delete all of the Service Manager server directories and subdirectories.

Install the Service Manager Windows Client

Follow these instructions to install the Service Manager Windows Client.

Meet the Service Manager Windows Client requirements

Install at least one Windows Client for the system administrator or group of power users. You must install the Windows Client on a Windows workstation. You can support clients running on other operating systems by installing the Service Manager web tier.

You must have local administrator privileges to install the Windows Client. By default, the client workspace and configuration information is stored in the following directory: C:\Users\<*username*>\Service Manager.

Caution: Make a backup of any customized Help files that you have created for your Service Manager clients. The installer for the Service Manager Windows Client overwrites Help from prior clients.

- The Windows Client installer also installs the Client Configuration Utility.
- You cannot upgrade previous Service Manager clients to the Service Manager9.50 Windows Client. Instead, simply install the Service Manager9.50 Windows Client in a new folder. HPE recommends that you remove previous Service Manager clients.

Make sure that your client workstation meets the requirements listed in the following table.

Requirement	Minimum	Recommended
OS	Windows 7 (32-bit or 64-bit)	Windows 8.1 or 10 (32-bit or 64-bit)
CPU	Pentium III 650Mhz	Pentium IV 2.4 GHz or higher
RAM	1G	4G
HD	1G	1G
Resolution	1280x800 (16 colors)	1280 x 1024 (256 colors)
Network	100 Megabit	100+ Megabit
Login account	Local administrator account	Local administrator account

Install a Windows Client

The Service Manager Windows Client is mainly for Service Manager administrators and implementers. HPE recommends that you use the web client for end users.

> **Note:** The Windows Client installer also installs the Client Configuration Utility in the following directory: <*Service Manager installation path*>\Client\ClientConfiguration. To run the utility, double-click the **confutil.bat** file in this directory.

You can install a Service Manager Windows Client (including the Client Configuration Utility) locally or on a network share where multiple users run from the shared client installation. Click a task below to view instructions for installing the Windows Client on a local machine or on a network share.

> **Caution:** If you share a Windows Client on a network share, you run the risk of running out of user licenses or network system resources to run the client.

Install a local Service Manager client and Client Configuration Utility

1. Make sure that the workspace and configuration folders are writeable.
2. Log in to the Windows server as a user with local administrator privileges.
3. Extract the SM9.50-1.zip file into the appropriate drive of the server.
4. Navigate to the **Installation\Client** directory.
5. Run **setupclient-9.50.exe** to start the Installer. The installation wizard starts.
6. Select the language for the installer and click **OK**. The Service Manager Client Installer opens.
7. Click **Next** to read the licensing agreement.

8. Select **I accept the terms of the License Agreement**. The **Next** button becomes active.
9. Click **Next** and the Choose Installation Folder page opens.
10. The default installation folder is: C:\Program Files (x86)\HPE\Service Manager 9.50\Client. Click **Choose** to navigate to a different location if you want to choose a different path.
11. The feature selection page opens, on which the **HPE Service Manager Client Administrative Tools** option selected by default. This option will install the client administrative tools, such as **Console** and **RAD Debugger**. If you do not want to install these administrative tools, deselect this option.
12. Click **Next** to prepare the installation process. The Summary page opens.
13. Click **Install** to begin copying the installation files. The HPEService Manager Client Installer displays summary information when the installation is complete.
14. Click **Finish** to exit.

Install a shared Windows Client and Client Configuration Utility

> **Caution:** If you share a Windows Client on a network share, you run the risk of running out of user licenses or network system resources to run the client.

1. Make sure that the workspace and configuration folders are writable.
2. Log in to the network share as a user with administrator privileges.
3. Extract the SM9.50-1.zip file into the appropriate drive of the server.
4. Navigate to the **Installation\Client** directory.
5. Run **setupclient-9.50.exe** to start the Installer. The installation wizard starts.
6. Select the language for the installer and click **OK**. The Service Manager Client Installer opens.
7. Click **Next** to read the licensing agreement.
8. Select **I accept the terms in the License Agreement**. The **Next** button becomes active.
9. Click **Next** and the Select Installation Folder page opens.
10. The default installation folder is: C:\Program Files (x86)\HPE\Service Manager 9.50\Client. Click **Choose** to navigate to a different location if you want to choose a different path.
11. The feature selection page opens, on which the **HPE Service Manager Client Administrative Tools** option selected by default. This option will install the client administrative tools, such as **Console** and **RAD Debugger**. If you do not want to install these administrative tools, deselect this option.
12. Click **Next** to prepare the installation process. The Summary page opens.

13. Click **Install** to begin copying the installation files. The HPE Service Manager Client Installer displays summary information the installation is complete.
14. Click **Done** to exit.
15. Create a Windows network share to the folder where you installed the Service Manager client and grant users access to the network share. For example, \\my_server\Service Manager Client.
16. Log in to the computer system of each user who will use the shared client and map the network share to a drive letter on the local system. For example, Drive letter: F: Mapped to: \\my_server\Service Manager Client.
17. Create a Windows shortcut to the ServiceManager.exe file on the network share. For example, F:\ServiceManager.exe.

    By default, all users share common client settings. If you want each user to have individual local client settings, modify the target properties of the Windows shortcut to add the following information after the executable name: `-data %USERPROFILE%\Service Manager\`

    The `-data` parameter enables you to specify a path where you want to store client settings. The example path above places a Service Manager folder in the Document and Settings folder of the currently logged in user.

    > **Note:** If your path name includes spaces, enclose the path in double quotation marks. For example, `F:\ServiceManager.exe -data "%USERPROFILE%\HPE Service Manager\workspace"`.

The Windows Client is now installed. Next, you need to define a connection from the Windows Client to the Service Manager Server.

Define a connection from the Windows Client to the Server

The first time you access the Windows Client, the Connections window opens, enabling you to define a connection to a Service Manager host server. You can add and save multiple connection settings from the Connections window.

You must set your connection to an active server process. These are the default settings:

- Client listener on ports 13080 (http) and 13443 (https/SSL) for HTTP clients, including Windows, web, and SOAP-API
- Special listener on port 12690 for SCAuto

- The login account (User name/Password) that you want to define for a new client connection must already exist in Service Manager.
- Service Manager provides an out-of-box login account with System Administrator privileges: **System.Admin** (with a blank password). You can use this login account the first time you connect to a Service Manager Server. Disable this account or change its password after creating accounts for all of your users. For information about how to create user accounts, see the Service Manager help.
- If the client computer already has a previous version of Service Manager Client installed, all the existing connection settings are still available in the new client version. However, some client settings in certain old versions may prevent Service Manager Client from running. In this case, you must remove the <*user_home*>\ServiceManager folder on the client computer (where <*user_home*> is the user profile folder) and restart Service Manager Client. This will remove all client settings and the user has to reconfigure the client.

1. From the Windows **Start** menu, click **All Programs** > **HPE** > **Service Manager 9.50** > **Service Manager Client**. The Connections window opens.
2. Click **New**. The Connections window displays a new node in the Connections pane.
3. Type or select the connection parameters:

Parameter	Default option	Description
Name	New_configuration	The name of this configuration
User name	User name of the Windows user currently logged on.	The name that you use to log in to the Server
Password	blank	The password that you use to log in to the Server
Remember my password	False	An option to tell the system whether to store your password
Automatically log in	False	An option to log in automatically when you start the Service Manager client
Server host name	localhost	The name of the server that hosts the Service Manager service
Server port number	13080	The port number that your computer uses to connect with the server
Language	blank	The language to use for this session (can differ from the language set on the computer)

Parameter	Default option	Description
Connection identified by a color	blank	An option to change the background color of your connection

4. Click **Advanced** if you want to set the optional advanced connection options:
   - **Connect to External Load Balancer**: An option that enables the Windows Client to connect to the server through an external hardware load balancer.
   - **Compress SOAP Messages**: An option that compresses SOAP messages using GNU zip (gzip) encoding to reduce the amount of data transmittal to and from the server.
   - **Use SSL Encryption**: An option that uses a Secure Socket Layer (SSL) encryption tool to protect your data when transmitting it over the network.

     > **Caution:** You must define a valid CA certificates file to enable SSL encryption. The client installation includes a sample CA certificate file: **cacerts**. The cacerts file exists in the <Service Manager installation path>\Client\ plugins\com.hp.ov.sm.client.common_ 9.50.xxxx folder.

   - **Trace SOAP Traffic**: An option that logs SOAP messages for debugging.
5. Click **OK** to add the advanced features.
6. Click **Apply** to add the connection.
7. To add additional connections, repeat steps 2 – 6.

Connect the Windows Client to the Service Manager Server

You can connect to multiple servers from one Service Manager client. Each connection opens in its own window.

1. From the Windows **Start** menu, click **All Programs** > **HPE** > **Service Manager9.50** > **Service Manager Client**. The Connection window opens.
2. Double-click a connection or click a connection and then click **Connect**.

Customize images used by the Windows Client

You can customize the images that the Windows Client uses by providing alternate versions of the

images from a local folder or web server virtual directory. The following guidelines and considerations apply to customized images:

- All custom images must retain their original file name.
- All custom images must retain their original relative path from the icons/obj16 folder.
- You only need to save customized images in the branded/obj16 folder. If the Service Manager client does find updated images in the branded/obj16 folder it uses the default images in the icons/obj16 folder.
- Providing custom images from a web server allows you to automatically update images without having to reinstall the Windows Client.

To provide custom images from a local folder

You can use the following steps to provide custom images with the repackaged client.

Note: This image customization method increases the amount of hard disk space required to install the Service Manager Windows Client as the custom images are installed in addition to the default images.

1. Copy the images from the Service Manager client into a temporary folder.

   The client images are located in the following folder: C:\Program Files\HPE\Service Manager 9.50\Client\plugins\ com.hp.ov.sm.client.eclipse.user_9.50\src\resources\icons\obj16.
2. Edit the images that you want to customize in the temporary folder.
3. Delete any images that you do not customize from the temporary folder.
4. Run the Client Configuration Utility and select the local images option.

   > **Tip:** To run the Client Configuration Utility, double-click the **confutil.bat** file in the <*Service Manager installation path*>\Client\ClientConfiguration\ directory.

   The Client Configuration Utility creates the following new folder in the Service Manager client installation: C:\Program Files\HPE\Service Manager 9.50\Client\plugins\ com.hp.ov.sm.client.eclipse.user_9.50\src\resources\icons\branded\obj 16.
5. Copy your custom images to the branded\obj16 folder. You can copy the custom images to the local folder while the Client Configuration Utility is open.
6. Repackage the client as a .zip file or another distribution format.

To provide custom images from a web server virtual directory

You can use the following steps to provide custom images from a central web server. This image customization method does not increase the amount of hard disk required to install the Service Manager Windows Client. In addition, any changes you make to images on a web server are automatically applied to the Windows Client.

1. Create a virtual directory on your web server to store the custom images.
2. Copy the images from the Service Manager client into a temporary folder. The Service Manager client images are located in the following folder: C:\Program Files\HPE\Service Manager 9.50\Client\plugins\ com.hp.ov.sm.client.eclipse.user_9.50\src\resources\icons\obj16.
3. Edit the images that you want to customize in the temporary folder.
4. Delete any images that you do not customize from the temporary folder.
5. Copy your custom images to the virtual directory on your web server.
6. Run the Client Configuration Utility and select the web server virtual directory option. The Client Configuration Utility configures the Service Manager client to point to the URL of your web server virtual directory.

   > **Tip:** To run the Client Configuration Utility, double-click the **confutil.bat** file in the <*Service Manager installation path*>\Client\ClientConfiguration\ directory.

Customize the Windows Client

The Service Manager Client Configuration Utility enables you to customize a Windows installation for deploying to end users. This utility is included in the Windows Client installation. For its installation requirements, see the *Meet the Service Manager Windows Client requirements* section.

> **Note:** The Client Configuration Utility cannot push customization changes to previously installed Windows Clients. To change existing installations of the Windows Client, you uninstall the existing client and reinstall using the customized files you create. The Client Configuration Utility only picks up changes made directly from the Windows Client interface or within the utility itself. The Client Configuration Utility cannot pick up changes made directly to Windows Client initialization files.

The Service Manager Client Configuration Utility changes the following Windows Client settings:

- Splash screen image that Service Manager displays when users open the Windows Client.
- Name of provider listed for Service Manager. For example, Hewlett-Packard Enterprise Development Company, L.P.
- Name of the Service Manager application. For example, Service Manager.
- Location of application images and icons.
- Location of the Help Server where the Windows Client can access documentation.

- Changes that an administrator saves within the Windows Client interface prior to running the Client Configuration Utility, including default login options, connection dialog box configuration options to display, default connection configuration settings, and Help Server configuration options.

Known issues

The Client Configuration Utility has the following known issues:

- You must customize images before you run the Client Configuration Utility. The Client Configuration Utility enables you to change the location of images but not to edit them directly.
- If you deploy a repackaged Windows Client that has a predefined connection over SSL, the Windows Client may display the connection error message “No trusted certificate found.” This error indicates that you are installing the customized client in a different path than the original client used. You can restore the client connection by providing the correct path to the CA certificate file in the client Preferences dialog box.

To customize the Windows Client, follow these steps:

1. Double-click <*Service Manager installation path*>\Client\ClientConfiguration\confutil.bat. The Windows Client Configuration Utility opens.
2. Click **Next**. The Specify Service Manager Directory page opens.
3. Type or select the path to an existing installation of the Service Manager Windows Client, and then click **Next**. The Change Startup Splash Image page opens.
4. Click **Skip** if you want to use the default splash screen image, or type or select the path to the splash screen image that you want to use.

   The default splash screen image, splash.bmp, is located in the following folder: C:\Program Files (x86)\HPE\Service Manager 9.50\Client\plugins\ com.hp.ov.sm.client.eclipse.user_ 9.50\src\resources\icons\obj16.
5. Follow these guidelines when you edit the splash screen image:
   - The image must retain its original file name.
   - The image must be in the Windows bitmap (.bmp) file format.
   - The image should be approximately 500 wide by 600 pixels high. The Client Configuration Utility crops larger images to this size.
6. Click **Next**. The Replace Provider and Application Strings page opens.
7. Click **Skip** to use the default application strings or type the text strings that you want to use for the following items:

- Provider: Type the company name that you want to display in the Windows Client interface. The default name is Hewlett-Packard Enterprise Development Company, L.P.
- Application: Type the application name that you want to display in the Windows Client interface. The default name is Service Manager.

8. Click **Next**. The Customize Where Service Manager Application Images are Located page opens.
9. Click **No customization** or **Skip** to use the default images. Or select the path to your customized images:
   - Locally: The Client Configuration Utility creates a \branded\obj16 folder where you can place customized images to override the default Windows Client images.
   - Remotely: Type the URL where the Windows Client can access customized images.
10. Click **Next** to continue. The Customize Default Login Options page opens.
11. Click **Skip** if you do not want to create a default connection. Or select whether to display the following options on Connections dialog box on your customized client:
    - Show the "Remember my password" option: Enabled by default. When disabled, the client's Connections dialog box will not display the "Remember my password" check box option.
    - Show the server parameters: Enabled by default. When disabled, the client's Connections dialog box will not display the "Use Login/ Password" and "Use Trusted Sign-on" radio buttons, or the "Server host name" and "Server port number". Also, the New and Delete buttons will be disabled.
    - Show the "Advanced" options page: Enabled by default. When disabled, the client's Connections dialog box will not display the "Advanced" notebook tab. Additionally, the "Trace SOAP Traffic" feature will not be available.
12. Provide the following information about the default connection that you want to create:
    - Hostname: Type the network name or IP address of the Service Manager server that you want the Windows Client to connect to.
    - Port Number: Type the communications port on which the Service Manager server listens to client connection requests. The default communications port is 13080.
    - Compress Messages: Select true to enable message compression between the Windows Client and the Service Manager server. Select false to have messages remain uncompressed.
    - Use SSL Connection: Select true to enable an SSL connection between the Windows Client and the Service Manager server. Select false to use a standard connection.
    - CA Certificate Path: Type or select the local path to the CA certificate used by your SSL connection. Leave this entry blank if you do not use an SSL connection.

Note: You can find a sample CA certificate file cacerts in the following path: C:\Program Files (x86)\HPE\Service Manager 9.50\Client\ plugins\com.hp.commons_9.50\.

13. Click **Next**. The Use and Configure Help Server page opens.
14. Click **Skip** if you do not want to provide online help from a Help Server. Or select the **Use Central Help Server** option to establish a connection to a Help Server. Type the following Help Server information:
    - Help Server Host: Type the network name of the Service Manager Help Server to which you want the Windows Client to connect.
    - Help Server Port: Type the communications port on which the Service Manager Help Server listens to client connection requests. The default communications port is 80.
15. Click **Next**. The Client Configuration Utility page opens.
16. Click **Exit**. The client is now configured with your customizations.
17. Zip the contents of the Service Manager 9.50 directories to prepare and deploy the customized configuration of the Service Manager 9.50 client to other users. The following two directories are necessary for a proper deployment:
    - C:\Program Files (x86)\HPE\Service Manager 9.50
    - %HOMEPATH%\Service Manager
18. Make sure that end users have the installation DLLs in their windows\system32 directory in order for the deployed client to work properly. Add the following path to their system environment variables: `<ServiceManagerHome>\plugins\com.hp.ov.sm.client.thirdparty_9.50\lib;`

Uninstall the Windows Client or its components

1. From the Windows **Start** menu, click **Settings** > **Control Panel** > **Add/ Remove Programs**. The Add/Remove Programs window opens.
2. Scroll to HPEService Manager Client and click **Remove**. A message prompts you to verify that you want to remove the program.
3. Click **Yes**. The uninstall process takes several minutes. Additional messages indicate the progress of the uninstall. When you complete the uninstall, click **Close** to close the Add/Remove Programs dialog box.

The client uninstall process intentionally preserves your client configuration settings and any other files that have changed since the initial installation. You must manually remove these files if you want to completely uninstall Service Manager from your system. HPE recommends that you delete the entire

client installation folder and the local writeable workspace and configuration folder if you do not want to preserve any existing client settings.

Install the Service Manager web tier

The web tier enables users to connect to the server by using a web browser. It can run on both Windows and UNIX platforms. There are scaling issues to consider, one web application server can only handle so many concurrent users before you need additional servers to handle the load.

Follow these instructions to install the Service Manager web tier.

Meet the browser and architecture requirements for the web tier

The Service Manager web tier uses both a web server and a web application server to access Service Manager forms through a web browser. The web server handles incoming HTTP requests while the web application server runs the Java and JSP necessary for connecting to Service Manager.

> **Note:** Some web application servers such as Tomcat and WebSphere include built-in web servers.

Install the web tier by deploying the webtier-9.50.war or webtier-ear-9.50.ear to your web application server. Some web application servers also require you to install the Sun J2SE Java Development Kit (JDK).

1. Enable the following browser settings:
   - Cookies
   - Java
   - JavaScript
   - Pop-ups. You can add the Service Manager server URL to the pop-up exception list.
2. The Service Manager Web tier uses SSL encryption between the web browser and web application server by default. You must provide a valid web application server certificate to use the following SSL features:

- Encrypt all communication with the web application server
- Protect against complex SSL-related attacks
- Authenticate that the web application server is a valid host

> **Note:** If you only want to demonstrate the web tier functionality, you can disable the secureLogin parameter from the web tier configuration file (<web tier .war file>\WEB-INF\web.xml)

For more information, refer to the online Help for Required SSL encryption.

3. To display the workflow graphical view, install the Sun Java Runtime Environment (JRE) on the local host.
4. Determine the web architecture that you need to support your web tier. A Service Manager web tier requires at least one web application server to run. Depending on the features and scale of your web tier, it may also require a dedicated production web server and additional web application servers. If you use any of the implementation options list below, you need to install and configure a dedicated production web server. If you are not running any of the configurations listed below, then you can run your web tier from a single web application server:
   - A trusted sign-on implementation: You want web client users to log in to Service Manager without entering a user name and password.

     A trusted sign-on implementation requires a web server to accept the pre-authenticated HTTP header information from your authentication software (such as SiteMinder or Integrated Windows Authentication). You must install and configure the authentication software separately. See your web server documentation for information about the HTML headers that your web server expects from your authentication software. For additional information, go to the Software Support Online site at https://softwaresupport.hpe.com/ and search for the following white paper on setting up single sign-on in Service Manager: *SSL Setup and Single Sign-on in Service Manager using Windows or Third Party Authentication*.
   - A load balanced implementation: You want to distribute web client connections among multiple web application servers.

     A load-balanced implementation uses a web server to route connection requests to two or more web application servers. You must configure the web server to identify the web application servers (also known as workers) that are available to accept web client requests. For some web server and web application server combinations, you may need to install additional connection software. For example, to route requests to Tomcat web application servers using the Apache web server, you must install the proper connector. See your web server and web application server documentation for information about routing HTTP requests to available worker web application servers.

- A scaled implementation to support a large number of concurrent users: You want to support 300 or more concurrent web client connections.

  A scaled implementation uses the load balanced implementation described above to support a large number of concurrent web client users. As a general rule, HPE recommends starting one worker web application server for every 300 concurrent web client connections you want your web tier to support. To help determine the number of connections your web tier can support, go to the Software Support Online site and search for the following white paper: *Service Manager 7 Reference Configurations*.

Deploy the web tier

The Service Manager web tier contains a J2EE-compliant web application that must run on a web application server. Before you proceed, you must have a supported web application server installed. For the supported versions of different web application servers, see Service Manager9.50 Support Matrix on the HPE Support matrices web site.

Once your web application server is ready for use, deploy the web tier on your web application server. Each web application server has its own method of deploying web applications. See your web application server documentation for specific instructions on deploying a web application. This section provides example implementation instructions.

> **Tip:** If you are upgrading from an earlier version of the web tier, search for "Upgrade the Web Tier" in the Service Manager Help Center.

Enable HTTPOnly and Secure session cookies in your web application server

> **Caution:** Be sure to set up your Web Tier with only the minimum required functionality. Enabling more functionality in web application servers (extra languages or scripts such as VB, PHP, CGI, and so on), increases the risk of security breaches. We recommend that you follow well-known best practices for a secure application server.

It is recommended to enable HTTPOnly and Secure cookies in your web application server to help prevent malicious JavaScript injection and make the browser (or other http clients) only send cookies over SSL connections. For more information, see KM02233778.

Deploy the new web tier

The following table provides a summary of the deployment method required for each supported web application server.

Web application server	Deployment method
Apache Tomcat	Copy the webtier-9.50.war file to the <Tomcat>\webapps folder and start the web application server. For detailed steps, see "Example deployment on Tomcat" below.
IBM Web Application Server	Open the administration console and install the web application from the webtier-ear-9.50.ear file. For detailed steps, see "Example deployment on WebSphere Application Server" on page 68.

Web tier log files: The default log file is sm.log, located in <web app install dir>\bin. You can change the default log file and location in log4jproperties, which is located in <web app install dir>\webtier-9.50\WEB-INF.

Example deployment on Tomcat

This example describes deploying the webtier-9.50.war file on Tomcat 7.0 and 8.0.

1. Log in to the server as a user with local administrator privileges.
2. Stop the Tomcat Web application server.
3. From SM9.50-1.zip, copy or save the webtier-9.50.war file onto your Tomcat webapps directory. For example, C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps.
4. If you use Tomcat 8.0, make sure that you change the "protocol" attribute as the following in the conf\server.xml file on Tomcat:

   <Connector port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol" connectionTimeout="20000" redirectPort="8443" />

   > **Note:** You do not need to do this if you use Tomcat 7.0.

5. Start the Tomcat server. Tomcat automatically opens the webtier-9.50.war file and creates a webtier-9.50 virtual directory.

   If Tomcat does not create a webtier-9.50 directory when started, check the log files and contact support with the information found in the log files.

6. Edit the web.xml file located in the virtual directory to add your server connection information. The settings you define in this file determine the client preferences for all web clients. View the Service Manager online help for a complete list and more detailed explanation of each parameter.

   a. Open the web.xml file in a text editor.

   b. Set the secureLogin, sslPort, serverHost, and serverPort parameters.

Parameter	Default value	Description
secureLogin	true	Controls the encryption of network communication between the web application server and the web browser. Set it to false if you do not use Secure Sockets Layer (SSL) connections to the web server. **Note:** To use secure login, you must enable SSL on your web application server. For details, refer to your web application server documentation.
sslPort	8443	This parameter is needed only when secureLogin is set to true. Set it to the SSL port of the web application server.
serverHost	localhost	Specifies the name of the Service Manager host server.
serverPort	13080	Specifies the communications port number to which the Service Manager server listens.

c. Set other common parameters as desired. The table below lists the commonly set parameters and their default values.

Parameter	Default value	Description
cacerts	WEB-INF/cacerts	Lists the path to the CA certificates required for SSL support.
compress_soap	true	Specifies if you want to use data compression between web clients and the web tier.
helpServerHost		Specifies the name of the Help Server.
helpServerPort		Specifies the communications port number to which the Help Server listens.
helpServerContext	help	Defines the context path when deploying the Service Manager help on a web server (for example, Apache). The context path refers to the virtual directory name where the Service Manager help is installed. It excludes the web server's document directory path. For example, if the help is deployed in C:/Apache/2.2/htdocs/sm_help, the document directory path is C:/Apache/2.2/htdocs/ and the virtual directory name is sm_help. Therefore, the context path is

Parameter	Default value	Description
		sm_help.
showHelp	false	Enabling this parameter causes Web clients to display the **Online Help** and **Shortcut List** options after users click the **Help** (question mark) button. The **Online Help** option allows users to access the Help Server you define in the web.xml file. If this parameter is set to **false**, clicking the **Help** button will directly bring up the web client keyboard shortcut list.
refreshMessages	true	Determines whether the browser checks for new messages from the application server.
refreshMessagesInterval	15000	Determines how often (in milliseconds) the browser checks for new messages from the application server.
ssl	false	Enables the web client to encrypt communications using the server's demonstration certificate.
viewactivenotes	false	Determines whether you see a pop-up message when the server sends a message.

7. Save and close web.xml.
8. Endorsed JAR files are no longer required. If you installed them in previous installations, remove them.
9. Restart the Tomcat server.
10. Set the web application server heap size. The web application server heap size determines how many connections each web application server can handle. Most application servers require a heap size of at least 256 MB for optimal performance. If you experience poor performance from your web client connections, increase the web application server heap size. See your web application server documentation for instructions.

Example deployment on WebSphere Application Server

This example describes deploying the webtier-ear-9.50.ear file on WebSphere Application Server versions 8.5.

1. Log in to the server as a user with local administrator privileges.
2. From the SM9.50-1.zip file, copy or save the webtier-ear-9.50.ear file onto your local system.

3. Start the WebSphere application server.
4. Set the web application server heap size. The web application server heap size determines how many connections each web application server can handle. Most application servers require a heap size of at least 256 MB for optimal performance. If you experience poor performance from your web client connections, increase the web application server heap size. See your web application server documentation for instructions.
5. Log on to the WebSphere administrative console with system administrator privileges.
6. Install the webtier-ear-9.50.ear file.
   a. Go to **Applications > New Application > New Enterprise Application**.
   b. Select **Local file system**, and browse to the webtier-ear-9.50.ear file.
   c. Click **Next**. WebSphere starts uploading the web tier application. This may take a while.
7. Click **Next** to accept the default settings in the next screens until you reach "Step 4: Summary", and then click **Finish**. The installation of the web tier ear file begins.
8. When the installation is complete, click **Save** to save your local configuration changes to the master configuration.
9. The webtier-ear-9.50.ear file contains webtier-9.50.war. Inside of that is the web tier configuration file (web.xml). Edit it to add your server connection information. The settings you define in this file determine the client preferences for all web clients. View the Service Manager online help for a complete list and more detailed explanation of each parameter.
   a. Open the web.xml file in a text editor. The web.xml file is deployed in the following folder: <WebSphere installation path>\AppServer\profiles\<Profile Name>\config\cells\<Node name>Cell\applications\HPE Service Manager 9.50 Web.ear\deployments\HPE Service Manager 9.50 Web\webtier-9.50.war\WEB-INF.

      For example: C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv02\config\cells\IWFVM01268Node02Cell\applications\HPE Service Manager 9.50 Web.ear\deployments\HPE Service Manager 9.50 Web\webtier-9.50.war\WEB-INF.
   b. Set the secureLogin, sslPort, serverHost, and serverPort parameters.

Parameter	Default value	Description
secureLogin	true	Controls the encryption of network communication between the web application server and the web browser. Set it to false if you do not use Secure Sockets Layer (SSL) connections to the web

Parameter	Default value	Description
		server. **Note:** To use secure login, you must enable SSL on your web application server. For details, refer to your web application server documentation.
sslPort	8443	This parameter is needed only when secureLogin is set to true. Set it to the SSL port of the web application server.
serverHost	localhost	Specifies the name of the Service Manager host server.
serverPort	13080	Specifies the communications port number to which the Service Manager server listens.

c. Set other common parameters as desired. The table below lists the commonly set parameters and their default values.

Parameter	Default value	Description
cacerts	WEB-INF	Lists the path to the CA certificates required for SSL support.
compress_soap	true	Specifies if you want to use data compression between web clients and the web tier.
helpServerHost	localhost	Specifies the name of the Help Server.
helpServerPort	80	Specifies the communications port number to which the Help Server listens.
helpServerContext	help	Defines the context path when deploying the Service Manager help on a web server (for example, Apache). The context path refers to the virtual directory name where the Service Manager help is installed. It excludes the web server's document directory path. For example, if the help is deployed in C:/Apache/2.2/htdocs/sm_help, the document directory path is C:/Apache/2.2/htdocs/ and the virtual directory name is sm_help. Therefore, the context path is sm_help.
showHelp	false	Enabling this parameter causes Web clients to display the help server option after users click the

Parameter	Default value	Description
		Help (question mark) icon, which allows users to access the Help Server you define in the web.xml file.
refreshMessages	true	Determines whether the browser checks for new messages from the application server.
refreshMessagesInterval	15000	Determines how often (in milliseconds) the browser checks for new messages from the application server.
ssl	false	Enables the web client to encrypt communications using the server's demonstration certificate.
viewactivenotes	false	Determines whether you see a pop-up message when the server sends a message.

d. Save, close and re-archive the files.

10. Configure the application properties.

a. Go to **Applications > Application Types > WebSphere enterprise applications**.

b. Click **HPE Service Manager9.50 Web** to open the **Configuration** tab, and under **Detail Properties** click **Class loading and update detection**, and make sure the default settings are selected.

Setting	Value (default)
Class load order	Classes loaded with parent class loader first
WAR class loader policy	Class loader for each WAR file in application

c. Click **Apply**.

11. Configure the **HPE Service Manager** module.

a. Go to **Applications > Application Types > WebSphere enterprise applications > HPE Service Manager 9.50 Web > Manage Modules**.

b. Click the **HPE Service Manager** module, and select the following setting.

Setting	Value
Class load order	Classes loaded with local class loader first (parent last) **Note:** Keep the other settings on the page as default.

c. Click **Apply**.

12. Configure the default http transport port of the WebSphere application server.

> **Note:** You will use this port when launching the Service Manager web client.

a. Go to **Servers** > **Server Types** > **WebSphere application servers > server 1**.

b. In the **Communications** > **Ports** section, make note of the **WC_defaulthost** port number (for example, 9082).

c. You can change this port number to one that is not in use (for example, 9085). This port number is automatically synchronized to the port number in **Application Servers > Server 1 > Web container transport chains > HttpQueueInboundDefault**.

d. Click **Environment > Virtual hosts > default_host > Host Aliases**, and make sure that the port number is in the Host Aliases list. If it is not, do the following to add the WC_defaulthost port number to the list.

i. Click **New**.

ii. Type the following port information:

- *Host Name*: ***
- *Port:* xxxx (for example, **9085**)

iii. Click **Apply** and then click **OK**. The port number is added to the Host Aliases list of default_host.

e. Click **Save** to save the changes to the master configuration.

f. Restart the WebSphere Application Server.
Now the server will start binding to the new port.

> **Note:** If you did not change the port number, you do not need to restart the server.

13. Add a Web container custom property setting. This step is required for particular error pages that match the error exception types defined in the web tier configuration file (web.xml) to display in the user's web browser.

a. In the administrative console, click **Servers** > **Server Types** > **WebSphere application servers**.

b. Click the server to which the custom property is to be applied.

c. Under **Configuration** > **Container settings**, click **Web Container Settings** > **Web container**.

d. Under **Configuration** > **Additional Properties**, click **Custom Properties**.

e. On the Custom Properties page, click **New**.

f. On the settings page, enter the following values in the Name and Value fields:

Name:**com.ibm.ws.webcontainer.enableErrorExceptionTypeFirst**

Value: **true**

g. Click **Apply** or **OK**.

h. In the "Messages" box that appears, click **Save**.

i. Restart the server for the custom property to take effect.

14. Go to **Applications** > **Applications Type** > **WebSphere enterprise applications**, select **HPE Service Manager 9.50 Web**, and click **Start**.

    When the application is successfully started, its state changes to green.

15. Launch the Service Manager web client using a URL like the following:
    http://<*WAS application server name*>:<*Port*>/webtier-9.50/index.do
    where: <*Port*> is the WC_defaulthost port number.

    For example: http://abc.def.hp.net:9085/webtier-9.50/index.do

Now, the new web tier is deployed. Next, you need to configure more web tier parameters or restore your previous configurations if you have upgraded from an existing web tier. For information about web tier configurations, see the Service Manager Help Center.

Configure a web server to redirect requests to the web tier

You can configure a web server to redirect web-client specific URLs to the Service Manager Web tier. The following instructions illustrate redirecting requests from a Windows Internet Information Services (IIS) web server to the default Web tier URL.

Edit the workers2.properties file in IIS to include the following five parameters:

- [uri:/webtier-9.50/servlet/*]
  info=Prefix mapping
- [uri:/webtier-9.50/*.jsp]
  info=Extension mapping
- [uri:/webtier-9.50/*.do]
  info=Extension mapping
- [uri:/webtier-9.50/attachments/*]
  info=Extension mapping
- [uri:/webtier-9.50/cwc/nav.menu]
  info=Extension mapping

> **Note:** If you change the default application name from webtier-9.50, you will need to change the URI mappings to match your Web tier's application name.

Access Service Manager by using a web client

To connect to Service Manager by using a browser:

1. Use the following URLs to access Service Manager from the web tier.
   For <*server*>, type the name of the web server running the web tier.
   For <*port*>, type the communications port number used to connect to the web tier.
   - Standard web client: http://<server>:<port>/webtier-9.50/index.do
   - Employee self-service web client: http://<server>:<port>/webtier-9.50/ess.do
   - Accessible web client: http://<server>:<port>/webtier-9.50/accessible.do. The accessible web client does not display a record list detail page.
   - Accessible employee self-service web client: http://<server>:<port>/webtier-9.50/accessible_ess.do

     > **Note:** You do not need to specify the communications port in the web tier URL if you use the default web server port (port 80). See your web server documentation for instructions on setting the communications port.
2. Enter the following information:
   - **User name** and **Password**: The user name and password that you use to log in to the server

     > **Note:** The login account that you enter must already exist in Service Manager. Service

> Manager provides an out-of-box login account with System Administrator privileges: **System.Admin** (with a blank password). HPE recommends that you disable this account or change its password after creating accounts for all of your users. For information about how to create user accounts, see the Service Manager help.

- Language: The language to use for this session (can differ from the language set on the computer)

3. Click **Log In**.

> **Note:** After logging in, do not use the buttons (such as Refresh, Back, and Forward) on your browser toolbar or their keyboard shortcuts (such as **Ctrl+R**, **Ctrl+Left**, and **Ctrl+Right**) to perform Service Manager actions. Instead, use the buttons on the Service Manager user interface.

Install language packs

Service Manager language packs are intended for new installations of Service Manager only. Once you have installed the Service Manager Server and Windows Client, you are ready to install the language packs.

> **Tip:** If you are upgrading to the current version, you need to run the Service Manager Upgrade Utility to upgrade your language packs instead of installing the language packs. The Upgrade Utility not only upgrades your applications to the current version, but also upgrade your language packs. For details, see the *Service Manager Upgrade Guide*.

> **Note:** The officially supported languages of Service Manager can meet most localization requirements. However, if you need to localize Service Manager into an unofficially supported language, refer to the Service Manager Open Localization Toolkit Documentation in the Service Manager Document Matrix.

Follow these instructions to install a language pack.

Language pack installation prerequisites

Important: If you are using a SQL Server database, make sure your database supports the languages that you want to install. When configuring a SQL Server database connection for the Service Manager Server, use the **Use Unicode Data Type** option if you need to support multiple languages that are not supported by one collation, otherwise use the right collation and do not select this option (see "Prepare your RDBMS" on page 24). For information about how to select SQL Server collations, refer to the SQL Server documentation.

Before you install HPE Service Manager 9.50 language packs, you must perform the following tasks:

1. Install the following components from the Service Manager installation media, if you have not done so already:
   - Service Manager 9.50 server
   - Service Manager 9.50 applications
   - Help (if you want an English version of the help)

   Note: You can install the latest patch because some issues might have been fixed in the patch releases.

   See the localized versions of the *HPE Service Manager 9.50 Installation Guide* on the Language Pack installation package for installation instructions for these components.
2. Back up your Service Manager application data.

Perform the following steps if you want to customize your Windows client.

1. Install the Client Configuration Utility from the English installation media.

   This task is needed only if you want to make customizations to your Windows clients such as changing the splash screen, adding custom images, adding company branding, saving default settings and connections, and configuring connections to a help server or update site.

   See the localized *HPE Service Manager 9.50 Installation Guide* on the Language Pack installation media for instructions on using the Client Configuration Utility.
2. Open the Client Configuration Utility and customize any additional settings you want the multilanguage Windows client to have.
3. Deploy the customized and localized Windows client installer to your development environment.

Installing the language pack

You must install the language pack on the same system where you installed the Service Manager server. You can install multiple languages on a Service Manager server. This allows users to select the language in which they want Service Manager to display the application forms.

While the server displays Service Manager application forms in the selected language, the operating system language of the client determines the language in which the client menus are displayed. For example, a Windows client running on an English operating system will display menus in English even though the application forms might be in Japanese.

You can install the Service Manager server language pack on either a Windows or Unix system.

Windows installation requirements

- Compatible Windows operating system (See the Service Manager support matrix at https://softwaresupport.hpe.com/group/softwaresupport/support-matrices)
  - Install the most current Windows updates
  - Install the Windows language pack
- Existing Service Manager server installation (in English)
  - Back up your application data
- 190 MB disk space for each language pack you install

Unix installation requirements

- Compatible Unix platform (See the Service Manager support matrix at https://softwaresupport.hpe.com/group/softwaresupport/support-matrices)
  - Install the most current Unix platform updates
  - Install the Unix language pack
- Existing Service Manager server installation (in English)

- Back up your application data
- 210 MB disk space per language installed

Service Manager language pack setup

Use the following steps to install the Service Manager server Language Pack.

> **Note:** Make sure that you use the same account that you used for the Service Manager server installation.

Preparation for installation

1. Extract the HPE Service Manager Language Pack installation package into an appropriate drive of the server.
2. Open the ClickMe.html file.
3. Click a flag icon to select an appropriate language. The corresponding information for this language pack and documentation is displayed.

Installation for Windows system

1. Run the Windows language pack installer (Setup.exe) to start the installation for Windows.
2. Select the language for the installation wizard, and then click **OK**. The setup wizard opens the installer in the language you selected, and the Installation Introduction page opens.
3. Click **Next** to read and accept the license agreement.
4. Select the **I accept the terms of the License Agreement** option if you accept the terms. The **Next** button becomes active.
5. Click **Next** to set the destination folder. The Destination Folder page opens.
6. Select the location where you have installed the Service Manager server.

   > **Note:** The Language Pack must be installed in the directory where the Service Manager server is installed.

7. Click **Next** to prepare the installation process. The Pre-installation Summary page opens.
8. Click **Install** to start the installation of the language pack. You can stop the installation by clicking **Cancel**.

   > **Note:** The setup wizard automatically uploads language data to your database. This process may take twenty minutes or more, depending on your system performance.

   The Install Complete page opens when the language data is successfully uploaded.
9. Click **Done** to exit the Setup wizard.
10. Restart your Tomcat server. The installed language is available upon your next login.

Installation for Linux

Run the Linux language pack installer (setupLinuxX64.bin) to start the installation for Linux.

You can install the language pack for Linux by using the command interface or the GUI interface. Follow corresponding instructions in the installer to install the language pack step by step.

> **Note:** It may take twenty minutes or more to load the language pack data, depending on your system performance.

Install and set up Service Manager Service Portal

As an end user portal built on the modern technology of HPE Propel , Service Manager Service Portal enables IT departments to offer their services in an online shopping experience, similar to what users experience today at popular online retailers. With Service Manager Service Portal, users can order, track, and manage their IT services, access knowledge articles, initiate chat conversations, and complete surveys.

- Service Manager Service Portal must be deployed on a Red Hat Enterprise Linux 7.2 system.
- The default passwords for the **consumer**, **orgadmin**, and **admin** users are listed in this section. To prevent access to your Service Manager Service Portal installation via these default passwords, you must change them. Refer to the Service Manager Service Portal Administration Guide for instructions.

This section provides instructions on how to install and set up a single instance of Service Manager Service Portal, as well as a distributed Service Manager Service Portal cluster.

Install and set up a single Service Manager Service Portal instance

Complete the following steps to install and set up a single instance of Service Manager Service Portal.

Tip: For instructions on high availability configuration of Service Manager Service Portal, see "Deploy a distributed Service Manager Service Portal cluster" on page 129.

Register your system to the Red Hat Subscription service

Service Manager Service Portal must be installed on a Red Hat Enterprise 7.2 system, and the installation requires the downloading of certain packages from the Red Hat Customer Portal. To be able to download the required packages during the installation, you must register your Red Hat 7.2 system to the Red Hat Subscription service.

> **Note:** Before you proceed, make sure your Red Hat system has Internet access.

To do this, follow these steps:

1. Log in to your Red Hat 7.2 system as root.
2. Run the following command followed by the credentials used to log in to Red Hat Customer Portal:

   ```
   subscription-manager register
   ```

3. Run the following command:

   ```
   subscription-manager attach --auto
   ```

Now, you are ready to install Service Manager Service Portal. See "Install Service Manager Service Portal" below.

Install Service Manager Service Portal

> **Important:** Before you proceed, make sure the following prerequisites are met:

- You have already registered your Red Hat 7.2 system to the Red Hat Subscription service. For details, see "Register your system to the Red Hat Subscription service" on the previous page.
- Your Red Hat 7.2 system has Internet access.

Tip: To assist copying and pasting commands from these installation instructions into your Red Hat 7.2 system's terminal window, set the $PROPEL_HOSTNAME environment variable to the Red Hat 7.2 system's fully qualified domain name. For example:

```
# export PROPEL_HOSTNAME=`hostname --fqdn`
```

Where `hostname --fqdn` returns the fully qualified domain name for your Red Hat 7.2 system.

(This environment variable is temporary and needs to be set after rebooting the Red Hat 7.2 system.)

Perform the following steps to install Service Manager Service Portal:

1. Log in to the Red Hat 7.2 system as the root user.
2. Create the Service Manager Service Portal directory structure:

   ```
   # mkdir /opt/hp
   # cd /opt/hp
   ```

3. From the Service Manager installation package SM950-1.zip, copy the archive file containing the installers and Ansible playbooks (propel_complete_installer.zip) to the /opt/hp directory on the Red Hat 7.2 system.
4. Unpack the propel_complete_installer.zip archive file:

   ```
   # unzip propel_complete_installer.zip
   ```

5. Install Ansible, depending on whether or not you need to use a proxy:
   - Without proxy:

     ```
     # cd /opt/hp/propel_complete_installer
     # ./install_ansible.sh 2>&1 | tee install_ansible.log
     ```

   - With proxy:

     ```
     # cd /opt/hp/propel_complete_installer
     # ./install_ansible.sh --proxy http://<Proxy_Hostname>:<Proxy_Port> 2>&1 |
     tee install_ansible.log
     ```

6. Prepare the Ansible environment for the Service Manager Service Portal prerequisites:
   a. Reset the SSH keys:

      ```
      # ssh-keygen -t rsa
      ```

Type the file name in which to save the key ("/root/.ssh/id_rsa") and then press Enter. Type the passphrase (empty for no passphrase) and then press Enter. Type the same passphrase again and then press Enter.

```
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@$PROPEL_HOSTNAME
```

b. Verify the SSH keys:

```
# ssh 'root@$PROPEL_HOSTNAME'
```

c. Prepare for the Ansible playbook:

```
# mkdir /opt/hp/propel_complete_installer/ansible_content/ssh
# cd /opt/hp/propel_complete_installer/ansible_content/ssh
# cp ~/.ssh/* .
# cp id_rsa id_rsa-propel
```

d. Obtain the fully qualified domain name (FQDN) for the Red Hat 7.2 system by running the following command. It will be used in the next step as the <Host.Domain.Com> value:

```
# hostname --fqdn
```

e. Add the fully qualified domain name of the Red Hat 7.2 system to the [redhat] section in the `ansible_targets` file:

```
# cd /opt/hp/propel_complete_installer/ansible_content
# vim ansible_targets
```

```
[redhat]
<Host.Domain.Com> ansible_ssh_user=root ansible_ssh_private_key_
file=./ssh/id_rsa-propel
```

7. Run the Ansible playbook to install the Service Manager Service Portal prerequisites, depending on whether or not you need to use a proxy:

   - Without proxy:

     ```
     # ansible-playbook -i ansible_targets deploy_rhel_complete.yml 2>&1 | tee
     ansible_deploy_rhel_complete.log
     ```

   - With proxy:

     ```
     # ansible-playbook -i ansible_targets deploy_rhel_complete.yml --extra-vars
     "httpproxy=http://<Proxy_Hostname>:<Proxy_Port> httpsproxy=http://<Proxy_
     Hostname>:<Proxy_Port>" 2>&1 | tee ansible_deploy_rhel_complete.log
     ```

8. Unpack the Service Manager Service Portal installer:

   ```
   # cd /opt/hp/propel_complete_installer
   # unzip propel-setup.zip -d /opt/hp
   ```

9. Create the Service Manager Service Portal-generated SSL certificates:

> **Important:** Third-party or corporate CA-signed certificates should be used in production systems; however, self-signed certificates generated by Service Manager Service Portal can be used in nonproduction systems. The `auto` option of the `propel-ssl-setup.sh` utility creates Service Manager Service Portal-generated certificates. To replace these types of certificates, see "Replace the Service Manager Service Portal generated SSL certificates" on page 98.

```
# cd /opt/hp/propel-setup*
# export PROPEL_HOSTNAME=`hostname --fqdn`
# ./propel-ssl-setup.sh auto --hostname $PROPEL_HOSTNAME [<CA_SUBJECT>] 2>&1 |
tee ssl-setup.log
```

Where $PROPEL_HOSTNAME is the fully qualified domain name for the Service Manager Service Portal system and CA_SUBJECT is the optional CA subject. By default the string "/CN=Generated Propel CA" is used. If you specify the CA_SUBJECT option, pay attention to the following:

- The "CN" field must be present and in uppercase. The value for "CN" can be any string.
- This is the subject of your private Service Manager Service Portal CA, not your Service Manager Service Portal system; it is not used for the hostname.
- All fields must be separated with a slash ("/").

10. Make sure your OpenJDK version is set to Java 1.8.x. You can verify this by running the command:

    ```
    # java –version
    ```

    If the OpenJDK version is not Java 1.8.x, you can change it by running the following command:

    ```
    /usr/sbin/alternatives --config java
    ```

    Choose the correct version and confirm it by pressing Enter.

11. Run the Service Manager Service Portal setup utility:

    ```
    # ./setup.sh install $PROPEL_HOSTNAME 2>&1 | tee install.log
    ```

    Where $PROPEL_HOSTNAME is the fully qualified domain name for the Service Manager Service Portal system. The output and any errors from the `setup.sh` utility are captured in the `install.log` file.

12. Start the Service Manager Service Portal services:

    ```
    # propel start
    ```

13. Run the Ansible playbooks to finalize the Service Manager Service Portal installation:

a. Configure LW-SSO:

```
# cd /opt/hp/propel_complete_installer/ansible_content
# ansible-playbook -i ansible_targets configure.yml --tags "initLWSSO" --
extra-vars '{"lwsso_init_string":"LWSSO_INIT_STRING"}'
```

Where the LWSSO_INIT_STRING must match the **initString** value in the `lwssofmconfig.xml` file located in the Service Manager Server's RUN directory.

> **Note:** This step configures LW-SSO in the following files:
>
> - /opt/hp/propel/idm-service/idm-service.war/WEB-INF/hpssoConfig.xml
> - /opt/hp/propel/sx/WEB-INF/classes/config/lwssofmconf.xml

b. Enable Chat:

> **Important:** Before you proceed, make sure that you have Service Manager Collaboration successfully deployed.

```
# ansible-playbook -i ansible_targets configure.yml --tags "enableChat" --
extra-vars '{"toggle_chat":"true","chat_url":"https://<ChatUI_url>"}'
```

> **Note:** You need to replace **https://<ChatUI_url>** with **https://<Apache server host>/chatui**, where <Apache server host> is the FQDN of the Apache server that you installed when deploying Service Manager Collaboration. For example: https://sm950.training.com/chatui.

> **Important:** If using SSL, the Apache server and Service Manager Service Portal must use SSL certificates issued by the same Certificate Authority (CA), and the SSL certificates (or the CA) must be trusted by the user's browser.

c. Enable Survey:

```
# ansible-playbook -i ansible_targets configure.yml --tags "enableSurvey" --
extra-vars '{"toggle_survey":"on","service_manager_url":"http(s)://<SM_
url>"}'
```

> **Note:** Replace the "service_manager_url" parameter value with your Service Manager Server web service base URL: For example: https://mysmhost.mycompany.net:13443. For security reasons, https is strongly recommended.

d. Install the Service Manager Service Portal online help:

```
# ansible-playbook -i ansible_targets configure.yml --tags "overrideDoc" --
extra-vars '{"doc_mode":"sm"}'
```

e. Enable rebranding:

```
# ansible-playbook -i ansible_targets configure.yml --tags "enableServices"
--extra-vars '{"toggle_services":"off"}'
```

14. Restart the Service Manager Service Portal services:

```
# propel stop
# propel start
```

Congratulations, you have successfully installed Service Manager Service Portal. You can now log in to Service Manager Service Portal by opening a browser window and entering any of the following URLs for the three Service Manager Service Portal roles:

- Service Manager Service Portal Administrator: https://$PROPEL_HOSTNAME:9000/org/Provider (Use "admin" as the user and "propel" as the password.)
- Organization Administrator: https://$PROPEL_HOSTNAME:9000/org/CONSUMER (Use "orgadmin" as the user and "propel" as the password.)
- Consumer: https://$PROPEL_HOSTNAME:9000/org/CONSUMER (Use "consumer" as the user and "propel" as the password.)

Continue with the following tasks:

- Installing a permanent license. For details, see "Install a permanent license" below. You can skip this step for a test environment.
- Setting up LDAP in Service Manager and Service Manager Service Portal. For details, see "Configure LDAP" on the next page.

> **Tip:** If you need to uninstall Service Manager Service Portal, see "Uninstall Service Manager Service Portal" on page 128.

Install a permanent license

A free license is required for Service Manager Service Portal. When installing Service Manager Service Portal, an instant-on license is installed. This license is temporary and limited to 60 days. In a production environment, you need to install a permanent one, which is provided by HPE for Service Manager customers for free.

- Only one license is required no matter whether you have deployed a single instance of Service

Manager Service Portal or a distributed Service Manager Service Portal cluster.

- To use the same license, the Service Manager Service Portal hosts in a clustered environment must meet this requirement: The first three sections of their IP addresses are the same (for example: 10.255.255.*).

To upload a license into Service Manager Service Portal, follow these steps:

1. Log in to Service Manager Service Portal as the administrator, using the following URL and user account:

   https://<Service Manager Service Portal host FQDN>:9000/org/Provider (Use "admin" as the user and "propel" as the password.)
2. Click the avatar and then select **License**. The License Management view opens.
3. In the License Management view, click **Upload License**.
4. In the File Upload dialog, select the Service Manager Service Portal license that you obtained, and then click **Open**.

   The license is applied and details are displayed in the License Management view.

Configure LDAP

Service Manager Service Portal has bundled HPE Identity Manager (IdM) as an identity management tool, which must integrate with an Active Directory system for user authentication.

Important: To prevent errors in Service Manager Service Portal log files that are related to unknown users, HPE recommends that Service Manager shares the same LDAP server with Service Manager Service Portal; otherwise, identically named users need to be created on both the Service Manager Service Portal system and the Service Manager system.

Tip: For more information on how to configure LDAP in Service Manager Service Portal, see the *Service Manager Service Portal Admin Help*.

Configure LDAP in Service Manager

For information on how to configure LDAP in Service Manager, see the *Lightweight Directory Access Protocol (LDAP)* section in the *Service Manager Help Center* and the *Service Manager LDAP Best*

Practices Guide.

Configure LDAP in Service Manager Service Portal

To configure LDAP in Service Manager Service Portal, perform the following tasks.

> **Tip:** The following steps use an out-of-box organization named Consumer for example. You can create your own organization either by using the **Add Organization** button or updating an out-of-box one.

Task 1. Configure an LDAP server

To do this, follow these steps:

1. Log in to Service Manager Service Portal as the administrator, using the following URL and user account:

   https://<Service Portal host name>:9000/org/Provider (Use "admin" as the user and "propel" as the password.)

2. Click **Identity**. The Organization List displays two out-of-box organizations: Consumer, and Provider.
3. Select **Consumer**.
4. On the **Authentication** tab, click **Add Configuration**.
5. Select the **LDAP Configuration** authentication type, and then click **Create**.
6. Configure the following settings.

   LDAP Server Information

Item	Description	Example value
Display Name	The display name for the LDAP server.	aaa
Hostname	The fully-qualified LDAP server domain name (server.domain.com) or IP address.	10.255.255.255
Port	The port used to connect to the LDAP server (by default, 389).	389
SSL Connection	If the LDAP server is configured to require ldaps (LDAP over SSL), select the SSL Connection checkbox.	Not selected

Item	Description	Example value
Base DN	Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the basis of a search.	dc=maxcrc,dc=com
User ID (Full DN)	The fully distinguished name of any user with authentication rights to the LDAP server. If the LDAP server does not require a User ID or password for authentication, this value can be omitted.	cn=Manager,dc=maxcrc,dc=com
Password	Password of the User ID. If the LDAP server does not require a User ID or password for authentication, this value can be omitted.	
Retype Password	Retype the password of the User ID.	

LDAP Attributes

Item	Description	Example value
Full Name	The name of the LDAP attribute used to store the full name of the user. Often, this is cn or Display Name, but different LDAP directories may use different attributes. Contact your LDAP administrator to determine the proper Full Name. Default: cn	cn
User Email	The name of the attribute of a user object that designates the email address of the user. The email address is used for notifications. If a value for this attribute does not exist for a user, the user does not receive email notifications. Default: mail	mail
Group Membership	The name of the attribute(s) of a group object that identifies a user as belonging to the group. If multiple attributes convey group membership, the attribute names should be separated by a comma. Default: member,uniqueMember	memberOf
Manager Identifier	The name of the attribute of a user object that identifies the manager of the user. Default: manager	manager
Manager	The name of the attribute of a user object that describes the	managedObjects

Item	Description	Example value
Identifier Value	value of the Manager Identifier's attribute. For example, if the value of the Manager Identifier attribute is a distinguished name (such as cn=John Smith, ou=People, o=xyz.com) then the value of this field could be dn (distinguished name). Or, if the Manager Identifier is an email address (such as admin@xyz.com) then the value of this field could be email. Default: dn	
User Avatar	LDAP attribute whose value is the URL to a user avatar image that is displayed for the logged-in user. If no avatar is specified, a default avatar image is used.	Empty value

User login Settings

tem	Description	Example value
User Name Attributes	The name of the attribute of a user object that contains the username that will be used to log in. The value for this field can be determined by looking at one or more user objects in the LDAP directory to determine which attribute consistently contains a unique user name. Often, you will want a User Name Attribute whose value in a user object is an email address. Examples: userPrincipalName or sAMAccountName or uid	uid
User Searchbase	The location in the LDAP directory where users' records are located. This location should be specified relative to the Base DN. If users are not located in a common directory under the Base DN, leave this field blank. Examples: cn=Users or ou=People	ou=Users
User Search Filter	Specifies the general form of the LDAP query used to identify users during login. It must include the pattern {0}, which represents the user name entered by the user when logging in. The filter is generally of the form {<attribute>= 0}, with<attribute> typically corresponding to the value entered for User Name Attribute. Examples: userPrincipalName={0} or sAMAccountName={0} or uid={0}	uid={0}
Search Option (Search Subtree)	When a user logs in, the LDAP directory is queried to find the user's account. The Search Subtree setting controls the depth of the search under User Searchbase.	Not selected

tem	Description	Example value
	If you want to search for a matching user in the User Searchbase and all subtrees under the User Searchbase, make sure the Search Subtree checkbox is selected. If you want to restrict the search for a matching user to only the User Searchbase, excluding any subtrees, unselect the Search Subtree checkbox.	

7. Save the configuration.
8. Click **Save**.

Task 2. Create groups

There are two ways to create groups in Service Manager Service Portal: synchronize groups from LDAP, or manually create groups in Service Manager Service Portal.

Synchronize groups from LDAP

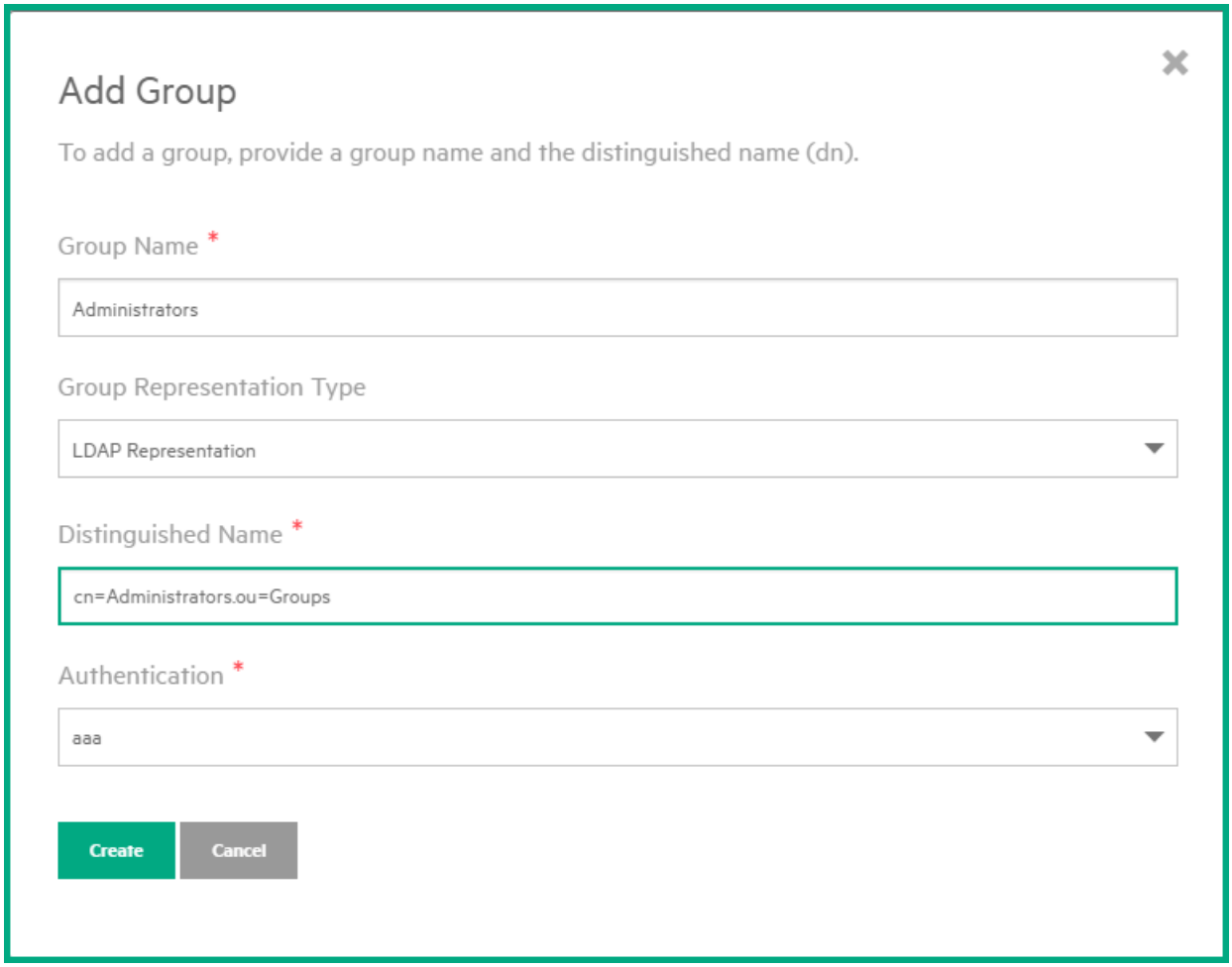
You are recommended to create groups in LDAP and then synchronize the groups to Service Manager Service Portal.

To synchronize a group from LDAP, follow these steps:

1. Log in to Service Manager Service Portal:

   https://<Service Portal host name>:9000/org/Provider (Use "admin" as the user and "propel" as the password.)
2. Click **Identity**. The Organization List displays two out-of-box organizations: Consumer, and Provider.
3. Select **Consumer** from the organization list.
4. On the **Groups** tab, click **Add Group**.
5. Enter the following information:
   - Group Name: Enter a name for the LDAP group. It can be the same name as the group name in LDAP or a different one.
   - Group Representation Type: Select **LDAP Representation**.
   - Distinguished Name: Enter a value according to your LDAP data hierarchy. For example: cn=<Group Name in LDAP>.ou=Groups
   - Authentication: Select the LDAP server you configured.

The following figure shows an example.



6. Click **Create**. The Group is added to the **Groups** tab.
7. Repeat the steps for the rest of your LDAP groups.

Manually create groups in *Service Manager Service Portal*

If you have no groups created in LDAP, you can manually create them in Service Manager Service Portal. To do this, follow these steps:

1. Log in to Service Manager Service Portal:

   https://<Service Portal host name>:9000/org/Provider (Use "admin" as the user and "propel" as the password.)
2. Click **Identity**. The Organization List displays two out-of-box organizations: Consumer, and Provider.

3. Select **Consumer** from the organization list.
4. On the **Groups** tab, click **Add Group**.
5. Enter the following values:
   - Group Name: enter a name. For example: admingroup.
   - Group Representation Type: Select **Database Representation**.
   - Associated User: Leave this field empty, as there are no users available to add at this point.
6. Click **Create**. The Group is added to the **Groups** tab.

> **Note:** Do not log out. Continue with associating user roles to the groups that you created.

Task 3. Associate user roles to the groups

After the groups are created, add user roles to the groups. To do this, follow these steps:

1. Select the group you created, and then click the Edit icon.
2. Click the **Associated Roles** field, select the **Consumer** role from the list, and then click **Add Role** to add the role to this group. Click **Save**. The Consumer role is associated to the group.

> **Note:** Service Manager Service Portal provides two out-of-box roles: Consumer, and Organization Administrator. You can create more rules if needed. For details, see the Service Manager Service Portal Admin Help.

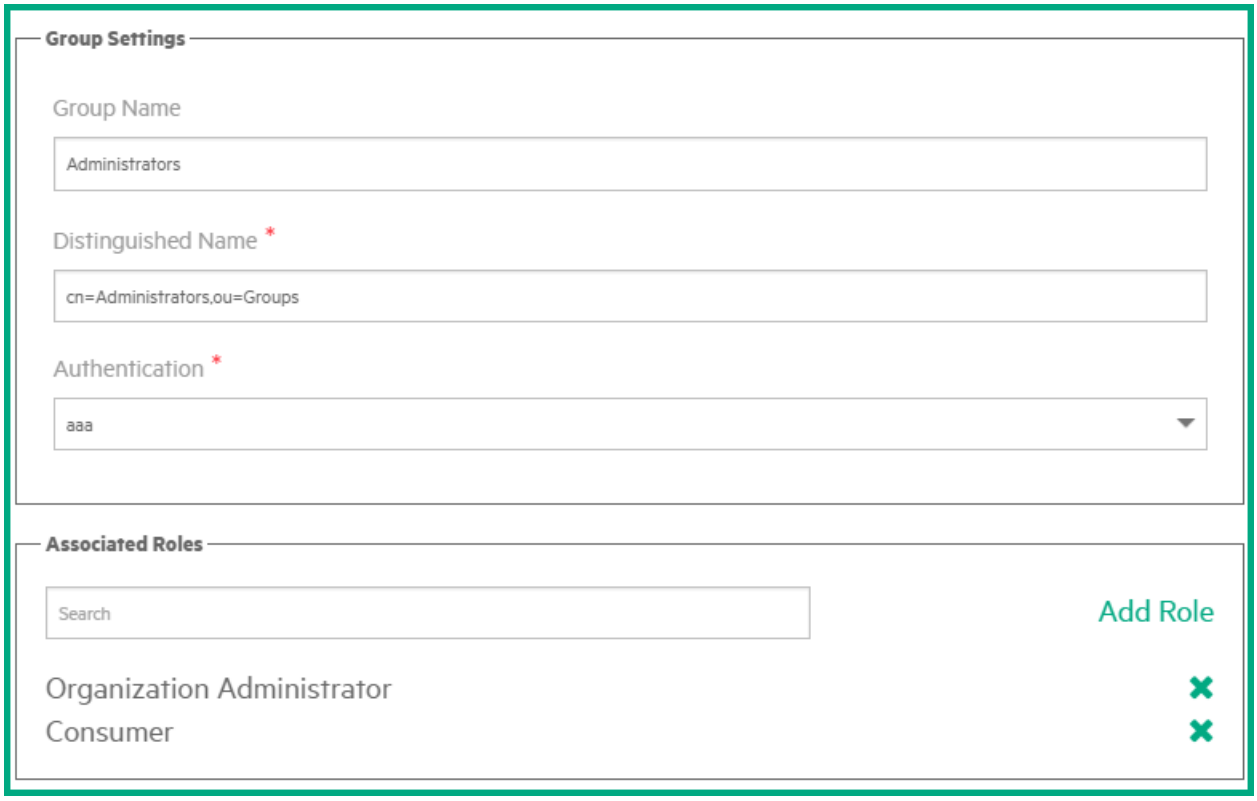
3. If needed, repeat the previous step to add more roles to the group.

> **Note:** Do not log out. Continue with adding the groups as impersonation groups.

The following figures shows examples.

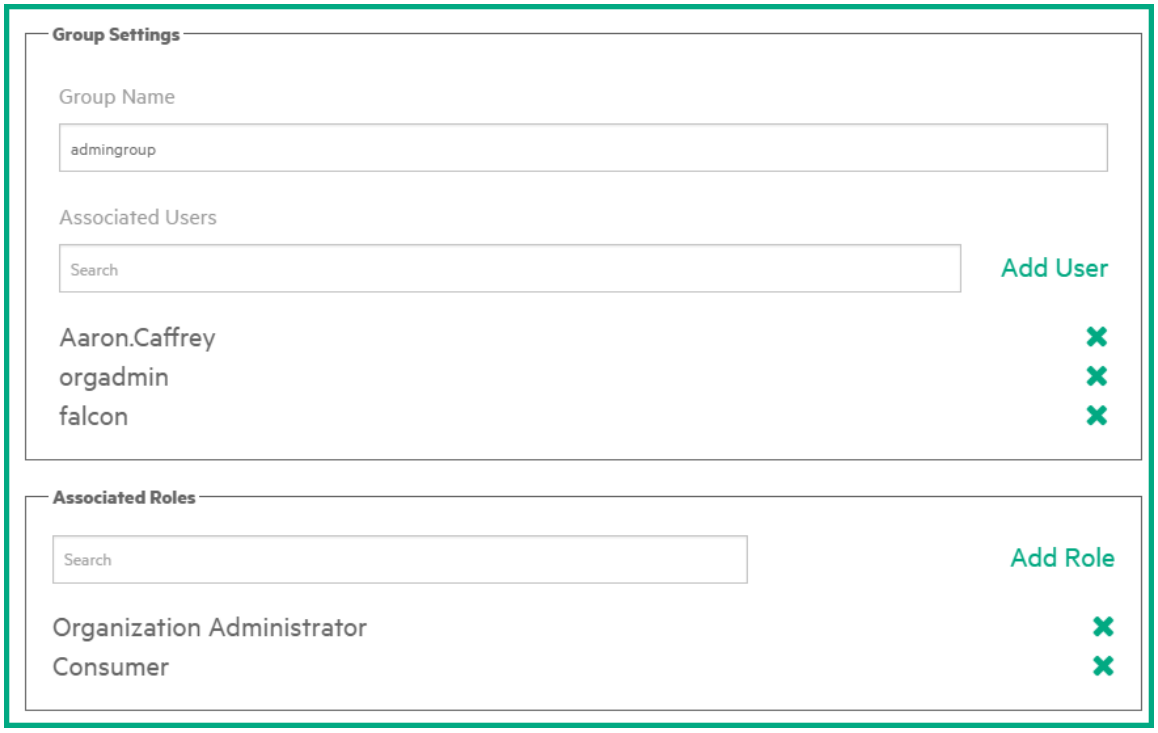
Example 1: User roles are associated to a group synchronized from LDAP.

> **Note:** You do not need to add LDAP users to this group (see "Task 6. Add LDAP users to each of the groups" on page 97). When logged in, the LDAP users in this group will be automatically granted the permissions of the group user roles.



Example 2: User roles are associated to a group manually created in Service Manager Service Portal.

> **Note:** Later, you will need to manually add users to this group. (see "Task 6. Add LDAP users to each of the groups" on page 97).



Task 4. Add the groups as impersonation target groups

Members of a organization's group can request catalog items on behalf of members in a different group within the organization. This capability is called request on behalf (RoB). This task is needed to enable the RoB capability for the groups.

To do this, follow these steps:

1. Click the **Impersonation** tab.
2. Click **Add Group**.
3. Select a group you created, and then click **Save**.
4. Repeat the steps for the rest of the groups.
5. Log out of Service Manager Service Portal.

Task 5 Create LDAP users in Service Manager Service Portal

> **Note:** An LDAP user is not created in Service Manager Service Portal until the user is logged in to Service Manager Service Portal. Once an LDAP user is created in Service Manager Service Portal, you are able to add the user to a group.

To do this, follow these steps:

1. Log in to Service Manager Service Portal with an LDAP user account:

   https://<Service Portal host name>:9000/org/Consumer (Use an LDAP user account: for example, "falcon" as the user and "1Qaz2wsx" as the password.)

   If you are successfully logged in, your LDAP configuration is working correctly.

2. Log out of Service Manager Service Portal.

The user (falcon) is now created in Service Manager Service Portal. You can add it to a group now.

Task 6. Add LDAP users to each of the groups

> **Tip:** This task is not needed if you selected to synchronize groups from LDAP, because users are synchronized along with each group. If you selected to manually create user groups, perform this step.

To do this, follow these steps:

1. Log in to Service Manager Service Portal:

   https://<Service Portal host name>:9000/org/Provider (Use "admin" as the user and "propel" as the password.)

2. Add LDAP users to each group.

   To add LDAP user to a group, follow these steps:

   a. Click **Identity**. The Organization List displays two out-of-box organizations: Consumer, and Provider.

   b. Select **Consumer** from the organization list.

   c. On the **Groups** tab, select a group that you created, and then click the Edit icon.

   d. Click the **Associated Users** field, select a user (for example, falcon) from the list, and then click **Add User**. The LDAP user is added to the group.

   e. Repeat the steps to add more LDAP users to the group.

   f. Click **Save**.

   > **Note:** Repeat the steps for the rest of the groups.

> **Tip:** Next, you need to add the RESTful API and SOAP API capabilities in Service Manager for users that need to connect to Service Manager from Service Manager Service Portal. For details, see "Add the RESTful API and SOAP API capabilities for Service Manager users" on the next page.

Add the RESTful API and SOAP API capabilities for Service Manager users

When Service Manager Service Portal is connected to Service Manager, which works as a supplier to Service Manager Service Portal, users must have the RESTful API and SOAP API capabilities to use all of the functionalities such as shopping, ticketing, survey, and so on.

The Service Manager administrator needs to add these capabilities for each user that needs to connect to Service Manager from Service Manager Service Portal.

To add the capability words for a user, follow these steps:

1. Log in to Service Manager as a system administrator.
2. Enter **operator** in the command line, and press Enter.
3. Enter your search criteria and click **Search**.
4. Select a user (operator) from the list, and then select the **Startup** tab.
5. Go to the **Execute Capabilities** section, and add **RESTful API** and **SOAP API** to the list.
6. Save the operator record.

> **Tip:** Next, you can optionally configure SSL between Service Manager and Service Manager Service Portal. For details, see "Replace the Service Manager Service Portal generated SSL certificates" below and "(Optional) Configure SSL for a Service Manager supplier" on page 107.
>
> Alternatively, you can skip the SSL steps and jump to the step to add a Service Manager supplier. For details, see "Add Service Manager as a supplier" on page 110.

Replace the Service Manager Service Portal generated SSL certificates

Service Manager Service Portal requires HTTPS (HTTP over SSL) for client browsers. Configuring HTTPS between Service Manager Service Portal and the Service Manager Server is optional but recommended. Third-party or corporate CA-signed certificates should be used in production systems;

however, self-signed certificates generated by Service Manager Service Portal can be used in non-production systems.

Important: Although HPE Service Manager Service Portal-generated certificates can be configured during installation and used in production, HPE recommends that you configure trusted certificates from a Certificate Authority (CA). Some organizations issue certificates that are signed by a corporate CA and some organizations get certificates from a trusted third-party CA, such as VeriSign.

This section explains how to replace the previously HPE Service Manager Service Portal-generated SSL certificates with CA-signed SSL certificates.

Note: The HPE Service Manager Service Portal-generated SSL certificates are created and configured by using the `/opt/hp/propel-setup/propel-ssl-setup.sh auto` command when installing HPE Service Manager Service Portal.

- In the following instructions, `$PROPEL_VM_HOSTNAME` represents the fully qualified domain name of the HPE Service Manager Service Portal host. You can set this as an environment variable with the following command on the HPE Service Manager Service Portal host:

  ```
  # export PROPEL_VM_HOSTNAME=`hostname --fqdn`
  ```

- The password is “changeit” for the HPE Service Manager Service Portal global Java keystore (`/usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts`)
- The password is “propel2014” for the HPE Service Manager Service Portal keystore (`/opt/hp/propel/security/.keystore`)

Preparation

Before performing these instructions and replacing the HPE Service Manager Service Portal-generated certificates, make sure an SSL configuration between the HPE Service Manager Service Portal host and a Service Manager supplier (endpoint) system works correctly. If you experience problems after replacing the SSL certificates, this will help you troubleshoot SSL issues.

Replace HPE Service Manager Service Portal-Generated SSL Certificates

The instructions in this chapter are written for IT organizations that require both a CA-signed root certificate and an intermediate certificate. If your IT organization requires only a root certificate, you can simplify the instructions

Perform the following steps to replace the previously HPE Service Manager Service Portal-generated SSL certificates with CA-signed SSL certificates.

> The following commands are run as `root` on the HPE Service Manager Service Portal host. (The default password is “propel2015” for the `root` user.)

1. Stop the HPE Service Manager Service Portal services:

   ```
   # propel stop
   ```

2. Backup the current HPE Service Manager Service Portal SSL directories:

   ```
   # cp -rp /opt/hp/propel-setup/ssl-tmp /opt/hp/propel-setup/ssl-tmp.backup
   # cp -rp /opt/hp/propel/security /opt/hp/propel/security.backup
   ```

3. Initialize the SSL working directory:

   ```
   # cd /opt/hp/propel-setup
   # ./propel-ssl-setup.sh init
   ```

   By default, the SSL working directory is `/opt/hp/propel-setup/ssl-tmp`.

   > **Note:** This re-creates the `/opt/hp/propel-setup/ssl-tmp` directory and removes all previous files.

4. Obtain your IT organization's CA certificates for use by HPE Service Manager Service Portal. Your IT organization can provide only a root certificate or both a root and an intermediate certificate. The instructions in this step are written for having both a root and an intermediate certificate. Considerations for the certificates are:

   - They must be in PEM format.
   - PEM certificates usually have extensions such as `.pem`, `.crt`, `.cer`, and `.key`.
   - They must be Base64 encoded ASCII files and contain:

     `"-----BEGIN CERTIFICATE-----"`

     and

     `"-----END CERTIFICATE-----"`

     lines.

   a. Copy the root certificate as `CA.crt` and the intermediate certificate as `intermediate.crt` to the `/opt/hp/propel-setup/ssl-tmp` directory.

   b. Merge both certificates in the `/opt/hp/propel-setup/ssl-tmp` directory:

      ```
      # cd /opt/hp/propel-setup/ssl-tmp
      # cat CA.crt intermediate.crt > rootPlusIntermediate.crt
      ```

5. Back up the existing HPE Service Manager Service Portal global Java keystore:

```
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security
# cp cacerts cacerts.backup
```

6. Import the root certificate (`CA.crt`) into the HPE Service Manager Service Portal global Java keystore

   ```
   # keytool -importcert -file /opt/hp/propel-setup/ssl-tmp/CA.crt
   -alias <CA_ALIAS> -trustcacerts -keystore cacerts
   ```

   Where <*CA_ALIAS*> is the CA alias you specify. The password is "changeit" for the global Java keystore.

7. Import the intermediate certificate (`intermediate.crt`) into the HPE Service Manager Service Portal global Java keystore

   ```
   # keytool -importcert -file /opt/hp/propel-setup/ssl-tmp/intermediate.crt
   -alias <INT_ALIAS> -trustcacerts -keystore cacerts
   ```

   Where <*INT_ALIAS*> is the intermediate alias you specify.

   > **Tip:** You can verify that the global Java keystore contains your CA certificates:
   >
   > ```
   > # keytool -list -keystore cacerts –storepass changeit | grep <ALIAS>
   > ```
   >
   > Where <*ALIAS*> is either the CA alias or the intermediate alias you specified in steps 6 and 7.

8. Generate the Certificate Signing Request (CSR) and Server Private Key pair:

   ```
   # cd /opt/hp/propel-setup
   # ./propel-ssl-setup.sh generateSigningRequest <SUBJECT>
   ```

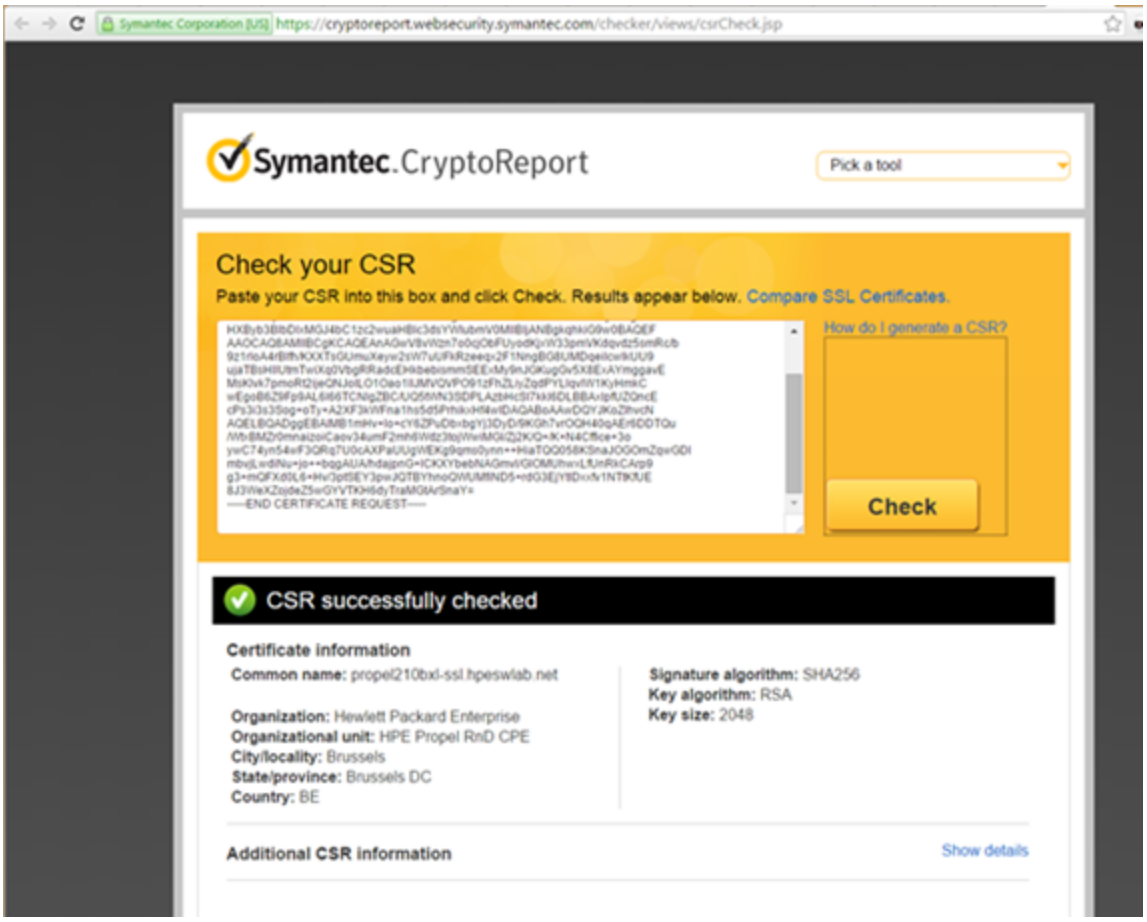
   Where *SUBJECT* is the signing request subject in the slash-separated form. "CN" must be the last field in the subject and contain the fully qualified hostname of the HPE Service Manager Service Portal host. Enclose the subject in double quotes, such as:
   "/C=US/ST=CA/L=San Jose/O=StartUpCompany/
   OU=Software/CN=mypropelserver.example.com"

   > **Note:** The private key password ("propel2014") is automatically created by the `propel-ssl-setup.sh` script.

   This command creates two new directories and four new files
   `/opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/` directory
   `/opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/out/` directory
   `/opt/hp/propel-setup/ssl-tmp/hostnames` file
   `/opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/private.key.pem` file

`/opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/propel_host.key.csr` file
`/opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.key.rsa` file

9. You can verify the content of your CSR by pasting its text in here:
https://ssltools.websecurity.symantec.com/checker/views/csrCheck.jsp



10. Send the CSR containing the public key to your CA. This is a process specific to your company, and network administrators should know how to accomplish this. Ask for the certificate to be delivered in PEM format. If it is not, you can convert formats with the `openssl` command.
11. After the certificate has been received from the CA, copy the new host certificate to:
`/opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt`

    If you need to extract the host certificate from a PEM file, you can extract the text beginning with "`-----BEGIN CERTIFICATE-----`" and ending with "`-----END CERTIFICATE-----`"

    The following is an example:

    ```
    [root@SGDLITVM034 out]# pwd
    /opt/hp/propel-setup/ssl-tmp/sgdlitvm034.domain.com/out
    ```

```
[root@SGDLITVM034 out]# cat propel_host.crt
-----BEGIN CERTIFICATE-----
MIIDgTCCAmkCCQDg9YGbj/CV+jANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlTYW4gRGllZ28xDTALBgNVBAoTBEhQ
U1cxDDAKBgNVBAsTA0JUTzEaMBgGA1UEAxMRc2VydmVyLmRvbWFpbi5jb20xHjAc
BgkqhkiG9w0BCQEWD3VzZXJAZG9tYWluLmNvbTAeFw0xNjA5MjIwNTM3MzNaFw0x
OTA5MjIwNTM3MzNaMH0xCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1UE
BwwIU2FuIEpvc2UxFzAVBgNVBAoMDlN0YXJ0VXBDb21wYW55MREwDwYDVQQLDAhT
b2Z0d2FyZTEiMCAGA1UEAwwZU0dETElUVk0wMzQ5LmhwZXN3bGFiLm5ldDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMLljL+tzjZHGzK1gHaZDNBvMXUt
kJPq+J73yqnaigIY/O1q0i1zWttqZJt8pju2BSlvQ517x4POr9pGAyDM7A0KqdsP
tGMGQ07U8gaX2fyZl+t9yBeg3fgrQ1cgqmIlrxuFx+o8GeBjSZJn6MO+BeWjLRWr
5PB1J0izBG3garSLL0jn+knV3i3M/BEB17bhmn5tETghC04cvZO5BaLkiRklbST4
Yt+rBjDBlhGS9eHVDuiQ1zzrAvtbGZLW4Mzss/nWvmkN55kfakdsYqYCe9m8mLKv
LZTZeFfoo7xoS+hGbSdZnXFRKIXOr+vA981KDrlLtgOZ+oOyvgpcFlm1LvUCAwEA
ATANBgkqhkiG9w0BAQUFAAOCAQEAb2TglwIa95V9k58b4z5mkpscb0Hkg7zGiIc3
E16AmNbNlZ/qVebnAM3gheAbD9V3ebQ61WQgJYYv7JzDiGcU5RhevSd7XJuuqm+p
0EuwDwLtalFKcETxtUv+/F5p1TmsdkBXBwVlFSElYQ/oaKxH2dPX7U15TF2gdMeM
2S7adpfLqX/yFod5pqjp0nU20iSsCzml7AR+enp3J257OngqhmnfMYLc4P+4iI0d
hC3nTqdi2nudSp0s0UJSghK4BTFURd3UxEropfCB5GC5oebIEnrrKfp5imZ9quM3
voGo4FaGVWLOMr+fc+QmfP82R4cP4Bl0ZmwNCeGdFIbj9objVg==
-----END CERTIFICATE-----
[root@SGDLITVM034 out]#
```

12. View the SSL certificate signing algorithm.

    > **Note:** HPE recommends reviewing the certificate-signing algorithm used and ensuring that strong encryption is used. For example, SHA1 is sometimes used, and instead, stronger algorithms such as SHA256 should be used.

    To view a certificate's signing algorithm, execute the following command:

    ```
    # keytool –printcert –file <SSL-CERTIFICATE> | grep –i algorithm
    ```

    For example:

    ```
    # keytool –printcert –file /opt/hp/propel/security/propel_host.crt | grep
    algorithm
    Signature algorithm name: SHA256withRSA
    #
    ```

13. Validate the host certificate and the CA match:

    ```
    # openssl verify -verbose -CAfile
    /opt/hp/propel-setup/ssl-tmp/rootPlusIntermediate.crt
    /opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt
    ```

    You should see the following message:

    ```
    /opt/hp/propel-setup/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt: OK
    ```

> **Caution:** Do not proceed if you see any error messages. The CA and certificate must match. Restore the HPE Service Manager Service Portal host's files that were backed up in previous steps (2 and 5) and restart this procedure if necessary.

14. Create the certificate and the keystores:

```
# cd /opt/hp/propel-setup/
# ./propel-ssl-setup.sh finish
```

The results of the `propel-ssl-setup.sh finish` script resemble the following example:

```
[root@SGDLITVM034 hp]# ls -la /opt/hp/propel-setup/overlay/*/security
/opt/hp/propel-setup/overlay/_ALL_HOSTS_/security:
total 8
drwxr-x---. 2 root root   43 Sep 21 10:57 .
drwxr-x---. 3 root root   21 Sep 21 10:57 ..
-rw-r-----. 1 root root 1627 Sep 22 13:54 CA.crt
-rw-r-----. 1 root root 2169 Sep 22 13:54 propel.truststore

/opt/hp/propel-setup/overlay/sgdlitvm034.domain.com/security:
total 24
drwxr-x---. 2 root root 4096 Sep 21 10:57 .
drwxr-x---. 3 root root   21 Sep 21 10:57 ..
-rw-r--r--. 1 root root 2285 Sep 22 13:54 .keystore
-rw-r-----. 1 root root 2904 Sep 22 13:54 propel_host.chain.crt
-rw-r--r--. 1 root root 1277 Sep 22 13:39 propel_host.crt
-rw-r--r--. 1 root root 1679 Sep 22 11:41 propel_host.key.rsa
-rw-r--r--. 1 root root 2689 Sep 22 13:54 propel_host.pfx
```

15. Move all the created files, `intermediate.crt`, and `rootPlusIntermediate.crt` into their final locations:

> The `yes` commands preceding the `cp` commands automatically sends a "y" when prompted to overwrite an existing file.

```
# cd /opt/hp/propel-setup/overlay/_ALL_HOSTS_/security
# yes | cp -p * /opt/hp/propel/security

# cd /opt/hp/propel-setup/overlay/$PROPEL_VM_HOSTNAME/security
# yes | cp -p * /opt/hp/propel/security
# yes | cp -p .keystore /opt/hp/propel/security

# cp /opt/hp/propel-setup/ssl-tmp/rootPlusIntermediate.crt
/opt/hp/propel/security/rootPlusIntermediate.crt
```

```
# cp /opt/hp/propel-setup/ssl-tmp/intermediate.crt
/opt/hp/propel/security/intermediate.crt
```

The following is an example:

```
[root@SGDLITVM034 security]# ls -la
total 36
dr-xr-x---.  2 propel propel 4096 Sep 21 11:12 .
drwxr-xr-x. 36 propel root   4096 Sep 21 11:14 ..
-r--r-----.  1 propel propel 1627 Sep 22 14:00 CA.crt
-r--r-----.  1 propel propel 2285 Sep 22 13:54 .keystore
-r--r-----.  1 propel propel 2904 Sep 22 13:54 propel_host.chain.crt
-r--r-----.  1 propel propel 1277 Sep 22 13:39 propel_host.crt
-r--r-----.  1 propel propel 1679 Sep 22 11:41 propel_host.key.rsa
-r--r-----.  1 propel propel 2689 Sep 22 13:54 propel_host.pfx
-r--r-----.  1 propel propel 2169 Sep 22 13:54 propel.truststore
```

16. Make sure the `CA.crt` and `intermediate.crt` files are in the `/opt/hp/propel/security` directory on the HPE Service Manager Service Portal host. (They should have already been copied in step 14 above.)
17. Import the intermediate certificate (`intermediate.crt` file) into the HPE Service Manager Service Portal truststore:

    ```
    # cd /opt/hp/propel/security
    # keytool -importcert -file intermediate.crt -keystore propel.truststore -
    trustcacerts
    ```

    > **Tip:** The password is "propel2014" for the HPE Service Manager Service Portal truststore.

18. Update the `app.json` files on the HPE Service Manager Service Portal VM with the following commands:

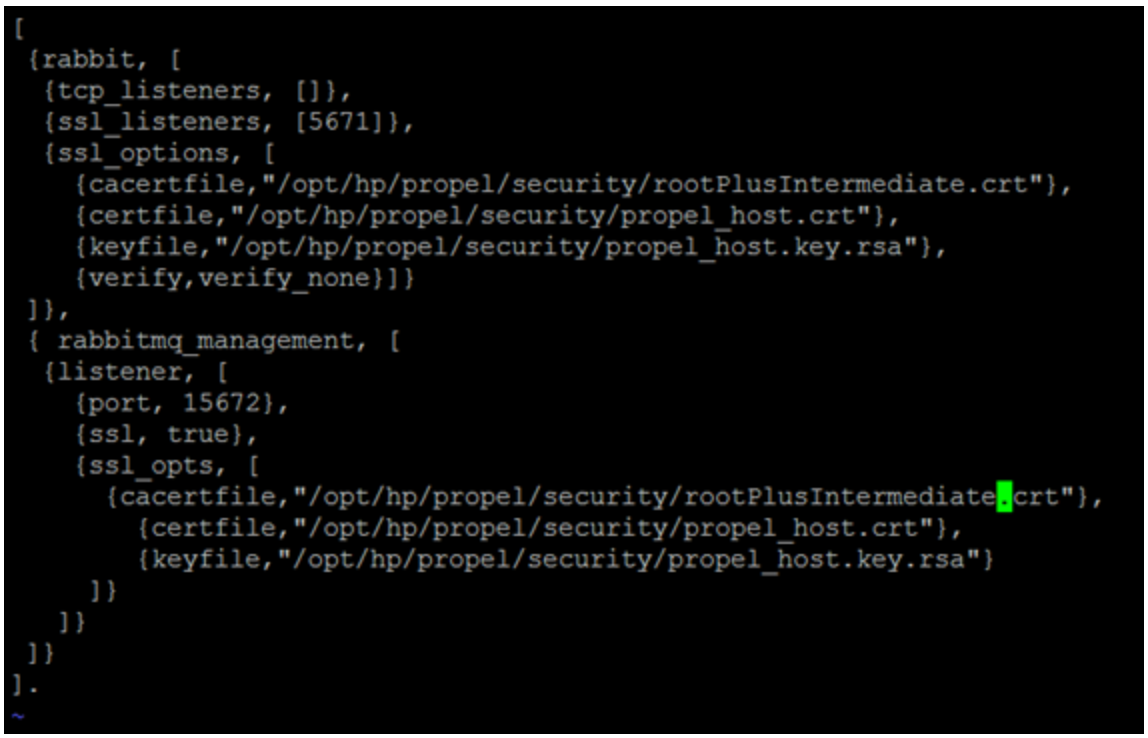
    ```
    # cd /opt/hp/propel
    # sed -i -
    e's!/opt/hp/propel/security/CA.crt!/opt/hp/propel/security/CA.crt,/opt/hp/prope
    l/security/intermediate.crt!' $(find . -print | grep app.json)
    ```

19. Update the Identity Management (IdM) `*.json` files on the HPE Service Manager Service Portal VM with the following commands:

    ```
    # cd /opt/hp/propel/idmAdmin/conf
    # sed -i -
    e's!/opt/hp/propel/security/CA.crt!/opt/hp/propel/security/CA.crt,/opt/hp/prope
    l/security/intermediate.crt!' $(find . -print | grep endpoint.json)
    # sed -i -
    e's!/opt/hp/propel/security/CA.crt!/opt/hp/propel/security/CA.crt,/opt/hp/prope
    l/security/intermediate.crt!' $(find . -print | grep idm.json)
    ```

Update RabbitMQ

1. Edit the `/etc/rabbitmq/rabbitmq.config` file so that the `cacertfile` property has either the single root certificate (`CA.crt` file) or both the root and intermediate certificates (`rootPlusIntermediate.crt` file) specified. The following is an example of using both certificates:



2. Restart RabbitMQ and clean up its log files

```
systemctl stop rabbitmq-server
rm -rf /var/log/rabbitmq/*
systemctl start rabbitmq-server
```

3. Make sure there are no errors in the `/var/log/rabbitmq/rabbit@<PROPEL_HOST_SHORTNAME>.log` file.

Update HPE Operations Orchestration

Perform the following steps to update HPE Operations Orchestration (HPE OO) on the HPE Service Manager Service Portal host.

1. Stop the HPE OO service on the HPE Service Manager Service Portal host:

```
# systemctl stop central
```

2. Back up the existing HPE OO configuration:

```
# cd /opt/hp/oo/central/var
# cp -rp security security.backup
```

3. Manually delete the old certificates from the HPE OO stores and install the new certificates:

```
# keytool -delete -keystore /opt/hp/oo/central/var/security/client.truststore-
alias propel_host -storepass changeit -noprompt
# keytool -importcert -keystore
/opt/hp/oo/central/var/security/client.truststore -file
/opt/hp/propel/security/propel_host.crt -alias propel_host -storepass changeit
-noprompt
# keytool -delete -keystore/opt/hp/oo/central/var/security/client.truststore -
alias propeljboss_$PROPEL_VM_HOSTNAME -storepass changeit -noprompt
# keytool -importkeystore -noprompt -srcstoretype PKCS12 -srckeystore
/opt/hp/propel/security/propel_host.pfx -srcstorepass propel2014 -destkeystore
/opt/hp/oo/central/var/security/client.truststore -deststorepass changeit
# keytool -delete -keystore /opt/hp/oo/central/var/security/key.store -alias
tomcat -storepass changeit -noprompt
# keytool -importkeystore -noprompt -srcstoretype PKCS12 -srckeystore
/opt/hp/propel/security/propel_host.pfx -srcstorepass propel2014 -destkeystore
/opt/hp/oo/central/var/security/key.store -deststorepass changeit -srcalias
propeljboss_$PROPEL_VM_HOSTNAME -destalias tomcat
# keytool -keypasswd -new changeit -keystore
/opt/hp/oo/central/var/security/key.store -storepass changeit -alias tomcat -
keypass propel2014
```

4. Restart HPE OO:

```
# systemctl start central
```

> **Tip:** Next, if you need to configure SSL between Service Manager and Service Manager Service Portal, go to "(Optional) Configure SSL for a Service Manager supplier" below; otherwise go to "Add Service Manager as a supplier" on page 110.

(Optional) Configure SSL for a Service Manager supplier

If HTTPS is used for communications between Service Manager Service Portal and a Service Manager supplier, HTTPS must be configured.

> **Note:** Third-party or corporate CA-signed certificates should be used in production systems; however, self-signed certificates generated by Service Manager Service Portal can be used in non-production systems.

To configure SSL, perform the following steps:

1. Import the Service Manager Service Portal host's CA-signed certificate into the Service Manager Server's keystore. The general steps to do this are:
   a. Copy the Service Manager Service Portal host's `/opt/hp/propel/security/CA.crt` file to the supplier's `/tmp` directory.
   b. On the supplier's system, import the CA-signed certificate:

      ```
      # keytool –importcert –file /tmp/CA.crt –alias Propel_CA –trustcacerts
      –keystore <SUPPLIER-KEYSTORE-PATH>/cacerts
      ```

      Where *SUPPLIER-KEYSTORE-PATH* is the location of the `cacerts` file on the supplier's system.

      The default `cacerts` file locations of Service Manager are:

      - HPE SM on Windows:
        `C:\Program Files (x86)\HPE\Service Manager9.xx\Server\RUN\cacerts`
      - HPE SM on Linux:
        `/opt/HPE/ServiceManager9.xx/Server/RUN`

   c. On the Service Manager system, restart the Service Manager Server service.
2. Import the supplier's CA certificate into the Service Manager Service Portal host's truststore. The general steps to do this are:
   a. Obtain the supplier's CA certificate, and then copy it to the Service Manager Service Portal host's `/tmp` directory. For examples of obtaining a supplier's certificate, see "SSL tips" on the next page. In the following step, the supplier's CA certificate is in a `CA.crt` file.
   b. On the Service Manager Service Portal host, import the supplier's CA-signed certificate:

      ```
      # keytool –importcert –file /tmp/CA.crt –alias Supplier_CA –trustcacerts
      –keystore /opt/hp/propel/security/propel.truststore
      ```

      > **Tip:** The default password is "propel2014" for the Service Manager Service Portal truststore.
3. On the Service Manager Service Portal host, restart the HPE Service Exchange (HPE SX) services:

   ```
   # systemctl restart jetty-sx
   ```
4. Launch the **Suppliers** application in Service Manager Service Portal , view the supplier details and then click the **Diagnostics** tab. The status should indicate there are no connection issues.

SSL tips

If you do not have an SSL certificate from the supplier's system, you can manually create a certificate. The following are examples of creating a supplier's SSL certificate:

Export the SSL certificate from the supplier's truststore

Use the following command on the supplier's system to export an SSL certificate from the supplier's truststore:

```
# keytool -exportcert -file <CERT-OUTPUT-FILE> -keystore
<SUPPLIER-KEYSTORE-PATH>/cacerts -alias <SUPPLIER-ALIAS>
```

Where: :

- *CERT-OUTPUT-FILE* is the output file that will contain the exported certificate.
- *SUPPLIER-KEYSTORE-PATH* is the location of the `cacerts` file on the supplier's system.
- *SUPPLIER-ALIAS* is the alias used in the supplier's truststore to identify the supplier's certificate.

Create supplier's host certificate

Use the following procedure to create a supplier's host certificate:

1. On the Service Manager Service Portal VM, execute the following command:

   ```
   # openssl s_client -connect <SUPPLIER-HOST>:<PORT> > supplier.crt
   ```

2. Edit the `supplier.crt` file and retain only the lines beginning with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----", deleting all other lines.

You can verify that the supplier's host certificate is valid with the following command:

```
# keytool -printcert -file supplier.crt
```

The output of the `keytool` command should identify the certificate owner and issuer.

> **Tip:** Once the SSL configuration is complete, you are ready to add your Service Manager system as a supplier of Service Manager Service Portal. For details, see "Add Service Manager as a supplier" on the next page.

Add Service Manager as a supplier

To enable Service Manager Service Portal to connect to Service Manager, you must add Service Manager as a supplier.

> **Important:** Service Manager Service Portal supports only the **SM** backend system type and only one Service Manager supplier.

Suppliers are associated with organizations, and the Organization Administrator manages the supplier systems for his organization.

> **Note:** If HTTPS is used for communication between Service Manager Service Portal and Service Manager, HTTPS must be configured. See "(Optional) Configure SSL for a Service Manager supplier" on page 107 for instructions.

The Organization Administrator can create new suppliers in Service Manager Service Portal. To add Service Manager as a new supplier, follow these steps:

1. Log in to Service Manager Service Portal as the `orgadmin` user by opening a browser and specifying the following URL:

   `https://<ServicePortal_HOSTNAME>:9000/org/CONSUMER`

   Where *ServicePortal_HOSTNAME* is the fully qualified domain name of Service Manager Service Portal.
2. From the Launchpad in Service Manager Service Portal, click the **Suppliers** application.
3. In the **Suppliers** view, click **Add Supplier**.
4. In the **Add Supplier** dialog, do the following:
   a. Type the **Name** of the new supplier. For example, type **SM9.50**.
   b. Select **SM** in the **Backend System Type** field.
5. After the **Backend System Type** is selected, additional **General** fields are displayed, such as integration account credentials and end-point URLs. Fill in and select the required **General** fields as described in the following table.

Field(s)	Description
Endpoint	Base url for SM web services in the form

Field(s)	Description
	http://<host>:<port>/SM For example: http://mysmhost.mycompany.net:13082/SM
With Process Designer	Select this option.
Use LWSSO	Select this option. **Note:** When this option is selected, you need to eanble LW-SSO in both the Service Manager Server and Service Exchange.
Locale	Expected in the language tag format like pt or pt-BR. Used for SM catalog locale and for locale of case exchange-related messages in SM. If left blank, English is used.
URL escaping charset	If the supplier needs REST URL encoded by a charset different from the default value of UTF-8, enter the charset code here (for example "windows-1252"). For a Service Manager supplier, leave this field blank.
Login name Password	Enter the login name and password of the Service Manager user account to be used for Service Manager Service Portal to access Service Manager through web services calls. **Note:** This user account must have system administration privileges in Service Manager, and the password cannot be blank. As best practice, create a dedicated user account for this purpose.
Protocol Host name Port	These are the protocol (http or https), host name, and port of your proxy server, respectively. If you are not using a proxy server, leave these fields blank.

6. Click **Create** in the **Add Supplier** dialog to finish and save your changes. The new supplier and its properties are displayed.
7. Configure LW-SSO in the Service Manager Server and Service Manager Service Portal.

   Configure LW-SSO in the Service Manager server

   a. Go to the <Service Manager server installation path>/RUN folder, and open `lwssofmconf.xml` in a text editor.

   b. Make sure that the `enableLWSSOFramework` attribute is set to `true` (default).

   c. Change the domain value `example.com` to the domain name of your Service Manager server host.

   d. Set the `initString` value. This value MUST be the same with the LW-SSO value that you specified during the installation of Service Manager Service Portal. For details, see the "Configure LW-SSO" step in "Install Service Manager Service Portal" on page 82.

   e. Restart the Service Manager Server.

   Set up Service Manager Service Portal to use LW-SSO

   You should have already done so during the installation of Service Manager Service Portal. For details, see the "Configure LW-SSO" step in "Install Service Manager Service Portal" on page 82.

   No additional steps are required. If you want to verify the LW-SSO settings, you can check the following files:

   - `/opt/hp/propel/sx/WEB-INF/classes/config/lwssofmconf.xml`
   - `/opt/hp/propel/idm-service/WEB-INF/classes/config/lwssofmconf.xml`
8. Validate connectivity between Service Manager Service Portal and Service Manager. To do this, run the Service Manager Service Portal **Diagnostics** application to verify Service Manager is configured and connected correctly. To do this, follow these steps:

   a. Log in to Service Manager Service Portal as the admin user (https://<Service Portal host name>:9000/org/Provider).

   b. Click the **Diagnostics** application. Refer to the Diagnostics help for details.

   c. In Diagnostics, click **Configuration Check** in the Supplier Detail view for an HPE Service Manager instance.

> **Tip:** Next, you need to configure shopping, ticketing, Knowledge Management (KM), and hot news so that users can order catalog items, submit support requests, perform KM searches, and so on. For details, see "Configure shopping, ticketing, Knowledge Management, and hot news" on the next page.

Configure shopping, ticketing, Knowledge Management, and hot news

After you have successfully installed Service Manager Service Portal and added a Service Manager supplier, the next steps are to configure shopping, ticketing, knowledge management, and Hot News, depending on the needs of the consumers using the Service Manager Service Portal Portal.

> **Tip:** For information on how to configure RSS feeds in the Service Manager Service Portal Hot News application, refer to the Service Manager Service Portal Administration Guide in the Service Manager Help Center for instructions.refer to the Service Manager Service Poratal Administration Guide.

Configure shopping and ticketing

The Organization Administrator can manage Service Manager Service Portal catalog items by creating aggregations. An aggregation contains catalog items that are imported from Service Manager. After an aggregation is created and the catalog items are imported, the Organization Administrator publishes the Service Manager Service Portal catalog items into a catalog, and then they are available for fulfillment in Service Manager Service Portal.

Catalog items in Service Manager Service Portal are divided into two types:

- Service Offering: A Service Offering is a catalog item that is used for shopping.
- Support Offering: A Support Offering is a catalog item that is used to request support.

To configure shopping for Service Manager Service Portal, the following needs to be completed:

1. *Create an aggregation*. Offerings from end-point systems are initially imported into an Service Manager Service Portal aggregation. For instructions to create an aggregation, refer to the *Add Catalog Aggregation* topic in the *Service Manager Service Portal Catalog Connect Help*.

   > **Note:** For shopping, be sure to select **Service Offering** in the **Offering Type** field.

2. *Create a new catalog*. Offerings from end-point systems are contained in Service Manager Service Portal catalogs as catalog items. For instructions to create a catalog and configure which users can access the catalog, refer to the *Service Manager Service Portal Catalogs Help*.

3. *Publish catalog items*. Catalog items must be published in an Service Manager Service Portal catalog for consumer fulfillment. For instructions to publish catalog items in catalogs, refer to the *Service Manager Service Portal Catalog Items Help*.

To configure ticketing for Service Manager Service Portal, repeat the same steps for configuring shopping except that you must select **Support Offering** in the **Offering Type** field.

Enable Knowledge Management search

This section provides instructions for enabling Knowledge Management (KM) search in Service Manager Service Portal. Two different scenarios are covered based on which search engine is enabled in SM.

Scenario 1: Service Manager uses the SOLR search engine

This section provides instructions for setting up KM Solr Search Engine and installing the Solr plugin for IDOL search.

Task 1: Setting Up KM Solr Search Engine

Make sure that you complete the following tasks in SM to enable KM Solr search engine for KM:

1. Install KM Solr search engine. For detailed instructions, see *"Install and configure the Solr Search Engine" on page 309*.
2. Complete KM indexing.

   The `KMUpdate` process controls indexing. Use HPE SM's **Update Indexes** form to stop and restart indexing, and to view the status statistics related to indexing. To access this form, from the Service Manager navigator menu, select **Knowledge Management** > **Configuration** > **Update Indexes**.

   For help with indexing, see the topic "*indexing the knowledgebases*" in Service Manager Help Center.

   > **Tip** To quickly verify that `KMUpdate` is running, type `status` in the Command window to display all processes currently running.

Task 2: Configuring Steps – After HPE Service Manager Service Portal Installation

Perform the following steps to configure HPE KM after the HPE Service Manager Service Portal installation.

1. On the HPE Service Manager Service Portal VM, stop the HPE SX UI service:

   ```
   # systemctl stop sx-client-ui
   ```

2. Add the following lines to the HPE SM's `sm.cfg` file. This configuration avoids using web services over the HPE SM LoadBalancer port, which is often port 13080:

   ```
   # Propel: port used by Catalog Aggregation and Catalog microservices
   sm -httpPort:21090 -httpsPort:21493 –debugnode
   –log:../logs/sm-propel-2.20.log –sslConnector:1 ssl:0
   ```

   This configuration allows connecting either with SSL (port 21493) or without SSL (port 21090).

3. HPE Service Manager Service Portal integration with HPE SM's KM module will use both the HPE KM Search Engine and an HPE SM integration servlet to gather the documents and related attachments. Determine which port the master HPE KM Search Engine uses as follows: from the HPE SM navigator menu, select **Knowledge Management** > **Configuration** > **Configure Search Servers**, then click **Search**. By default, this will be port 8080.

4. On the HPE Service Manager Service Portal VM, modify the `/opt/hp/propel/sxClientUI/app.json` file. The following partial example shows modifications to the `knowledge` section:

   ```
   }, "knowledge": {
    "mount": "/api/km",
    "kmUrl": "http://SM_Solr_Server:8380",
    "kmContextPath": "/KMCores",
    "kmStrictSSL": true,
    "kmSecureProtocol": "TLSv1_method",
    "kmCa": "/opt/hp/propel/security/CA.crt",
    "kmAttachUrl": "https://SM_SERVER:21493",
    "kmAttachContextPath": "/SM/9/rest",
    "kmAttachStrictSSL": false,
    "kmAttachSecureProtocol": "TLSv1_method",
    "kmAttachCa": "/opt/hp/propel/security/CA.crt",
    "kmAttachUsername": "falcon",
    "kmAttachPassword": "",
   },
   ```

   Where *SM_SERVER* is the fully qualified hostname of the HPE SM server. Other considerations for configuring the `knowledge` section are:

   - The `KMUrl` property contains the host and port of the HPE SM SOLR server. The default HPE SM SOLR port is 8380, but the port number can vary.

- The `kmAttachUrl` property can also use port 21090, but then `https` should be changed to `http`.
- The default value for the `kmAttachStrictSSL` property is `true`, but this needs to be set to `false` in case self-signed SSL certificates are used.
- The `kmAttachUsername` property contains the HPE SM integration account. This can be a clone of the `falcon`HPE SM user.

5. Load the HPE Service Manager Service Portal VM's CA-signed certificate into the HPE SM system's keystore. The general steps to do this are:
   a. Copy the HPE Service Manager Service Portal VM's `/opt/hp/propel/security/CA.crt` file to the HPE SM system's `/tmp` directory.
   b. On the HPE SM system, import the HPE Service Manager Service Portal CA-signed certificate:

      ```
      # keytool –import –file /tmp/CA.crt –alias Propel_CA –trustcacerts –keystore <SM-KEYSTORE-PATH>/cacerts
      ```

      Where *SM-KEYSTORE-PATH* is the location of the `cacerts` file on the HPE SM system.
   c. On the HPE SM system, restart HPE SM:

      ```
      # service sm restart
      ```

6. Load the HPE SM system's CA-signed certificate into the HPE Service Manager Service Portal VM's keystore. The general steps to do this are:
   a. Copy the HPE SM system's `CA.crt` file to the HPE Service Manager Service Portal VM's `/tmp` directory.
   b. On the HPE Service Manager Service Portal VM, import the HPE SM CA-signed certificate:

      ```
      # keytool –import –file /tmp/CA.crt –alias SM_CA –trustcacerts –keystore /usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts
      ```

   c. On the HPE Service Manager Service Portal VM, start the HPE SX UI service:

      ```
      # systemctl restart sx-client-ui
      ```

Task 3: Solr Plugin Installation and Configuration

To configure HPE SM and HPE KM to work with HPE Service Manager Service Portal Search, you must install the Solr plugin and configure it to send changes to HPE Service Manager Service Portal Search.

HPE SM indexes HPE KM articles to Solr. HPE Service Manager Service Portal has a plugin to Solr, so all articles written to Solr are sent to HPE Service Manager Service Portal, which indexes it to IDOL.

Solr Plugin Installation Steps

1. On the HPE Service Manager Service Portal VM, copy the `/opt/hp/propel/search/propel-solr-plugin.zip` file to the HPE SM/HPE KM machine.
2. Unzip the `propel-solr-plugin.zip` file. The contents are:
   `jackson-mapper-asl-1.9.13.jar`
   `jackson-core-asl-1.9.13.jar`
   `jasypt-1.9.2.jar`
   `KMExtAccess.unl`
   `propel-solr-plugin-1.1.0.jar`
3. Copy the `.jar` files to your primary search server. That is, copy `propel-solr-plugin-1.1.0.jar`, `jackson-mapper-asl-1.9.13.jar`, `jackson-core-asl-1.9.13.jar`, and `jasypt-1.9.2.jar` to <*Primary_Search_Server*>`\Search_Engine\tomcat\webapps\KMCores\WEB-INF\lib\`.
4. Edit the <*Primary_Search_Server_Home*>`\Service Manager 9.xx\Search_Engine\kmsearchengine\KMCores\kmcore\conf\solrconfig.xml` file to add an `updateRequestProcessorChain`:

   Add `updateRequestProcessorChain` to `solrconfig.xml` File Example

   ```
   <updateRequestProcessorChain name="propelSearch" default="true">
     <processor class="com.hp.propel.solr.plugin.PropelPushUpdateFactory">
       <str name="baseUrl">https://{Hostname:Port}/api/search/v1/article</str>
       <str name="username">searchTransportUser</str>
       <str name="password">{Password}</str>
       <str name="tenant">Provider</str>
     </processor>
     <processor class="solr.RunUpdateProcessorFactory"/>
   </updateRequestProcessorChain>
   ```

   Where:

   - *Hostname* is the hostname of the HPE Service Manager Service Portal server.
   - *Port* is the port defined for the `search.endpoint` parameter in the `/opt/hp/propel-install/setup.properties` file on the HPE Service Manager Service Portal server. The port number is visible in the HPE Service Manager Service Portal Search services `/opt/hp/propel/search/search.yml` configuration file, and is 9040 by default.

```
[root@ propel]# cd /opt/hp/propel/search/
[root@ search]# ls
lib  propel-solr-plugin.zip  search.yml  server.log
[root@ search]# cat search.yml
server:
#  softNofileLimit: 1000
#  hardNofileLimit: 1000
  rootPath: /api/search/v1/*
  registerDefaultExceptionMappers: false
  applicationConnectors:
    - type: https
      port: 9040
      keyStorePath: /opt/hp/propel/security/.keystore
```

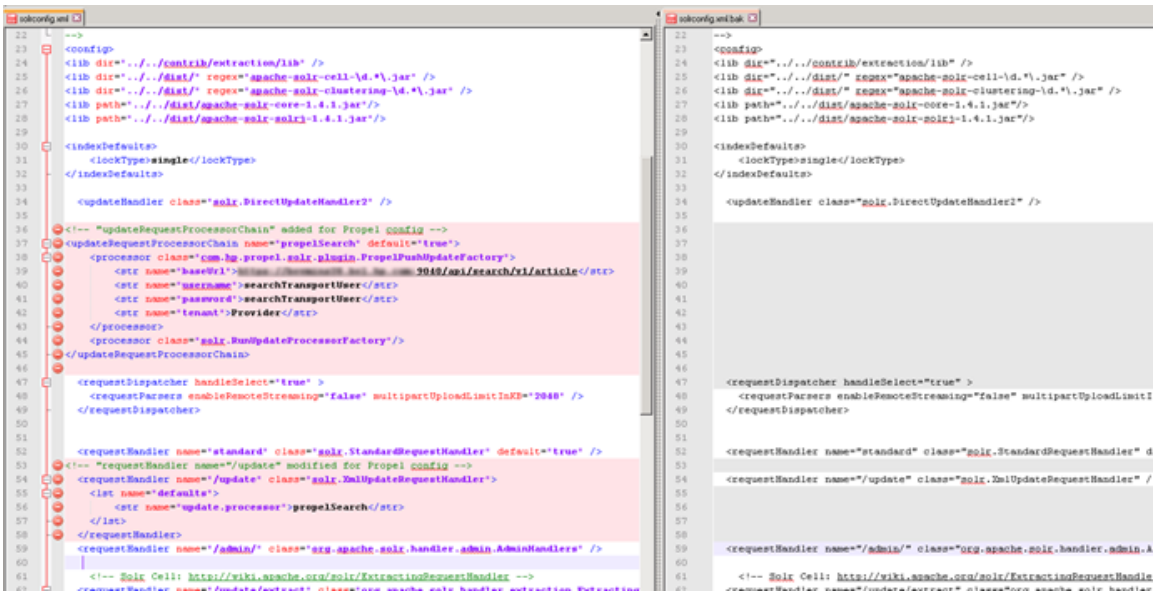
- *Password* is the password for `searchTransportUser`. (The default password is `searchTransportUser`.

5. Update the same `solrconfig.xml` and modify the `requestHandler`.

   Modify `requestHandler` in `solrconfig.xml` File Example

```
<requestHandler name="/update" class="solr.XmlUpdateRequestHandler">
  <lst name="defaults">
    <str name="update.processor">propelSearch</str>
  </lst>
</requestHandler>
```

   Example content for steps 4 and 5 (compared with an out-of-the-box `solrconfig.xml` file):



6. In the HPE SM client, apply the `KMExtAccess.unl` unload file.

7. Restart HPE KM.
8. Restart HPE SM.
9. In the HPE SM client, reindex HPE KM.
   a. Select **Knowledge Management** -> **Administration** -> **Environment**.
   b. Check **SRC**.
   c. Select the **Search Server Name**.
   d. Click **Full Reindex**.
10. In the HPE SM client, reindex the HPE KM Libraries:
    a. Select **Knowledge Management** -> **Knowledgebases**.
    b. Click on each of the libraries, and then click **Full Reindex**.

Scenario 2: Service Manager uses Smart Analytics as the search engine

This section provides instructions for enabling KM search in Service Manager Service Portall when Smart Analytics is enabled in SM.

Task 1: Setting up Smart Analytics in SM

Make sure that you complete the following tasks in SM to enable Smart Search for KM:

1. Install Smart Analytics for Service Portal successfully. For instructions, see "Set up Smart Analytics for Service Manager Service Portal" on page 278.
2. Enable Smart Analytics.
3. Configure Smart Search and complete a full indexing.

> **Tip:** For more information, see "Install and configure Smart Analytics" on page 242.

Once you finish the full indexing in SM and SM can search from knowledge library by using Smart Search, go to the next task to set the “smaEnabled” flag in Service Manager Service Portal.

Task 2: Configuring Service Manager Service Portal

To configure Service Manager Service Portal to use Smart Analytics as the search engine, follow these steps:

1. Go to the VM that installs the search and sxClientUI services.
2. Stop the search and sxClientUI services.
3. Open and edit the /opt/hp/propel/search/search.yml file:
   a. Set the "smaEnabled" parameter to "true" as shown in the following example:

      ```
      idol:

      ...

      smaEnabled: true

      ...
      ```

   b. For each IDOL component, change the hostname value to the address of the single IDOL server (Smart Analytics) and update the port accordingly:

      ```
      query:
          hostname: localhost
          port: 14000

      index:
          hostname: localhost
          port: 14001

      attach:
          hostname: localhost
          port: 7000

      qms:
          hostname: localhost
          port: 16000


      agentStore:
          hostname: localhost
          port: 14051
      ```

      Refer to the following table to locate the port number for each component in Smart Analytics.

Component	Where to locate the port number

query	Location: <*Smart Analytics installation*>/IDOL/IDOLServer.cfg
	
	`[Server]`
	`//SecurityDebugLogging=true`
	`Port=9000`

Component	Where to locate the port number
	`IndexPort=9001`

index	Location: <*Smart Analytics installation*>/IDOL/IDOLServer.cfg
	`[Server]`
	`//SecurityDebugLogging=true`
	`Port=9000`
	`IndexPort=9001`

attach	Location: <*Smart Analytics installation*>/CFS/CFS.cfg
	`[Server]`
	`Port=7000`
	`QueryClients=*,,127.0.0.1,::1`
	`AdminClients=*,,127.0.0.1,::1`

qms	Location: <*Smart Analytics installation*>/QMS/QMS.cfg
	`[Server]`
	`Port=16000`
	`AdminClients=*,127.0.0.1,::1`
	`QueryClients=*,127.0.0.1,::1`

agentStore	Location: <*Smart Analytics installation*>/IDOL/agentstore/portinfo.dat
	`[Ports]`
	`ACIPort=9050`
	`IndexPort=9051`
	`QueryPort=9052`
	`ServicePort=9053`

4. Start the “search” services.
5. Open the /opt/hp/propel/sxClientUI/apps.json file, and then add the smaEnabled flag and configure kmAttachUrl as highlighted in the following example.

   ```
   "knowledge": {
   "mount": "/api/km",
   "smaEnabled": true,
   "kmAttachUrl": "https://SM_SERVER: 13080",
   ```

6. Start the “sx-client-ui" service.
7. Set the SM user with the RESTful API capability in /opt/hp/propel/sxClientUI/app.json.

   The user in /opt/hp/propel/sxClientUI/app.json such as falcon in the following configuration example should have the RESTful API capability added in SM. By doing so, the users can drill down to the km article detail page and to the km attachment.

```
"knowledge": {
"mount": "/api/km",
"smaEnabled": true,
"kmUrl":"",
"kmContextPath": "/KMCores",
"kmStrictSSL": true,
"kmSecureProtocol": "TLSv1_method",
"kmCa": "/opt/hp/propel/security/CA.crt",
"kmAttachUrl": "https://SM_SERVER: 13080",
"kmAttachContextPath": "/SM/9/rest",
"kmAttachStrictSSL": true,
"kmAttachSecureProtocol": "TLSv1_method",
"kmAttachCa": "/opt/hp/propel/security/CA.crt",
"kmAttachUsername": "falcon",
"kmAttachPassword": ""
},
```

> **Note:** In Service Manager Service Portal, users can only search for externally published KM documents. In addiction, as currently Service Manager Service Portal does not support permission control for document search, every user can search out all the externally published KM documents.

Configure the **Hot News** application

The **Hot News** application in HPE Service Manager Service Portal enables you to specify RSS feeds and view them in HPE Service Manager Service Portal.

To configure **Hot News**:

1. Log in to the HPE Service Manager Service Portal host as `root` and navigate to the `/opt/hp/propel/launchpad/conf` directory.
2. Edit the `rss.json` file and add your RSS feeds, similar to the following:

   ```
   [
     "http://investors.hpe.com/rss/news",
     "http://rss.cnn.com/rss/cnn_topstories.rss",
     "http://sports.espn.go.com/espn/rss/news"
   ]
   ```

   > **Note:** The feed must support RSS 2.0 format.

To configure organization-specific RSS feeds, create an `rss.`*`ORG_NAME`*`.json` file, where *`ORG_NAME`* is the name of the HPE Service Manager Service Portal organization.

Running the RSS Interface in Launchpad Behind a Firewall

If HPE Service Manager Service Portal is installed and running behind a firewall, then you need to configure a proxy so that the RSS interface in Launchpad can fetch the RSS feeds appropriately. Perform these instructions to configure the proxy for Launchpad:

1. Log in to the HPE Service Manager Service Portal host as `root`.
2. Create an `/etc/systemd/system/launchpad.service.d` directory.
3. Within the directory, create a `local.conf` file.
4. Edit the `local.conf` file and add the following entries, where *`PROXY_HOST`* and *`PROXY_PORT`* contain your proxy information:

   ```
   [Service]
   Environment=http_proxy=PROXY_HOST:PROXY_PORT
   Environment=https_proxy=PROXY_HOST:PROXY_PORT
   ```

5. Run the following command to reload the new proxy configuration:

   ```
   systemctl daemon-reload
   ```

6. Run following command to restart the HPE Service Manager Service Portal Launchpad:

   ```
   systemctl restart launchpad
   ```

After these steps are done, you should now see the RSS feeds load correctly.

Test the Service Manager Service Portal setup

Once you have completed the installation and configuration steps for Service Manager Service Portal, perform the following steps to test the setup.

1. Log in to Service Manager Service Portal:

   https://<Service Portal host name>:9000/org/Consumer (Use an LDAP user account: for example, "falcon" as the user and "1Qaz2wsx" as the password.)

2. Do the following to verify that shopping is correctly configured:
   a. From the Launchpad, click **Shop**.
   b. Select an item or find an item through a search, and then click **Order Now**.

c. Provide your order information, and then click **Submit**.

An order number is returned and a message is displayed indicating your request is pending approval.

3. Do the following to verify that ticketing is configured correctly:
   a. Return to the Launchpad.
   b. Click **Request Support**.
   c. Select an item or find an item through a search.
   d. Provide required information in the request form, and then click **Submit**.

   A Request ID is returned for the support request, whose status is **In Progress**.
4. Test the Survey and Chat features. For details, see the Survey and End User Chat documentation in the Service Manager Help Center and the Service Manager Service Portal Consumer Help.

Troubleshoot the Service Manager Service Portal installation

This section provides troubleshooting information that can assist you in installing Service Manager Service Portal.

HPE Operations Orchestration installation failed

Symptom:

HPE OO re-install is not successful when re-running the Ansible playbook.

Cause:

HPE OO installation failed and residual files and the central service are present on the Service Manager Service Portal host.

Fix:

1. Try running the HPE OO uninstaller:

```
# cd /opt/hp/oo
# ./uninstall --silent central
```

```
# cd opt/hp/
# rm -rf oo/
```

2. The central service might still be present:

```
# systemctl status central
# systemctl disable central
# systemctl reset-failed central
# rm -rf /etc/rc.d/init.d/central
```

OO configuration tasks fail due to proxy settings

Add the following lines to ansible_content/roles/oo/main.yml for each of the tasks that require to perform an HTTPS request:

```
environment:
no_proxy: <myVM.domain>
```

These tasks include:

- name: "Setup the admin user in OO"
- name: "Enable authentication in OO"
- name: "Create deployment number in OO"
- name: "Upload the base content pack to OO"
- name: "Deploy base content pack in OO"

The following is an example:

```
- name: "Deploy base content pack in OO"
  # This takes a while (in the background)
  uri:
    url: https://{{ ansible_fqdn }}:8443/oo/rest/latest/deployments/{{
deployment.json.deploymentProcessId }}?force=false
    method: PUT
    body_format: json
    validate_certs: no
    user: admin
    password: changeit
    force_basic_auth: yes
    use_proxy: no
status_code: "200,204"
environment:
no_proxy: <myVM.domain>
```

Installer fails if offline repository is not properly enabled

Symptom:

Cannot install required packages for the Service Manager Service Portal installer.

Cause:

The Service Manager Service Portal installer failed when using an offline repository that is not enabled properly.

Fix:

To add and enable an offline repository, follow these steps:

```
# yum repolist all
# yum-config-manager --add-repo http://<Repo_IP>/downloads/RHEL70/media.repo
# yum repolist all
```

repo id	repo name	status
MediaRepo	MediaRepo	disabled

```
# yum-config-manager --enable InstallMedia
```

> **Note:** This step might not enable the repo, and thus the next step is to manually edit the repo file.

```
# vi /etc/yum.repos.d/media.repo
```

```
[InstallMedia]
name=Red Hat Enterprise Linux 7.2
mediaid=1424360759.989
metadata_expire=-1
baseurl=http://<Repo_IP>/downloads/RHEL70/
enabled=1
cost=500
gpgcheck=0
# yum repolist all
```

repo id	repo name	status
MediaRepo	MediaRepo	enabled

Analytics service fails to start

Symptom:

The following error occurs:

```
Failed to start analytics.service: Unit analytics.service failed to load: No such
file or directory.
```

Cause:

The analytics service failed to start.

Fix:

Run the following commands to solve this problem:

```
#cd /etc/init.d
#rm –f analytics
# cat /opt/hp/propel/etc/services.d/analytics.daemon.sh >analytics
#chmod 777 analytics
#service analytics start
```

Installing Service Manager Service Portal on a different disk partition fails to create hardlinks for services

Symptom:

When installing Service Manager Service Portal services, if the /opt/hp directory points to a system on a different disk partition than /etc, the `setup.sh` setup utility will fail to install Service Manager Service Portal services.

Cause:

The Service Manager Service Portal setup utility tries to create hardlinks between systemd services under /etc/systemd/system and Service Manager Service Portal service definition files under /opt/hp/propel/etc/system/system. However, Red Hat Enterprise Linux only supports hardlinks for files under the same disk partition (because they share inodes), hence, the failure to install Service Manager Service Portal services.

Fix:

1. Copy the files physically from /opt/hp/propel/etc/systemd/system to /etc/systemd/system:

   ```
   #cp -a /opt/hp/propel/etc/systemd/system/* /etc/systemd/system/
   ```

2. Reload the systemctl daemon:

   ```
   # systemctl daemon-reload
   ```

3. Enable the HPE Propel services:

```
# systemctl enable <Services_Names>
```

Uninstall Service Manager Service Portal

If you need to uninstall Service Manager Service Portal and its components, perform the following steps:

1. Uninstall Operations Orchestration (OO):

```
# cd /opt/hp/oo
# ./uninstall --silent central
# cd opt/hp/
# rm -rf oo/
```

2. Remove the OO Central Service if it is still present:

```
# systemctl status central
# systemctl disable central
# systemctl reset-failed central
# rm -rf /etc/rc.d/init.d/central
```

3. Remove the OO database:

```
# su - postgres
#psql
postgres=# drop database oo;
postgres=# drop user oo;
```

4. Uninstall IDOL.

```
# cd /opt/hp/SmartAnalytics/_uninstall
# ./uninstaller -i silent
# cd /opt/hp
# rm -rf SmartAnalytics/
```

5. Uninstall Service Manager Service Portal:

```
# cd /opt/hp/propel-setup*
# ./setup.sh purge
```

Deploy a distributed Service Manager Service Portal cluster

Follow the instructions in this section to set up a distributed cluster of Service Manager Service Portal instances.

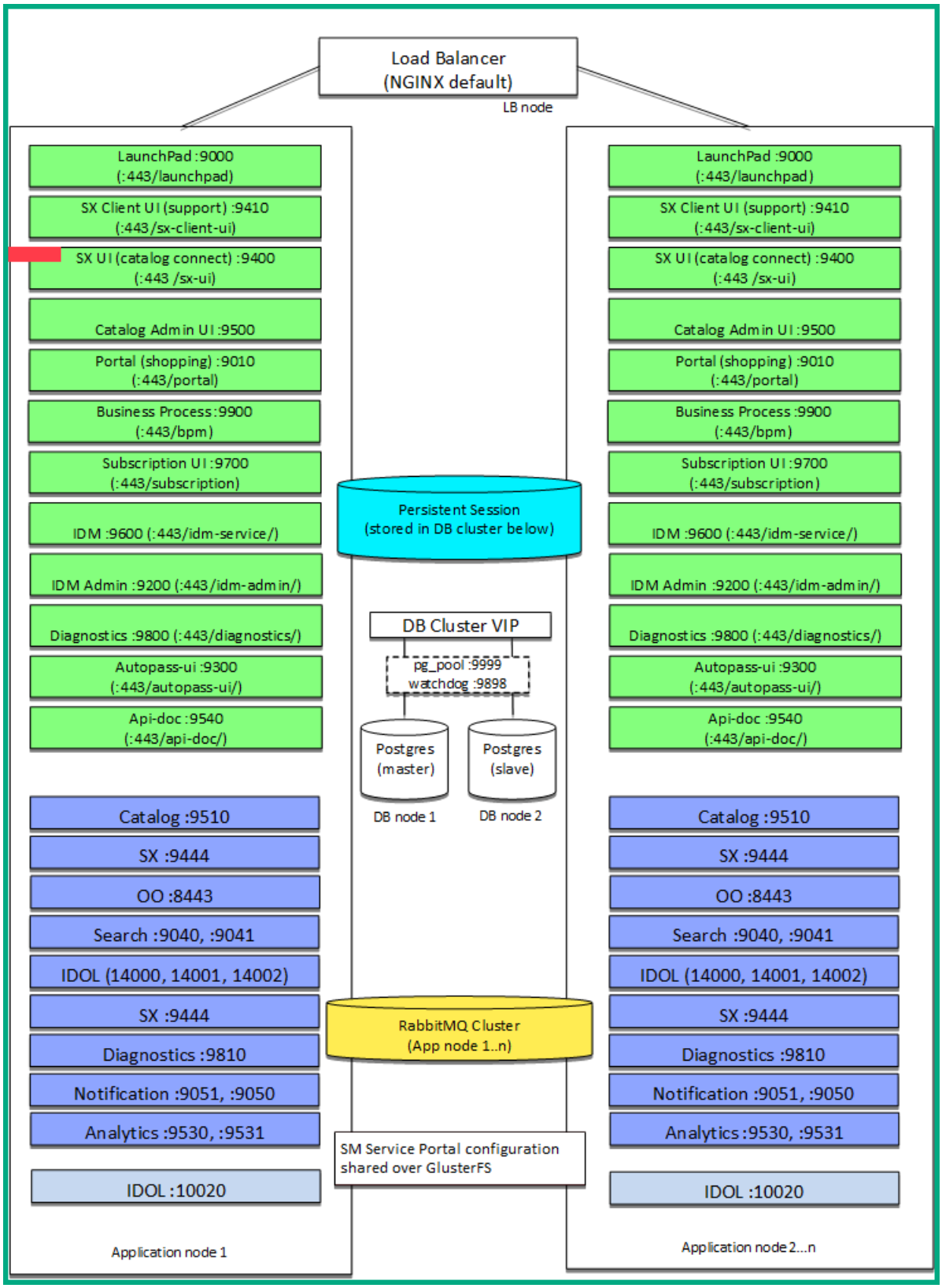
> **Tip:** For instructions on installing a single Service Manager Service Portal instance, see "Install and set up a single Service Manager Service Portal instance" on page 81.

Overview of distributed Service Manager Service Portal configuration

There are a minimum of five nodes recommended for distributed Service Manager Service Portal:

- One load balancer (VIP)
- Two Service Manager Service Portal application nodes
- Two Service Manager Service Portal database nodes. You can add additional Service Manager Service Portal nodes as desired. A DB VIP must also be set up.

The following figure shows a cluster with a Load Balancer node, a master DB node, a slave DB node, and two application nodes.


Load Balancer
(NGINX default)
LB node
LaunchPad :9000
(:443/launchpad)
SX Client UI (support) :9410
(:443/sx-client-ui)
SX UI (catalog connect) :9400
(:443 /sx-ui)
Catalog Admin UI :9500
Portal (shopping) :9010
(:443/portal)
Business Process :9900
(:443/bpm)
Subscription UI :9700
(:443/subscription)
IDM :9600 (:443/idm-service/)
IDM Admin :9200 (:443/idm-admin/)
Diagnostics :9800 (:443/diagnostics/)
Autopass-ui :9300
(:443/autopass-ui/)
Api-doc :9540
(:443/api-doc/)
Catalog :9510
SX :9444
OO :8443
Search :9040, :9041
IDOL (14000, 14001, 14002)
SX :9444
Diagnostics :9810
Notification :9051, :9050
Analytics :9530, :9531
IDOL :10020
Application node 1
Persistent Session
(stored in DB cluster below)
DB Cluster VIP
pg_pool :9999
watchdog :9898
Postgres
(master)
Postgres
(slave)
DB node 1
DB node 2
RabbitMQ Cluster
(App node 1..n)
SM Service Portal configuration
shared over GlusterFS
LaunchPad :9000
(:443/launchpad)
SX Client UI (support) :9410
(:443/sx-client-ui)
SX UI (catalog connect) :9400
(:443 /sx-ui)
Catalog Admin UI :9500
Portal (shopping) :9010
(:443/portal)
Business Process :9900
(:443/bpm)
Subscription UI :9700
(:443/subscription)
IDM :9600 (:443/idm-service/)
IDM Admin :9200 (:443/idm-admin/)
Diagnostics :9800 (:443/diagnostics/)
Autopass-ui :9300
(:443/autopass-ui/)
Api-doc :9540
(:443/api-doc/)
Catalog :9510
SX :9444
OO :8443
Search :9040, :9041
IDOL (14000, 14001, 14002)
SX :9444
Diagnostics :9810
Notification :9051, :9050
Analytics :9530, :9531
IDOL :10020
Application node 2...n

Service Manager Service Portal services communicate with each other over HTTP (RESTful) APIs. This allows the services to communicate with each other over the load balancer and enables further resilience inside of the Service Manager Service Portal application stack.

The Service Manager Service Portal PostgreSQL database will be clustered to provide redundancy. The default setup enables replication between two PostgreSQL DB nodes and provides automatic master-slave failover to the slave if the master goes down. We are not providing the enablement of a High Availability database which would imply scalability beyond two database nodes.

SSL is an important capability of the Service Manager Service Portal system. Managing and generating signed certificates is important for the security of the system. The configuration implemented in the Distributed Service Manager Service Portal scripts enables communications to be always encrypted. The default setup ensures that encryption is still enabled, but allows for self-signed certificates. In production systems, HPE recommends using only Certificate Authority-signed and trusted certificates.

The steps described in this section will accomplish the following distributed Service Manager Service Portal configuration:

- On the Load Balancer node, only NGINX is running. During the distributed Service Manager Service Portal configuration, this node is used to run the Ansible playbook scripts.
- On the two Service Manager Service Portal application nodes, all Service Manager Service Portal application services are running. The PostgreSQL instances should not be running here.
- On the two Service Manager Service Portal DB nodes, all Service Manager Service Portal services, OO and IDOL are disabled. These nodes are only used for DB purposes and are clustered using pgpool.

Terminology

The following table explains the common terms that you will find throughout the Service Manager Service Portal documentation.

Term	Description
Ansible	An Open Source software platform designed to consistently, reliably and securely configure and manage server and similar nodes with minimum overhead.
Ansible playbooks	Ansible playbooks leverage YAML and Jinja templates to organize complex Ansible jobs into roles and tasks. For more information, refer to the Ansible documentation.

Term	Description
DB VIP	A virtual IP address that does not correspond to an actual physical network interface. It is primarily used by pgpool as a floating IP address.
Distributed Service Manager Service Portal Cluster	A term used to describe a cluster of Service Manager Service Portal system servers (nodes) configured in such a way that they function as a single logical unit. The cluster provides both the High Availability and Scalability of the Service Manager Service Portal system.
Load balancer	A load balancer acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent users) and the availability of applications.
Master and slave databases	PostgreSQL refers to a multiple node database setup as Master/Slave.
NGINX	An Open Source high-performance load balancer. The default supported configuration of Distributed Service Manager Service Portal uses this product. For more information, see the NGINX documentation.
OO	HPE Operations Orchestration. Enables enterprise scale IT process automation. This product is used by Service Manager Service Portal.
pgpool	Middleware that supports PostgreSQL to provide connection pooling.
PostgreSQL	Open source object oriented relational DBMS. For more information, visit https://www.postgresql.org.
Service Manager Service Portal DB Node - High Availability	If a Service Manager Service Portal DB node or network route (connection) to a node goes down in a planned or unplanned outage, the Service Manager Service Portal system is still available to users. If the Master DB node breaks down, a fault is automatically detected and the Slave is automatically promoted to the Master, with no downtime.
Service Manager Service Portal Node - High Availability	When a Service Manager Service Portal server (node) or network route (or connection) to a node

Term	Description
	or a service instance goes down in a planned or an unplanned outage, the Service Manager Service Portal system is still available to users.
Service Manager Service Portal Scalability	The ability to add Service Manager Service Portal nodes to increase the scale of the Service Manager Service Portal system. Nodes are typically added to either increase the number of users that can be supported or the volume of transactions that can be processed.
RabbitMQ	Open source message-broker software that implements Advanced Message Queuing Protocol (AMQP). https://www.rabbitmq.com

Set up a distributed Service Manager Service Portal cluster

This section describes the detailed steps to set up a distributed Service Manager Service Portal cluster.

Prerequisites

Before you proceed, make sure that you have met the following prerequisites:

- Five (or more) VMs are available to use for the distributed Service Manager Service Portal cluster.

  For the minimum hardware and software requirements of each VM, see the Service Manager Service Portal section in the "Support matrix" on page 22.

- You have made a note of the fully qualified domain names (FQDNs) and IP addresses of the five (or more) VMs.

  This section uses the following items to refer to the host FQDNs.

Item	Description
<LB node host FQDN>	FQDN of the load balancer node host

Item	Description
<application node 1 FQDN>	FQDN of the Service Manager Service Portal application node 1 host
<application node 2 FQDN>	FQDN of the Service Manager Service Portal application node 2 host
<master DB node FQDN>	FQDN of the Service Manager Service Portal master database node host
<slave DB node FQDN>	FQDN of the Service Manager Service Portal slave database node host

- You have obtained one virtual IP address, which will be used as the DB VIP (a floating IP address for the database nodes)

Item	Description
<DB VIP>	Virtual IP address for the database nodes

The setup process consists of the following tasks.

> **Note:** In this section, it is assumed that five Service Manager Service Portal nodes will be set up; however, you can add additional Service Manager Service Portal cluster nodes according to your needs.

Task 1. Install Service Manager Service Portal on all nodes

In this task, you will install a Service Manager Service Portal instance on all nodes in the cluster.

Step 1. Register each node to the Red Hat Subscription service

You need to register each node to the Red Hat Subscription service. For more information, see "Register your system to the Red Hat Subscription service" on page 82.

To register a node, follow these steps:

1. Log in to your Red Hat 7.2 system as root.
2. Run the following command followed by the credentials used to log in to Red Hat Customer Portal:

   ```
   subscription-manager register
   ```

3. Run the following command:

   ```
   subscription-manager attach --auto
   ```

Step 2. Unzip the installation package on each node

On each node, run the following commands to unzip the Service Manager Service Portal installation package:

```
# mkdir /opt/hp
# cd /opt/hp
# unzip propel_complete_installer.zip
```

Step 3. Install Ansible on each node

On each node, run the following commands:

```
# cd /opt/hp/propel_complete_installer
# ./install_ansible.sh --proxy http://<proxy host>:<port>
```

Step 4. Prepare SSH connectivity for the root user to run Ansible playbooks

In this step, you will generate an SSH pubic key and copy the key to all nodes in the cluster. This key will be used by the root user to log in from the load balancer node to other nodes. The purpose of this step is to enable the root user on the load balancer node to log in to the other nodes in the cluster without being prompted for a password.

On the load balancer node, run the following commands:

```
# ssh-keygen -t rsa
# ssh-copy-id root@<LB node host FQDN>
# ssh-copy-id root@<application node 1 FQDN>
# ssh-copy-id root@<application node 2 FQDN>
# ssh-copy-id root@<master DB node FQDN>
# ssh-copy-id root@<slave DB node FQDN>
# mkdir /opt/hp/propel_complete_installer/ansible_content/ssh
```

```
# cd /opt/hp/propel_complete_installer/ansible_content/ssh
# cp ~/.ssh/* .
# cp id_rsa id_rsa-propel
```

Step 5. Run Ansible playbooks to prepare all nodes

In this step, you will configure an ansible_targets file on the load balancer node to set all cluster nodes as the Ansible targets and then run a command to run installation required Ansible playbooks on all of the configured nodes.

On the load balancer node, do the following:

1. Run the following commands:

   ```
   # cd /opt/hp/propel_complete_installer/ansible_content/
   # vim /opt/hp/propel_complete_installer/ansible_content/ansible_targets
   ```

2. In the ansible_targets file, add the following content:

   ```
   [redhat]
   <LB node host FQDN> ansible_ssh_user=root ansible_ssh_private_key_
   file=./ssh/id_rsa-propel
   <application node 1 FQDN> ansible_ssh_user=root ansible_ssh_private_key_
   file=./ssh/id_rsa-propel
   <application node 2 FQDN> ansible_ssh_user=root ansible_ssh_private_key_
   file=./ssh/id_rsa-propel
   <master DB node FQDN> ansible_ssh_user=root ansible_ssh_private_key_
   file=./ssh/id_rsa-propel
   <slave DB node FQDN> ansible_ssh_user=root ansible_ssh_private_key_
   file=./ssh/id_rsa-propel
   ```

3. Run the following command:

   ```
   # ansible-playbook -i ansible_targets deploy_rhel_complete.yml --extra-vars
   "http_proxy=http://<web proxy host>:<port> https_proxy=https://<web proxy
   host>:<port>"
   ```

Step 6. Install Service Manager Service Portal on each node

On each node, run the following commands to install Service Manager Service Portal:

```
# cd /opt/hp/propel_complete_installer
# unzip propel-setup*.zip -d /opt/hp/
# cd /opt/hp/propel-setup*/
# ./propel-ssl-setup.sh auto --hostname `hostname --fqdn` 2>&1 | tee ssl-setup.log
# ./setup.sh install `hostname --fqdn` 2>&1 | tee install.log
```

Step 7. Start Service Manager Service Portal on each node

On each node, do the following:

1. Run the following command to start Service Manager Service Portal:

   ```
   # propel start
   ```

2. Run the following command to check that all of the 35 services are active:

   ```
   # propel status
   ```

Step 8. Run Ansible playbooks to finalize the installation

The Ansible playbook scripts should be installed onto and run from the load balancer server.

On the load balancer node, run the Ansible playbooks to finalize the Service Manager Service Portal installation:

```
# cd /opt/hp/propel_complete_installer/ansible_content/
# ansible-playbook -i ansible_targets configure.yml --tags "initLWSSO" --extra-vars
'{"lwsso_init_string":"LWSSO_INIT_STRING"}'
# ansible-playbook -i ansible_targets configure.yml --tags "enableChat" --extra-
vars '{"toggle_chat":"on","chat_url":"https://<Apache server host>/chatui"}'
# ansible-playbook -i ansible_targets configure.yml --tags "enableSurvey" --extra-
vars '{"toggle_survey":"on","service_manager_url":"http://<SM server host
FQDN>:<port>"}'
# ansible-playbook -i ansible_targets configure.yml --tags "overrideDoc" --extra-
vars '{"doc_mode":"sm"}'
# ansible-playbook -i ansible_targets configure.yml --tags "enableServices" --
extra-vars '{"toggle_services":"off"}'
```

Where:

- **LWSSO_INIT_STRING** must match the **initString** value in the lwssofmconfig.xml file located in the Service Manager Server's RUN directory.
- **<Apache server host>** must be the FQDN of the Apache server that you installed when deploying Service Manager Collaboration.
- **http://<SM server host FQDN>:<port>** must be the Service Manager Server web service base URL. For example: http://mysmserverhost.mycompany.net:13080.

Step 9. Restart Service Manager Service Portal on each node

On each node, do the following:

1. Run the following commands to restart the application:

   ```
   # propel stop
   # propel start
   ```

2. Run the following command to check the status of services:

   ```
   # propel status
   ```

   > **Note:** Check that 37 services, including the **survey** and **survey-ui** services, are active.

Step 10. Verify the installation on each node

On each node, try logging in to Service Manager Service Portal with both the Consumer and Provider URLs and the corresponding user accounts. If the installation on a node is successful, you should be able to log in to the application on that node.

URL	User account
One of the following: • https://<LB node host FQDN>:9000/org/CONSUMER • https://<application node 1 FQDN>:9000/org/CONSUMER • https://<application node 2 FQDN>:9000/org/CONSUMER • https://<master DB node FQDN>:9000/org/CONSUMER • https://<slave DB node FQDN>:9000/org/CONSUMER	orgadmin/propel
One of the following: • https://<LB node host FQDN>:9000/org/Provider • https://<application node 1 FQDN>:9000/org/Provider • https://<application node 2 FQDN>:9000/org/Provider • https://<master DB node FQDN>:9000/org/Provider • https://<slave DB node FQDN>:9000/org/Provider	admin/propel

Task 2. Set a password for "propel" on each node

In this task, you will set a password for the "propel" user and allow this user to run any commands from anywhere.

> **Note:** This password will be used in later configuration tasks.

On each node, do the following:

1. Run the following command:

   ```
   # passwd propel
   ```

   When prompted, enter a password (for example, **propel2015**).

2. Run the following command:

   ```
   # visudo
   ```

3. Insert the following line below the “root ALL=(ALL) ALL” line, as shown below:

   ```
   propel  ALL=(ALL)    ALL
   ```

   After this change, the lines should look like the following:

   ```
   root ALL=(ALL)       ALL
   propel  ALL=(ALL)    ALL
   ```

Task 3. Change the host name to lowercase on each database node

On each of the two database nodes, do the following:

1. Run the following commands:

   ```
   # hostname <database node FQDN in lowercase>
   ```

2. Change the host name in the hostname file to lowercase:

   ```
   # vi /etc/hostname
   ```

Task 4. Prepare the load balancer node

Perform the following steps to prepare the load balancer node.

Important: Before performing the steps, log on to the load balancer node as the "propel" user.

Step 1. Check network connectivity and get the hosts keys

Verify the network connectivity between the Load Balancer Node (acting as the Ansible Management Node) and all the Service Manager Service Portal Node servers by making an ssh connection from the Load Balancer to the Service Manager Service Portal servers (Cluster and DB nodes) using the FQDN.

Caution: Do not forget to make an ssh connection to the Load Balancer server as well.

Run the following command:

```
# su - propel
# cd /opt/hp/propel/contrib/propel-distributed*
# ssh-keygen -t rsa -f ~/.ssh/id_rsa
# ssh-copy-id propel@<LB node host FQDN>
# ssh-copy-id propel@<application node 1 FQDN>
# ssh-copy-id propel@<application node 2 FQDN>
# ssh-copy-id propel@<master DB node FQDN>
# ssh-copy-id propel@<slave DB node FQDN>
```

Note: After completing this step, ssh calls should execute without a password prompt.

Step 2. Define Ansible nodes (hosts)

1. Navigate to the /opt/hp/propel/contrib/propel-distributed.<version> directory.
2. Copy the inventory/hosts.example file to inventory/hosts.default:

   ```
   # cp inventory/hosts.example inventory/hosts.default
   ```

3. In the inventory/hosts.default file, change the fully qualified host names of all cluster nodes in the [lb], [propel], [db_m], and [db_s] sections, the IP address of the load balancer node in the [lb_ip] section, and the virtual IP address of the database cluster in the [db_vip] section to values that describe your actual configuration. The following table provides a description of each section.

Section	Description
[lb]	Front-end load balancer address
[lb_ip]	IP address of the load balancer
[propel]	All Service Manager Service Portal application nodes within the Service Manager Service Portal cluster
[db_m]	Service Manager Service Portal master DB node within the Service Manager Service Portal cluster (one)
[db_s]	Service Manager Service Portal slave DB node within the Service Manager Service Portal cluster
[db_vip]	The VIP address for the PostgreSQL cluster. A VIP is a virtual IP address; so this is an address that uses a virtual adapter on the pg_pool cluster. Pgpool has a watchdog service that will float the IP address between the cluster nodes to provide a reliable connection. This unused IP should be ping-able, reachable within the same subnet as the Service Manager Service Portal application and DB nodes, and will be linked to the primary Ethernet port (eth0) of the Service Manager Service Portal DB nodes.
[*:children]	Support roles. **Caution:** Do not change this part unless you know what you are doing.

```
#Vi inventory/hosts.default
[lb]
<LB node host FQDN>

[lb_ip]
<LB node host IP address>

[propel]
<application node 1 FQDN>
<application node 2 FQDN>

[db_m]
<master DB node FQDN>

[db_s]
<slave DB node FQDN>

[db_vip]
<database cluster virtual IP address>
```

The following is an example:

```
[lb]
vm0541.hpe.net

[lb_ip]
1x.1xx.1xx.xx

[propel]
vm0546.hpe.net
vm0624.hpe.net

[db_m]
vm0671.hpe.net

[db_s]
vm0682.hpe.net

[db_vip]
1x.1xx.1xx.1xx
```

Step 3. Check your Ansible Node Hosts file

Verify that your Ansible node hosts file is set up correctly and recognized by Ansible. Run the following commands and verify the results look correct:

```
# cd /opt/hp/propel/contrib/propel-distributed*
# ansible propeld -u propel -m ping -c paramiko
```

> **Note:** For every host you may be asked if the fingerprint is correct. Type 'yes' and press Enter. This command should finish without user input next time. The script should finish in matter of seconds. If the execution takes longer, it might be waiting for your input.

Step 4. Install the distributed Service Manager Service Portal scripts

1. Copy the group_vars/propeld.yml.example file to group_vars/propeld.yml:

   ```
   # cp group_vars/propeld.yml.example group_vars/propeld.yml
   ```

2. Online installation: follow this step if your cluster has access to the Internet:

   Update Proxy Settings in group_vars/propeld.yml according to your corporate proxy settings:

```
# vim group_vars/propeld.yml

proxy_env:
http_proxy: http://proxy.example.com:8080
https_proxy: http://proxy.example.com:8080
```

3. Offline installation: follow these steps if your cluster has no Internet access:
   a. Set propeld.packages.download to false in group_vars/propeld.yml:

      ```
      # vim  group_vars/propeld.yml
      ```

   b. Copy Service Manager Service Portal Distributed scripts to a machine that is connected to the Internet and run download_packages.sh. The script should finish without any errors. If not, check the script output, resolve possible issues and run it again. After a successful run, the .packages directory should be populated with RPM packages required for the installation.
   c. Copy the .packages directory to the load balancer node's Service Manager Service Portal Distributed scripts directory and proceed with the installation.

Step 5. Define an alternate network interface name on all database nodes

1. Run 'ip a' and check the network interface name.

   > **Note:** The default interface name is `ens32`, which is used as an example in the following steps.

2. Run the following command:

   ```
   # vi group_vars/propeld.yml
   ```

   Uncomment the line:

   ```
   # interface: eth0
   ```

   Change `eth0` in the line above to your network interface name. For example:

   ```
   interface: ens32
   ```

3. Run the following command:

   ```
   # vi postgresql_handlers/defaults/main.yml
   ```

   Change `eth0` in the `interface` line to `ens32`:

   ```
   interface: ens32
   ```

Task 5. Run the Distributed Service Manager Service Portal scripts on the load balancer node

Before you perform this task, make sure you have completed the previous tasks. This task will execute a set of scripts to set up a distributed Service Manager Service Portal cluster.

Caution: Once this task is performed, you cannot rerun configure.yml and deploy_rhel_complete.yml anymore.

- If you modified any of the Ansible YAML scripts, use the online parser to check for syntax errors before running them: http://yaml-online-parser.appspot.com/.
- When prompted by the first script for the SUDO Password, you need to provide the password of the **propel** user on the target server (that is, **propel2015**).
- If any of the scripts are aborted before completion, it is safe to rerun them.

On the load balancer node, do the following:

1. Run the following commands:

   ```
   # cd /opt/hp/propel/contrib/propel*
   # ansible-playbook propeld.yml -c paramiko --ask-become-pass -u propel 2>&1 |
   tee setup.out
   ```

   When prompted, enter the password for the "propel" user.

2. If the previous commands successfully finish, your Service Manager Service Portal cluster should be installed and ready for use.

Caution: If you have added "propel ALL=(ALL) ALL" to /etc/sudoers, do not forget to remove it from all machines to minimize security risks.

Task 6. Configure OO database connection on application nodes

On each of the two application nodes, do the following:

1. Log on to the application node (for example, application node 1) as root.
2. Copy the following files from the master database node:

   ```
   # cd /opt/hp/oo/central/var/security
   # scp root@<master DB node FQDN>:/opt/hp/oo/central/var/security/encryption_
   repository .
   # scp root@<master DB node
   FQDN>:/opt/hp/oo/central/var/security/credentials.store .
   ```

3. Run the following commands to obtain an encrypted value of the OO database password (the default password value is "oo"):

   ```
   #cd /opt/hp/oo/central/bin
   [root@<application node 1 FQDN> bin]# ./encrypt-password --encrypt --password
   oo
   ```

   An encrypted password is returned. For example:

   ```
   {ENCRYPTED}H2UfmdGFuAhvd5ysuX+PBw==
   ```

4. Copy the encrypted password to OO:
   a. Open the OO Central database.properties file:

      ```
      #vi /opt/hp/oo/central/conf/database.properties
      ```

   b. In this file, replace the db.password value with the encrypted password value you obtained previously, and change "==" at the end of the string to "\=\=". For example:

      ```
      db.password={ENCRYPTED}H2UfmdGFuAhvd5ysuX+PBw\=\=
      ```

Task 7. Configure Survey for the cluster

This task includes the following steps.

> **Note:** After completing the this task, you also need to update the Service Manager Service Portal URL in the System Information Record in Service Manager so that survey links sent through email can work. For details, see "Task 8. Update the System Information Record in Service Manager" on page 147.

Step 1. Open two survey ports for the application nodes

In this step, you will open two ports (9980 and 9981) for the two application nodes for the Survey functionality.

Note: Perform this step from the load balancer node as root.

1. Log on to the load balancer node as root.
2. Add the following lines in the /etc/nginx/conf.d/propel.conf file:

```
upstream survey {
    server <application node 1 FQDN>:9980;
    server <application node 2 FQDN>:9980;
}

upstream survey-ui {
    server <application node 1 FQDN>:9981;
    server <application node 2 FQDN>:9981;
}

server {
    listen 9981 ssl;

    proxy_cookie_domain idm $host;

    proxy_http_version 1.1;

    proxy_set_header Connection "upgrade";
    proxy_set_header Host $host:$server_port;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header X-Forwarded-For $remote_addr;
    proxy_set_header X-Real-IP $remote_addr;

    ssl_certificate /opt/hp/propel/security/propel_host.crt;
    ssl_certificate_key /opt/hp/propel/security/propel_host.key.rsa;

    location / {
        proxy_pass https://survey;
    }
}

server {
    listen 9980 ssl;

    proxy_cookie_domain idm $host;

    proxy_http_version 1.1;

    proxy_set_header Connection "upgrade";
    proxy_set_header Host $host:$server_port;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header X-Forwarded-For $remote_addr;
```

```
        proxy_set_header X-Real-IP $remote_addr;

        ssl_certificate /opt/hp/propel/security/propel_host.crt;
        ssl_certificate_key /opt/hp/propel/security/propel_host.key.rsa;

        location / {
            proxy_pass https://survey-ui;
        }
    }
```

3. Restart Nginx:

```
# systemctl restart nginx
```

Step 2. Modify the survey configuration on the application nodes

In this step, you will update the survey configuration on each of the two application nodes by changing the FQDN of each node to the FQDN of the load balancer node.

On each of the application nodes, perform the following steps:

1. Open the following files:
   - /opt/hp/propel/survey/config.yml
   - /opt/hp/propel/survey-ui/app.json
2. Change the local host FQDN in each file to the FQDN of the load balancer node.
3. Restart the survey service:

```
# systemctl stop survey
# systemctl start survey
```

Task 8. Update the System Information Record in Service Manager

For a cluster configuration, you must configure the Service Manager Service Portal URLs in the System Information Record based on the load balancer node.

> **Note:** These URLs are used by the Survey and End User Chat functionalities.

To update the System Information Record, follow these steps:

1. Log on to Service Manager as a system administrator.
2. Click **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
3. Click the **Active Integrations** tab.
4. In the **Service Manager Service Portal URL** field, enter the load balancer node base URL:

   ```
   https://<LB node FQDN>:9000
   ```

5. In the **Service Manager Service Portal Support Ticket URL** field, enter the load balancer node support ticket URL:

   ```
   https://<LB node FQDN>:9410/support/requests/create
   ```

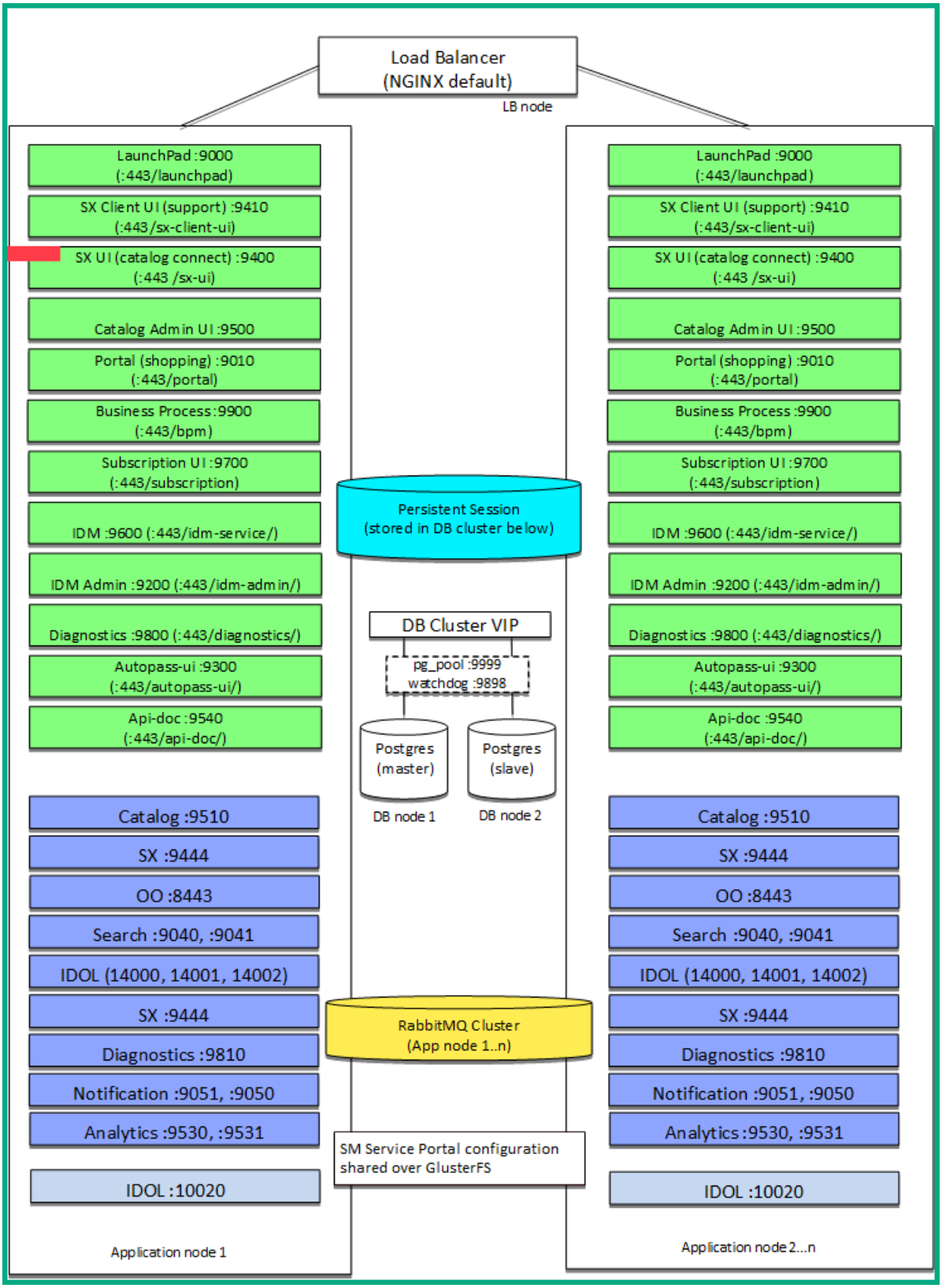
6. Save the record.

Next, you will need to deploy IDOL content servers in high availability mode. See "Set up IDOL content servers" below.

Set up IDOL content servers

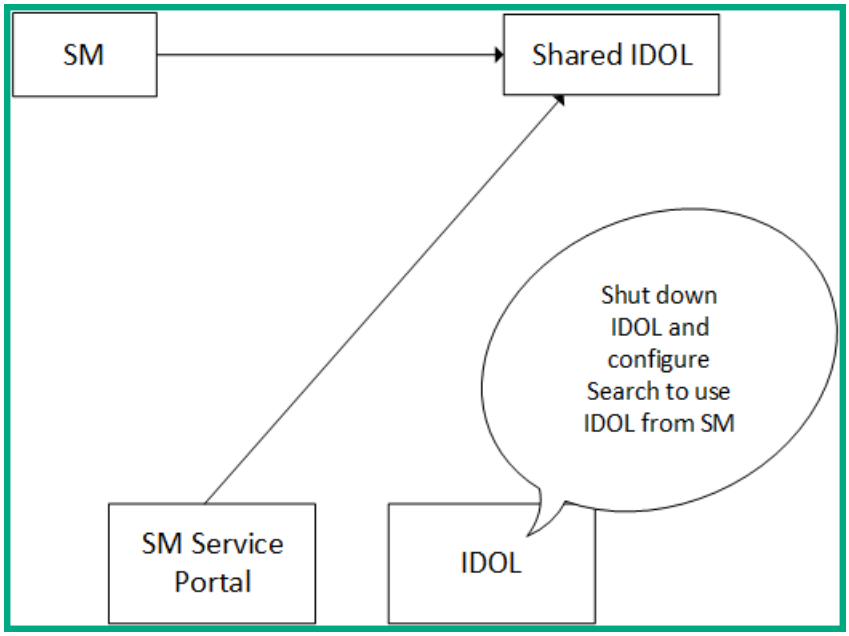
There are two possible deployment configurations for Service Manager Service Portal and its use of IDOL:

- Smart Analytics is not enabled in Service Manager, and Service Manager uses the Solr Search Engine for Knowledge Management search; IDOL is installed on the Service Manager Service Portal application node servers. See the following figure for an example.


Load Balancer
(NGINX default)
LB node
LaunchPad :9000
(:443/launchpad)
SX Client UI (support) :9410
(:443/sx-client-ui)
SX UI (catalog connect) :9400
(:443 /sx-ui)
Catalog Admin UI :9500
Portal (shopping) :9010
(:443/portal)
Business Process :9900
(:443/bpm)
Subscription UI :9700
(:443/subscription)
IDM :9600 (:443/idm-service/)
IDM Admin :9200 (:443/idm-admin/)
Diagnostics :9800 (:443/diagnostics/)
Autopass-ui :9300
(:443/autopass-ui/)
Api-doc :9540
(:443/api-doc/)
Catalog :9510
SX :9444
OO :8443
Search :9040, :9041
IDOL (14000, 14001, 14002)
SX :9444
Diagnostics :9810
Notification :9051, :9050
Analytics :9530, :9531
IDOL :10020
Application node 1
Persistent Session
(stored in DB cluster below)
DB Cluster VIP
pg_pool :9999
watchdog :9898
Postgres
(master)
Postgres
(slave)
DB node 1
DB node 2
RabbitMQ Cluster
(App node 1..n)
SM Service Portal configuration
shared over GlusterFS
LaunchPad :9000
(:443/launchpad)
SX Client UI (support) :9410
(:443/sx-client-ui)
SX UI (catalog connect) :9400
(:443 /sx-ui)
Catalog Admin UI :9500
Portal (shopping) :9010
(:443/portal)
Business Process :9900
(:443/bpm)
Subscription UI :9700
(:443/subscription)
IDM :9600 (:443/idm-service/)
IDM Admin :9200 (:443/idm-admin/)
Diagnostics :9800 (:443/diagnostics/)
Autopass-ui :9300
(:443/autopass-ui/)
Api-doc :9540
(:443/api-doc/)
Catalog :9510
SX :9444
OO :8443
Search :9040, :9041
IDOL (14000, 14001, 14002)
SX :9444
Diagnostics :9810
Notification :9051, :9050
Analytics :9530, :9531
IDOL :10020
Application node 2...n

An Ansible playbook configures mirrored IDOL as explained in "Set up mirrored IDOL" below.

- Smart Analytics is enabled in Service Manager, and IDOL is installed on Service Manager application nodes. Service Manager Service Portal and Service Manager use shared IDOL instances. See the following figure.



In this configuration, the Service Manager Service Portal Search service on all application nodes must be modified to reference the shared IDOL instances.

For details, see "Set up shared IDOL" on page 155.

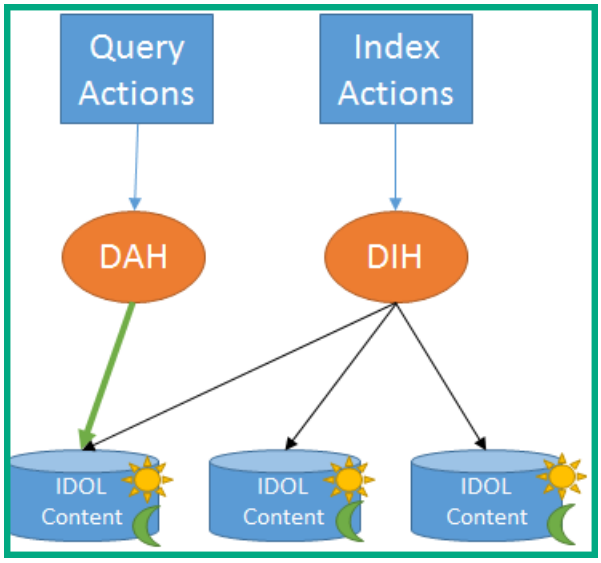
Set up mirrored IDOL

The default Service Manager Service Portal configuration is to have each application node maintain its own instance of IDOL. This is problematic in a distributed cluster system because the IDOL instances are not synchronized in any way. To solve this problem, you can mirror the IDOL content servers so they are kept in sync across multiple distributed Service Manager Service Portal nodes.

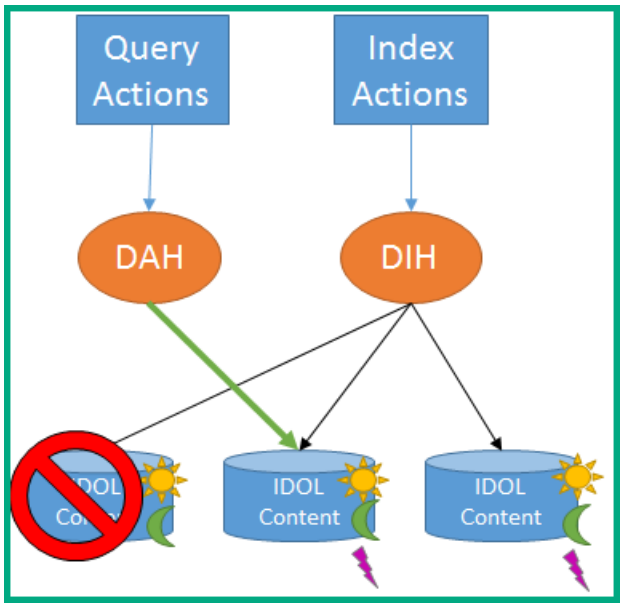
A distributed IDOL setup is composed of a few different components, the important ones are as follows: Distributed Index Handler (DIH), Distributed Action Handler (DAH), and Content Servers. Mirroring the data between IDOL content servers allows for high availability by having multiple identical servers. If one server goes down, we can failover to another that is an exact copy and continue seamlessly.

The following figures show a simple mirroring architecture where the DIH replicates all changes to every IDOL content server. In this solution, the DAH uses a single IDOL instance as a primary server and only uses others as a backup if the primary fails. All actions are queued for the failed servers. Once the failed servers are up again, all queued actions are replayed, but the primary server is not reverted to the original.

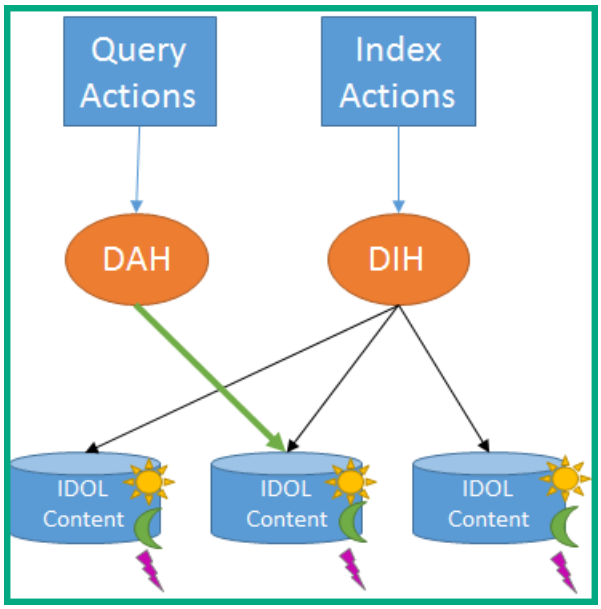
Before failure



During failure



After failure



Set up load balancing

The default of the Distributed Service Manager Service Portal installation is to use an identical IDOL configuration on each node and rely on NGINX for load balancing. By configuring each instance of the Service Manager Service Portal Search service to point to its local IDOL instance (that is identically configured), Search will point to the same IDOL server no matter which instance of Search is used, and seamlessly failover to the same IDOL if the primary goes down.

Change IDOL configurations

The IDOL configuration is identical on all of the Service Manager Service Portal nodes.

> **Important:** Use the actual IP addresses or host names of the machines in the configurations. Do not use 127.0.0.1 or localhost so that the configuration files can be copied across servers without errors.

The Distributed Service Manager Service Portal scripts implement the following changes to the main IDOL server configuration file /opt/hp/SmartAnalytics/IDOL/IDOLServer.cfg on each Service Manager Service Portal node:

1. Whitelist all the IP addresses of all servers.

   The following figure shows an example, where IP addresses 1.1.1.1, and 2.2.2.2 have been added in 5 locations.

```
[Service]
ServicePort=14002
//the IP address of clients that are permitted to send queries to IDOL.
//they should be altered to your SM server address, and admin ip address range
ServiceStatusClients=*,127.0.0.1,::1,127.0.0.1,1.1.1.1,2.2.2.2
ServiceControlClients=*,127.0.0.1,::1,127.0.0.1,1.1.1.1,2.2.2.2
Access-Control-Allow-Origin=*

[Server]
. . .
//------------------------- Clients Settings -------------------------//
//the IP address of clients that are permitted to send queries to IDOL.
//they should be altered to your SM server address, and admin ip address range
QueryClients=*,127.0.0.1,::1,127.0.0.1,1.1.1.1,2.2.2.2
AdminClients=*,127.0.0.1,::1,127.0.0.1,1.1.1.1,2.2.2.2
IndexClients=*,127.0.0.1,::1,127.0.0.1,1.1.1.1,2.2.2.2
```

2. Enable mirror mode and remove any non-mirror mode configurations.

   Here, the **mirrormode** parameter is set to True, all the DIH settings are commented out, and "DistributionMethod=0" is added.

```
[DistributionSettings]
StoredStateTokenLifetime=0
mirrormode=True
//DIH settings:
#DistributeByFields=True
#DistributeByFieldsCSVs=*/ContentStore
#UnknownFieldValueAction=Default
#UnknownFieldValueDefaultEngine=0
#DistributeOnMultipleFieldValues=True
//The following parameter is required for the DAH if mirrormode is set to false
#VirtualDatabases=1
#UseEngineAlias=true
// DAH Settings
DistributionMethod=0
```

3. Configure IDOL servers and remove Virtual Database Configurations.

   - The "Number" field MUST equal the total number of Configured IDOL Servers.
   - Each [IDOLServerN] section must be sequential starting at 0.
   - IDOL will choose the first Server (having the lowest sequential number) as the primary.

- Do not use localhost or 127.0.0.1 for the Host so that the file can be copied around to the servers without trouble.

The following figure shows an example.

```
//This section is equivalent to the [engines] section
// in the DAH and DIH standalone configuration

[DistributionIDOLServers]
Number=2

[IDOLServer0]
Name=Content-Propel
Host=1.1.1.1
Port=10020

[IDOLServer1]
Name=Content-Propel-Failover-1
Host=2.2.2.2
Port=10020

// Remove or comment out all [vdbX] sections
```

4. As a precautionary measure, IDOL will not allow a user to switch from mirror mode to non-mirror mode or vice versa, because it will result in data loss. Assuming you are fine with losing all your data (indexes) stored in IDOL, delete the /SmartAnalyitcs/IDOL/dih/main directory on each of the servers before restarting the service.

   In the context of Service Manager Service Portal, a simple catalog reindex will suffice for repopulating data indexes in IDOL:

   ```
   # cd /opt /hp/ propel/catalog
   # java -jar lib/catalog.jar reindex
   ```

5. Restart the idol services:

   ```
   # cd /opt/hp
   # service idolserver restart
   ```

For testing purposes, you can disable a single Service Manager Service Portal IDOL content instance to manually trigger the failover:

```
# cd /opt/hp
# service idol-content-propel stop
```

Note: Currently, the NGINX configuration does not have a health check for both the Search service and DAH/DIH endpoints. Until the health checks are correctly configured, this solution will

not support high availability if the DAH/DIH fails.

Tip: Next, you will need to replace the Service Manager Service Portal generated certificates for the Service Manager Service Portal cluster. See "Replace Service Manager Service Portal generated certificates" below.

Set up shared IDOL

For high availability, if you want Service Manager Service Portal to use the IDOL instances deployed for Service Manager for Knowledge Management search, follow the instructions in this section.

To set up shared IDOL, follow these steps:

1. Deploy the SM shared IDOL in high availability mode. For details, see "Configure Smart Analytics for high availability" on page 272.
2. Shut down the IDOL services on each Service Manager Service Portal node:

   ```
   #service idolserver stop
   ```

3. Configure each Service Manager Service Portal node to use the SM shared IDOL. For details, see the instructions in the *Service Manager uses Smart Analytics as the search engine* part in "Enable Knowledge Management search" on page 114.

Tip: Next, you will need to replace the Service Manager Service Portal generated certificates for the Service Manager Service Portal cluster. See "Replace Service Manager Service Portal generated certificates" below.

Replace Service Manager Service Portal generated certificates

The Service Manager Service Portal Cluster uses GlusterFS to synchronize Service Manager Service Portal configuration files across the entire cluster. Therefore, all SSL configuration changes should be made on a single node (usually the load balancer node).

To set up SSL, replace the Service Manager Service Portal generated SSL certificates with CA-signed certificates. To do this, follow these steps:

1. Connect to load balancer node:

   ```
   # ssh propel@<lb_host>
   ```

2. Stop Service Manager Service Portal:

   ```
   # ansible propel -a "propel stop"
   ```

3. Follow the steps in "Replace the Service Manager Service Portal generated SSL certificates" on page 98.

4. Restart Service Manager Service Portal:

   ```
   # ansible propel -a "propel start"
   ```

Failover and recovery

The following describes typical failover scenarios and their recovery actions.

Pgpool stops on the standby database server

Verify that the standby database server is healthy:

1. From the primary database server:

   ```
   # sudo -u postgres psql -h <standby> -p 5432 -c 'select pg_is_in_recovery()'
   pg_is_in_recovery
   -------------------
   t
   (1 row)
   ```

2. If this query returns "t" as shown above, then all that is required is to restart pgpool from the standby database server:

   ```
   # systemctl start pgpool.service
   ```

3. Confirm pgpool is running properly:

   ```
   # systemctl status pgpool.service
   ```

Pgpool stops on the primary database server

Verify that the primary database server is healthy:

1. From the standby database server:

   ```
   # sudo -u postgres psql -h <primary> -p 5432 -c 'select pg_is_in_recovery()'
   pg_is_in_recovery
   -------------------
   f
   (1 row)
   ```

2. If this query returns "f" as shown above, then all that is required is to restart pgpool from the primary database server:

   ```
   # systemctl start pgpool.service
   ```

3. Confirm pgpool is running properly:

   # systemctl status pgpool.service

PostgreSQL stops on the standby database server

1. First, perform a backup of the primary database server.
2. Address the root cause of PostgreSQL's stoppage.
3. From the primary server, run the following command to confirm that connectivity exists with the primary server:

   ```
   # ssh <standby> service pgpool status
   ```

   <- should see normal pgpool status output ->

4. From the standby server, restart PostgreSQL:

   ```
   # systemctl status pgpool.service
   ```

5. From the primary server, confirm that pgpool has attached to both the primary and standby servers:

   ```
   # sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"
   ```

The command should return something like this:

```
node_id | hostname | port | status | lb_weight | role
---------+----------+------+--------+-----------+---------
0 | <primary> | 5432 | 2 | 0.500000 | primary
1 | <standby> | 5432 | 2 | 0.500000 | standby
```

The "role" column should contain the appropriate primary/standy value and the status column should be "2" for both nodes.

6. Confirm replication is active. To do this, run the following command from the primary server:

   ```
   # sudo -u postgres psql -h <primary> -p 5432 -c 'select sent_location, replay_
   location from pg_stat_replication'
   ```

   The command should return something like this:

   ```
   sent_location | replay_location
   ---------------+-----------------
   7D/90004B0 | 7D/9000478
   ```

   (1 row)

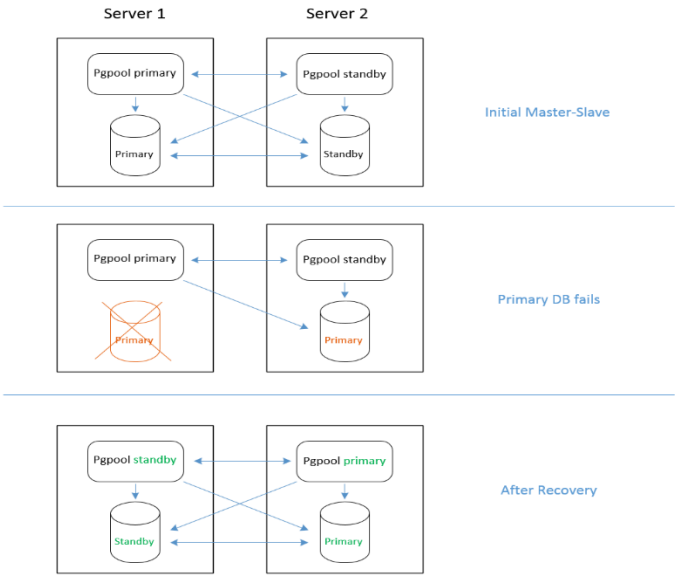
7. Wait 60 seconds, and run the same command. The results should differ.

PostgreSQL stops on the primary database server

Recovery will involve a Service Manager Service Portal service outage. After recovery, the primary and standby databases will swap roles.

> **Note:** In the following steps, "new-primary" refers to the original standby server, which has been promoted. Similarly, "new-standby" refers to the original primary server, which has stopped.

The following diagram illustrates how the system changes when a failover event occurs.



1. On the new-standby, stop pgpool and confirm PostgreSQL is stopped:

   ```
   # systemctl stop pgpool.service
   # systemctl status pgpool.service
   ```

2. Stop Service Manager Service Portal and OO on all Service Manager Service Portal nodes:

   ```
   # propel stop
   # systemctl stop central.service
   ```

3. Perform a backup of new-primary database server.

4. On the new-primary, restart PostgreSQL and pgpool:

   ```
   # systemctl restart pgpool.service
   # systemctl restart postgresql-9.5.service
   ```

5. Confirm that the new-primary has been promoted:

   ```
   # sudo -u postgres psql -h <new-primary> -p 5432 -c 'select
   pg_is_in_recovery()'

   pg_is_in_recovery

   ------------------

   f

   (1 row)
   ```

   The result should be "f", as shown above.

6. Run the following command:

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"

node_id | hostname | port | status | lb_weight | role

---------+--------------+------+--------+-----------+---------

0 | <new-standby> | 5432 | 3 | 0.500000 | standby

1 | <new-primary> | 5432 | 2 | 0.500000 | primary
```

The “role” values should be reset. The new-primary should have a status “2” (up), and the new-standby should have a status of “3” (down).

7. On the load-balancer node, create a new inventory file with the primary and standby servers reversed. For example, if the original primary server was db1.hpe.net and the original standby server was db2.hpe.net, your new inventory would have this content:

```
[postgres]
db2.hpe.net ansible_ssh_user=root
db1.hpe.net ansible_ssh_user=root
[db_master_nodes]
db2.hpe.net ansible_ssh_user=root
[db_slave_nodes]
db1.hpe.net ansible_ssh_user=root
```

8. For this example, we assume the new inventory file is /opt/hp/propel/contrib/propeldistributed.<version>/inventories/recovery_cluster. Then from the directory /opt/hp/propel/contrib/propel-distributed.<version> on the load balancer node, rerun Ansible playbook db.yml:

```
# ansible-playbook db.yml -c paramiko --ask-become-pass -u propel 2>&1 | tee
recovery.out
```

9. Verify the new-primary and new-master are running. From the load balancer node, run the following command:

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"

node_id | hostname | port | status | lb_weight | role
---------+--------------+------+--------+-----------+---------
0 | <new-primary> | 5432 | 2 | 0.500000 | primary
1 | <new-standby> | 5432 | 2 | 0.500000 | standby
```

The “role” column should reflect the new server statuses. The “status” column should be “2” for both nodes.

10. Confirm replication is active:

```
# sudo -u postgres psql -h <new-primary>; -p 5432 -c 'select sent_location,
replay_location from pg_stat_replication'
```

```
sent_location | replay_location
--------------+-----------------
7D/90004B0 | 7D/9000478
(1 row)
```

11. Wait 60 seconds, and run the same command. The results should differ.
12. On each Service Manager Service Portal node, start Service Manager Service Portal and start OO:

    ```
    # propel start
    # service central start
    ```

13. Verify that the mpp service has initialized properly and restart it if necessary:

    ```
    # service mpp status
    ```

Standby server down or unavailable

After addressing the root cause of the server outage, see the ""PostgreSQL stops on the standby database server" on page 157" failover scenario.

> **Note:** If the server exited abruptly, pgpool may not initialize properly. See troubleshooting note ""Pgpool not attaching to nodes" on page 167".

Primary server down or unavailable

After addressing the root cause of server outage, see the ""Pgpool stops on the primary database server" on page 157" failover scenario.

> **Note:** If the server exited abruptly, pgpool may not initialize properly. See troubleshooting note ""Pgpool not attaching to nodes" on page 167".

Service Manager Service Portal node down or unavailable

1. After addressing the root cause of server outage, restart Service Manager Service Portal and OO:

   ```
   # propel stop
   # propel start
   # systemctl restart central.service
   ```

2. Verify that the Portal service has initialized properly and restart if necessary:

   ```
   # systemctl status portal
   ```

Load balancer down or unavailable

1. After addressing the root cause of the server outage, restart nginx:

   ```
   # service nginx restart
   ```

   If the backup image of the load balancer contains a Service Manager Service Portal installation, it may be necessary to stop Service Manager Service Portal and OO:

   ```
   # propel stop
   # systemctl restart central.service
   ```

2. Verify that no node processes are running:

   ```
   # ps –ef | grep node
   ```

Disaster recovery

This section assumes that a Distributed Service Manager Service Portal Disaster Recovery (DR) system has already been set up.

Set up a Service Manager Service Portal Disaster Recovery (DR) cluster

1. Make sure that Service Manager Service Portal is stopped on the Service Manager Service Portal nodes of the DR cluster.
2. On the DR cluster's master DB node:
   a. [Optional] Make a backup of the /var/lib/pgsql/9.5/data directory.
   b. Delete the data directories:

      ```
      # rm -rf /var/lib/pgsql/9.5/data/*
      ```

   c. Set up replication from the Primary Cluster master DB node to the DR cluster master DB nod:

      ```
      # su - postgres
      # pg_basebackup --dbname="postgresql://repl:replpass@<primary-cluster-
      master-db>/" -D /var/lib/pgsql/9.5/data -P --xlog-method=stream
      ```

   d. Create recovery.conf under /var/lib/pgsql/9.5/data:

      ```
      # vi /var/lib/pgsql/9.5/data/recovery.conf
      standby_mode = 'on'
      primary_conninfo = 'host=< primary-cluster-master-db> user=repl
      password=replpass'
      restore_command = 'cp /var/lib/postgresql/9.5/archive/%f %p'
      recovery_target_timeline='latest'
      trigger_file = '/tmp/pgsql.trigger'
      ```

   e. Changes the permissions:

      ```
      # chown postgres:postgres recovery.conf
      ```

   f. Restart postgres on both the DR master and slave nodes:

      ```
      # service postgressql-9.5 restart
      ```

g. Verify the setup:
   i. On the DR cluster, make sure both DB nodes are on standby.

	Step	Command	Output
a)	Check the Master postgres	sudo -u postgres psql -h <primary> -p 5432 -c "SELECT pg_is_in_recovery()"	pg_is_in_recovery --- f
b)	Check Master postgres using DB-VIP	sudo -u postgres psql -h <DB-VIP> -p 5432 -c "SELECT pg_is_in_recovery()"	pg_is_in_recovery --- f
c)	Check the Slave postgres	sudo -u postgres psql -h <standby> -p 5432 -c "SELECT pg_is_in_recovery()"	pg_is_in_recovery --- t

   ii. Verify if replication is happening to the DR cluster master from the Primary cluster master.

> **Note:** Replication from the DR cluster master to the DR cluster slave is stopped in this mode. Once the DR site is enabled as the primary site, replication starts from the master to the slave.

Switch Service Manager Service Portal to your Disaster Recovery cluster

1. Make sure that all nodes on the Primary cluster are down.
2. Rerun Ansible playbook script db.yml from the `/opt/hp/propel/contrib/propel-distributed.<version>` directory on the DR cluster LB node:

```
# ansible-playbook db.yml -c paramiko --ask-become-pass -u propel 2>&1 | tee recovery.out
```

3. Verify the configuration:
   a. On the DR cluster, make sure both DB nodes are on standby:

	Step	Command	Output
a)	Check the Master postgres	sudo -u postgres psql -h <primary> -p 5432 -c "SELECT pg_is_in_recovery()"	pg_is_in_recovery ---------- f
b)	Check Master postgres using DB-VIP	sudo -u postgres psql -h <DB-VIP> -p 5432 -c "SELECT pg_is_in_recovery()"	pg_is_in_recovery ---------- f
c)	Check the Slave postgres	sudo -u postgres psql -h <standby> -p 5432 -c "SELECT pg_is_in_recovery()"	pg_is_in_recovery ---------- t

   b. Check if replication is happening to the DR cluster slave.
   c. Check pgpool (show pool_nodes) :

      From the primary db of the DR cluster, confirm pgpool has attached to both the primary and standby servers:

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"

node_id | hostname | port | status | lb_weight | role
------------+-----------+------+-----+------------+----------
0 | <primary> | 5432 | 2 | 0.500000 | primary
1 | <standby> | 5432 | 2 | 0.500000 | standby
```

      The “role” column should contain the appropriate primary/standy value and the status column should be “2” for both nodes.

4. Start the Service Manager Service Portal nodes and restart Nginx on the DR cluster.
5. Log in to the DR user interface and check whether the data created on the Primary site is present on the DR.

Troubleshoot distributed Service Manager Service Portal clustering

This section provides troubleshooting hints and tips that can help you set up a Distributed Service Manager Service Portal Cluster.

NGINX 504 Gateway Time-out

When this error occurs, do the following:

1. Check if pgpool is running and listening:

   ```
   # systemctl status pgpool
   # sudo -u postgres psql -h <DB VIP> -p 9999 –l
   ```

2. Check if IdM on node1/2 can connect to the DB (see logs in /var/log/propel/idm). If not, restart the Launchpad and IdM. If they can connect to the DB, try the LB connection again. If that works, restart all other services on alService Manager Service Portal nodes. Test again the LB connection.

Pgpool not starting

Make sure that version 3.4.7 is installed (see the following figure for an example). This is the version that HPE validated with in the Distributed Service Manager Service Portal configuration.

You can update the propel-distributed/roles/pgpool/tasks/main.yml for the pgpool role to force to install a specific version:

```
name: roles:pgpool Install older pgPool
yum: name=http://www.pgpool.net/yum/rpms/3.4/redhat/rhel-7-x86_64/pgpool-II-pg94-
3.4.7-
1pgdg.rhel7.x86_64.rpm state=installed
ignore_errors: yes
```

Pgpool not attaching to nodes

When both databases are running, the “show pool_nodes” query should show a status of “2” for both nodes.

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"
node_id | hostname | port | status | lb_weight | role
---------+----------+------+--------+-----------+---------
0 | <PRIMARY> | 5432 | 2 | 0.500000 | primary
1 | <STANDBY> | 5432 | 3 | 0.500000 | standby
```

To obtain the expected result, try the following:

1. On the primary server, restart pgpool:

   ```
   # service pgpool restart
   ```

   On the standby server, restart pgpool:

   ```
   # service pgpool restart
   ```

   Check the result:

   ```
   # sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"
   ```

2. If the status is still incorrect, perform the following steps:

   On the standby server, stop pgpool:

   ```
   # service pgpool stop
   ```

   On the primary server, stop pgpool:

   ```
   # service pgpool stop
   ```

   On the primary server, confirm eth0:0 is down:

   ```
   # ifdown eth0:0
   ```

   On the primary server, verify that pgpool exited gracefully:

   ```
   # rm –i /tmp/.s.PGSQL.9898
   # rm –i /var/run/postgresql/.s.PGSQL.9999
   ```

   On the primary server, restart pgpool:

   ```
   # service pgpool start
   ```

Check the result:

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"
```

If the status is “2” for both nodes, restart pgpool on the standby server:

```
# service pgpool start
```

3. If the status is still incorrect, perform the following steps:

   On the standby server, stop pgpool:

   ```
   # service pgpool stop
   ```

   Confirm the status of primary server. The result should be “f”:

   ```
   # sudo -u postgres psql -h <Primary> -p 5432 -c 'select pg_is_in_recovery()'
   pg_is_in_recovery
   -------------------
   f
   (1 row)
   ```

   Confirm the status of the standby server. The result should be “t”:

   ```
   # sudo -u postgres psql -h <Standby> -p 5432 -c 'select pg_is_in_recovery()'
   pg_is_in_recovery
   -------------------
   t
   (1 row)
   ```

   If these are incorrect, the issue is more likely with the configuration of PostgreSQL. Otherwise, perform these steps:

   On the primary server, run these commands using the node_id that reports a status of “3”:

   ```
   # /usr/pgpool-9.4/bin/pcp_detach_node -U pgpool -h localhost -p 9898 -W -n
   <node_id>
   Password:
   # /usr/pgpool-9.4/bin/pcp_attach_node -U pgpool -h localhost -p 9898 -W -n
   <node_id>
   Password:
   # /usr/pgpool-9.4/bin/pcp_detach_node -U pgpool -h localhost -p 9898 -W -n
   <node_id>
   ```

   By default, the password is **pgpool**.

Wait 60 seconds and then check the result:

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"
```

PostgreSQL queries on VIP fail

When one or both databases are up and pgpool is running, this error should not occur:

```
# sudo -u postgres psql -h <DB-VIP>-p 9999 -c 'SELECT now()'
psql: server closed the connection unexpectedly
This probably means the server terminated
```

To fix the issue, follow the same steps in "Pgpool not attaching to nodes" on page 167.

“show pool_nodes” shows both databases

When one or both databases are up and pgpool is running, this error should not occur:

```
# sudo -u postgres psql -h <DB-VIP> -p 9999 -c "show pool_nodes"
node_id | hostname | port | status | lb_weight | role
---------+------------+------+--------+-----------+---------
0 | <PRIMARY> | 5432 | 2 | 0.500000 | standby
1 | <STANDBY> | 5432 | 2 | 0.500000 | standby
```

To fix the issue, follow the same steps in "Pgpool not attaching to nodes" on page 167.

Load Balancer node information

nginx logs : /var/log/nginx

nginx conf : /etc/nginx/conf.d/virtual.conf

Command to restart nginx: service nginx restart

Database node information

The following section contains information about a DB node.

How to change postgreSQL to listen to all interfaces

1. Edit the pg_hba.conf file:

   ```
   # su – postgres
   # vi /var/lib/pgsql/9.5/data/pg_hba.conf
   ```

   host all all 0.0.0.0/0 trust

2. Edit the postgresql.conf file:

   ```
   # vi /var/lib/pgsql/9.5/data/postgresql.conf
   ```

   listen_address = '*'

3. Restart PostgreSQL:

   ```
   # service postgresql-9.5 restart
   ```

DB Log locations:

/var/lib/pgsql/9.5/data/pg_log

DB restart:

```
# service postgresql-9.5 restart
```

DB not responding:

If PostgreSQL runs out of space and does not respond:

http://blog.endpoint.com/2014/09/pgxlog-disk-space-problem-on-postgres.html

RabbitMQ commands

The following section provides some useful commands for RabbitMQ.

Broker status

rabbitmqctl status

SX: config for MQ

/opt/hp/propel/sx/WEB-INF/classes/config/infrastructure.json

Check if rabbitmq is running correctly

- 5671 is used by rabbit broker:

  # netstat -an | grep 5671

- 25672 is used by rabbit to manage clustering:

  # netstat -an | grep 25672

RabbitMQ failed to start on a node

BOOT FAILED - Timeout contacting cluster nodes: [rabbit@awha22p4].

BACKGROUND -This cluster node was shut down while other nodes were still running.

To avoid losing data, you should start the other nodes first, then start this one. To force this node to start, first invoke "rabbitmqctl force_boot". If you do so, any changes made on other cluster nodes after this one was shut down may be lost.

DIAGNOSTICS - attempted to contact: [rabbit@awha22p4]

If you see the type of error described above, run the following commands:

```
# rabbitmqctl force_boot
# rabbitmqctl start_app
```

Install Service Request Catalog (SRC)

SRC is an end user portal that provides end users with an online shopping experience. SRC enables end users to submit support requests, order catalog items, search knowledge, and take surveys.

To install SRC, you only need to deploy a WAR achieve on Tomcat.

For detailed instructions, see the *SRC Interactive Installation Guide*, which you can access from the **Install** information node of the Service Manager Help Center.

For information about how to customize SRC, see the *Service Request Catalog Customization Guide*, which you can access from the **Administer** information node of the Service Manager Help Center.

Install the Mobile Applications client

The field engineers are typically tasked to work with business users at a customer site, and they spend most of their time away from the office to resolve tickets. When Change Approvers are away from the office, they need a way to quickly approve or deny changes, so that pending work orders can be assigned. Service ManagerMobile Applications connect your company's people and information by providing your team access to the Change Management, Incident Management, and Service Desk applications through the use of smartphones. When these IT operators are away from the office, they can receive and view work assignments and perform the tasks below by using the Mobile Applications:

- Approve and deny change requests.
- Approve and deny interaction.
- Reassign incidents/changes to the proper support group.
- Search the knowledge base.
- Open a support ticket.
- Continue working on-site with customers.

These quick responses improve business metrics, as service level objectives are met.

This section provides instructions on how to install the Mobile Applications client (also referred to as the Mobility Client).

Introduction

The field engineers are typically tasked to work with business users at a customer site, and they spend most of their time away from the office to resolve tickets. When Change Approvers are away from the office, they need a way to quickly approve or deny changes, so that pending work orders can be assigned. Service Manager Mobile Applications connect your company's people and information by providing your team access to the Change Management, Incident Management, and Service Desk applications through the use of smartphones. When these IT operators are away from the office, they can receive and view work assignments and perform the tasks below by using the Mobile Applications:

- Approve and deny change requests.
- Approve and deny interaction.
- Reassign incidents/changes to the proper support group.
- Search the knowledge base.
- Open a support ticket.
- Continue working on-site with customers.

These quick responses improve business metrics, as service level objectives are met.

System administration

This chapter provides details about how to install, implement and tailor Service Manager Mobile Applications to support your business processes.

This chapter includes:

Installing Service Manager Mobile Applications

This section provides details about how to install Service Manager Mobile Applications to support your business processes.

This section includes:

Before you start

As the System Administrator, you must:

- Have already installed HPE Service Manager 9.34 or later on a web accessible location. For installation information, see the *HPE Service Manager Installation Guide* and the *HPE Service Manager 9.50 Release Notes*.

  > **Note:** For the Mobile Applications client, only the Service Manager 9.34 server and later versions are supported.

- Your web application server meets the requirements that are described in the Service Manager compatibility matrix. For details, refer to the *Service Manager Support Matrix* at HPE Support Matrices.
- Configure the JVM memory settings on the web application server as below:
  - Minimal setting: `-Xms:1024m, -Xmx:1024m, -XX:PermSize=256m`
  - Recommended setting: `-Xms:1500m, -Xmx:1500m`
- Set `JAVA_HOME` to the location where the JDK was installed (for Tomcat only), or enable the profiles to use the version 7.0 SDK (for WAS 8.5.5 only).

  For example, use the following command on a 32-bit operation system:

  managesdk -enableProfileAll -sdkname 1.7_32 -enableServers
- Review the browser requirements for smartphones.
- Set up your Mobile Applications preferences.
- Configure Service Manager.

Install Service Manager Mobile Applications

When you have finished preparing for your installation (see "Before you start" on the previous page), you can perform the following tasks to install Service Manager Mobile Applications.

1. "Edit the configuration file in the war archive" below.
2. "Install Service Manager Mobile Applications" on the next page.

Edit the configuration file in the war archive

To edit web.properties in webapp-9.50.xxxx.war, follow these steps:

1. Open webapp-9.50.xxxx.war in an archive management program.
2. Extract the web.properties file from the WEB-INF directory to your local system, and then open this file in a text editor.
3. Set the Service Manager server and port parameters as follow to add your server connection information:

Required parameters for Service Manager Mobile Applications client connection

Parameter	Default value	Description
endpoint	`http://localhost:13080/SM/ui`	Change `localhost:13080` to your Service Manager server host name and port number.
resourceRoot	None	This parameter is commented-out by default. You need to update this value only when the *.js image files and the *.css files are stored on another server. For example, if you moved the static files to another Apache server, change this value to `resourceRoot=http://<host name of another Apache server>:8080/mobile/statics/`.

Tip:

- Optionally, you can also define the number of records that appear in every page of the List View by configuring the value in the *recordlistcount* parameter.
- If FIPS (Federal Information Processing Standards) mode is enabled on the Service Manager side, you need to enable FIPS mode in the Mobility client. For details, see the following topics of the *Service Manager Help Center*:
  - *Configure LW-SSO in the Mobility Client for FIPS mode*
  - *Configure FIPS mode in the Mobility Client*

4. Save the file and add the updated file back to the WEB-INF directory of the webapp-9.50.xxxx.war archive.

Install Service Manager Mobile Applications

The Service Manager Mobile Applications contains a J2EE-compliant web application that runs on your web application server. Each web application server has its own method of deploying web applications. See your web application server documentation for specific instructions on deploying a web application.

Note: For the specific versions of the application servers that are currently supported by the Service Manager Mobile Applications client, refer to the *Service Manager Support Matrix* at HPE Support Matrices.

The following table provides a summary of deployment methods required.

Web application server	Deployment method
Apache Tomcat	Copy the webapp-9.50.xxxx.war file to the <Tomcat>\webapps folder and start the web application server.
IBM Web Application Server	Open the administration console and install the web application from the webapp-9.50.xxxx.war file.

Note: If you are working with Service Manager 9.34 or later 9.3x versions and are planning to upgrade both platform and applications to version 9.50, the Mobile Applications will be upgraded to the latest version which supports both power user view and self-service user view.

Tailoring Mobile Applications in Service Manager

When you have finished installing Mobile Applications, you can tailor the following in HPE Service Manager:

Set up email notifications to include URL links

The HPE Service Manager System Administrator can set up email notifications to include the mobility URL so that when tickets are assigned, field engineers can receive email notifications and click on the URL links in the emails to go directly to the assigned ticket.

Service Manager Mobile Applications automatically synchronizes users' mobile data with information in the Service Manager database. When an email notification is sent to a field engineer, Service Manager Mobile Applications searches for the record by name and then displays it. If the record is not in the cached database, Service Manager will be queried to fetch the record.

To set up email notifications, follow these steps:

1. Restart the Service Manager Mobile Applications server.
2. Log on to the Service Manager server as a System Administrator.
3. Click **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
4. Select the **Active Integrations** tab.
5. In the **Mobility URL** field, type the fully-qualified URL to the Service Manager server from the Mobile Applications client.

   For example: `http://<servername>:<portnumber>/<appname>/std/`

   Where:

   `servername` is the host name or IP address of the Service Manager server.

   `portnumber` is the port number. For example, `8080`.

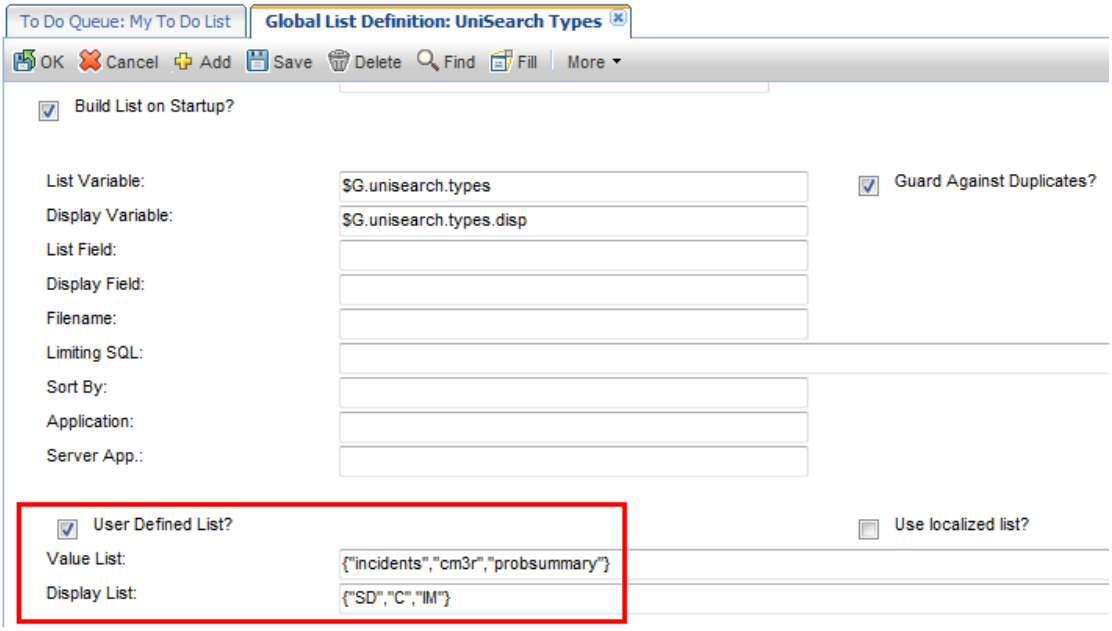
   `appname` is the name of the deployed Service Manager Mobile Applications client WAR/EAR file. For example, `webapp-9.50.xxxx.war`.

   The server stores the value of this field in the `$L.mobility.url` global variable.
6. Save your changes.

Configure the prefix of a record

To configure the prefix of an incident record or a change request which already has a prefix, follow these steps:

1. Log on to the HPE Service Manager server as a System Administrator.
2. Type `gl` in the Service Manager command line field, and then press **Enter**.
3. Type `UniSearch Types` in the **List Name** field, and then click **Search**.
4. Verify and configure the values in the **Value List** field and the **Display List** field. Refer to the following screenshot as an example:

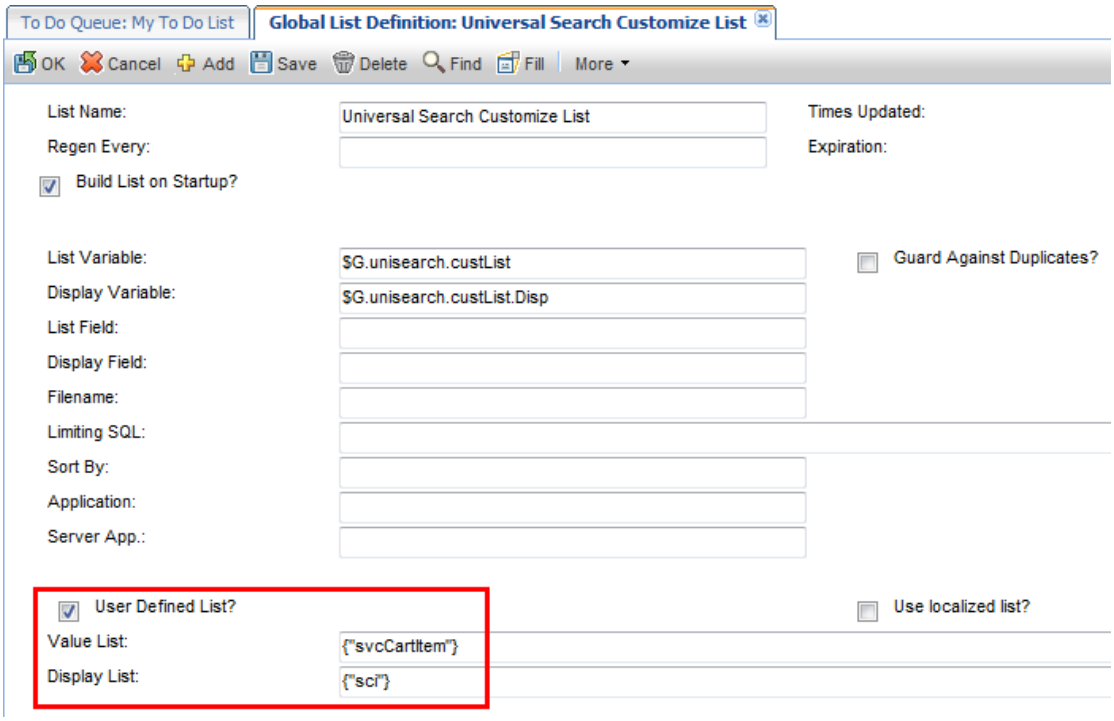


5. Click **Save**, and then click **OK**.

To configure the prefix of an incident record or a change request which does not have a prefix, follow these steps:

1. Log on to the Service Manager server as a System Administrator.
2. Type `gl` in the Service Manager command line field, and then press **Enter**.
3. Type `Universal Search Customize List` in the **List Name** field, and then click **Search**.
4. Add customized record type to the **Value List** field and then add the corresponding prefix to the **Display List**.

   Refer to the following screenshot as an example:



The out-of-the-box record is `svcCartItem` with the prefix `sci`. When you search for `sci1`, the svcCartItem record with the ID of 1 is displayed in the List view.

5. Click **Save**, and then click **OK**.

Add a view for Mobile Applications

Service Manager Mobile Applications provides several out-of-box views to access individual and group records. For example, the default views of Incidents are **My Group's Incidents** and **My Incidents**. As the system administrator, you can create more views for one or more users to customize the default log-on view. For example, if a group of users regularly searches on the same query, you can provide them with a shared query view as their default whenever they log on to Service Manager from the Mobile Applications client.

To display an existing view in the Mobile Applications client, follow these steps:

1. Log on to HPE Service Manager using the Windows client as a System Administrator.
2. From the System Navigator, click **Favorites and Dashboards**.
3. Right-click the favorite that you want to edit, and then select **Properties**. The View Definition form opens.

4. Select the **Mobile Accessible** check box.
5. In the **Audience** tab, update the audience which are exposed to the view and then click **Save**.

> **Tip:** You may need to configure the access to browse for certain views:
>
> 1. From the System Navigator, click **System Administration** > **Base System Configuration** > **Miscellaneous** > **View/Favorites**.
> 2. Select the view and click the **Audience** tab.
> 3. Select **Selected Groups** and update the Groups list.

To create a new view for the Mobile Applications client, follow these steps:

1. Log on to Service Manager using the Windows client as a System Administrator.
2. Click **System Administration** > **Base System Configuration** > **Miscellaneous** > **Views/Favorites**.
3. Click **New**. The New View wizard opens.
4. Select the Area to create the view in and then click **Next**.
5. Specify the name and type for the view you wish to create, and then click **Next**.
6. Select the fields you want in your view:
   a. Click **Fields**.
   b. To add fields, select items from the table menu and click **Add to List**.

      > **Note:** If you select a field that has a link to another table, select from the secondary menu to add fields you want in the view.
7. Select properties for Group By, Sort By, Filter, and Autoformat as desired.
8. Click **Finish**.
9. Select the **Mobile Accessible** check box.
10. In the **Audience** tab, select an audience for the view and then click **Save**.
11. Open the To Do Queue, select the area in the Queue field as you defined in *step 4* and check which form is used by the new view.
12. Open Form Designer and search for the form.
13. Click **More Actions** > **Copy/Rename** to copy the form with a mobile suffix.

> **Note:** When copying the forms, do not omit the .g suffix which is used by some forms. For example, you can copy sc.manage.cmr.g to sc.manage.cmr.g.mobile.

To remove a view from the Mobile Applications client, follow these steps:

1. Follow *step 1* to *step 3* as described in "To display an existing view in the Mobile Applications client, follow these steps:".
2. In the **Audience** tab, update the audience which are to be excluded from the view; or you can clear the **Mobile Accessible** check box to remove the view from Mobile Applications.
3. Click **Save**.

Add a form for Mobile Applications

After you added a new view which enables you to navigate through lists of records, you need to add forms for these records in the List view.

To add a form for the Mobile Applications, follow these steps:

1. Log on to HPE Service Manager using the Windows client as a System Administrator.
2. Select the area in the **Queue** field as you defined in *step 4* of "To create a new view for the Mobile Applications client, follow these steps:" on the previous page.
3. Select the view you created in the **View** field.
4. Open a record and check which form is used by the record .
5. Click **Tailoring** > **Forms Designer** and search for the form.
6. Click **More Actions** > **Copy/Rename** to copy the form with a mobile suffix. For example, you can copy IM.close.incident to IM.close.incident.mobile.

> **Note:** The form used by a record may vary with different status or phases of that record. You need to add a form for each status or phase respectively. For example, the form associates with an Incident can be either IM.close.incident or IM.update.incident. If you have made any omissions, the Mobile Applications client will automatically synchronize data with the original form in the Service Manager database after you logged on to the system.

Customize the fields on Mobile Applications form

For a better appearance of a record's Detail view on the screen of your smartphone, you may need to add, rearrange or remove the fields on a Mobile Applications form.

For detailed information about the widgets on HPE Service Manager Mobile Applications forms, see "Appendix A: Mobile Applications Form Widgets" on page 217.

To customize the fields on a Mobile Applications form, follow these steps:

1. Follow *step 1* to *step 4* as described in "Add a form for Mobile Applications" on the previous page.
2. Click **Tailoring** > **Forms Designer** and search for the form with the .mobile suffix.
3. Click **Design** to open design mode.
4. Remove the fields which are not exposed to be displayed on the form. The field groups will be displayed as corresponding tabs in the Detail view on Mobile Applications client.

   > **Note:**
   > - Do not nest field groups.
   > - For usability and performance issues, do not include more than ten fields in a group.
   > - If there is one field group defined on a form at a minimum, the widgets which are not included in this group will not be displayed on a Mobile Applications form.

5. Specify the **Label for** property of every lable to match with the **Name** property of the widget next to it.

   Take the IM.close.incident.mobile form for example. If the **Name** property of the Incident ID text box is `id`, the **Label for** property of the Incident ID lable must be specified to `id`.

6. Before adding a field, make sure the field exists in the Database Dictionary.Otherwise, you must firstly add this new field to the Database Dictionary. See *Service ManagerService Manager Help Center* > *Tailoring* > *Data management* > *Fields and Keys tab* > *Add a field to a table* for detailed steps.
7. Click **OK** to save your customization.

Customize the action bar options

To customize the action bar options on the Mobile Applications client, follow these steps:

1. Log on to HPE Service Manager using the Windows client as a System Administrator.
2. Select the area in the **Queue** field as you defined in *step 4* of "To create a new view for the Mobile Applications client, follow these steps:" on page 182.
3. Open a record and check which display screen is used by the record . For example, cm.view.display.
4. From the System Navigator, click **Tailoring** > **Tailoring Tools** > **Display Screens** and search for the display screen.
5. Click **Show in Mobility**.
6. Select the area in the **File Name** field.
7. Select **Mobile** in the **Client Type** field, and then click **Search**. IDs of the action bar options are displayed in the **Button Ids** field.
8. Refer to the option IDs and the actions listed in the **Options** tab, add or remove the IDs.
9. Click **Save** to save your customization.

Configure the maxRequestPerSecond parameter

The *maxRequestPerSecond* parameter in the HPE Service Manager Mobile Applications configuration file (web.xml) defines the maximum allowed request per second for one user session from the Service Manager Mobile Applications client. The default value for this parameter is 10. To allow unlimited requests, set the value to -1.

Localize Service Manager Mobile Applications

The officially supported languages of Service Manager can meet most localization requirements. However, if you need to localize Mobile Applications to support additional languages, follow these steps:

1. Service Manager configurations.
   a. Refer to the Service Manager Open Localization Toolkit Documentation in the Service Manager Document Matrix to localize the Service Manager server (including messages and formats) to the new language.

b. Refer to "Add a form for Mobile Applications" on page 183 to add new forms for Mobile Applications.

2. Service Manager Mobile Applications configurations.

   a. Copy <mobile web application directory>\WEB-INF\classes\appLoginBundle.properties and save this file as <mobile web application directory>\WEB-INF\classes\appLoginBundle_<Service Manager language ID>.properties.

      Tip: Refer to the Service Manager language table for a list of language IDs. For example, if the new language is Malay, change appLoginBundle_<Service Manage Language ID>.properties to appLoginBundle_z3.properties.

   b. Translate each text string in appLoginBundle_<Service Manager language ID>.properties to the new language and then save this file.

   c. Using native2ascii or other tools to convert appLoginBundle_<Service Manager language ID>.properties to one with ASCII and/or Unicode escapes.

      Tip: For detailed usage of native2ascii, refer to the following Oracle web page: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/native2ascii.html

   d. Copy <mobile web application directory>\WEB-INF\classes\appMainBundle.properties and save this file as <mobile web application directory>\WEB-INF\classes\appMainBundle_<Service Manager language ID>.properties.

   e. Translate each text string in appMainBundle_<Service Manager language ID>.properties to the new language and then save this file.

   f. Using native2ascii or other tools to convert appMainBundle_<Service Manager language ID>.properties to one with ASCII and/or Unicode escapes.

   g. Restart the web applications server and launch Service Manager Mobile Applications again.

Customizing the Service Manager Mobile Applications CSS

To customize the HPE Service Manager Mobile Applications CSS, perform the following tasks:

1. "Update LESS files" on the next page
2. "Test Customized LESS files" on page 188

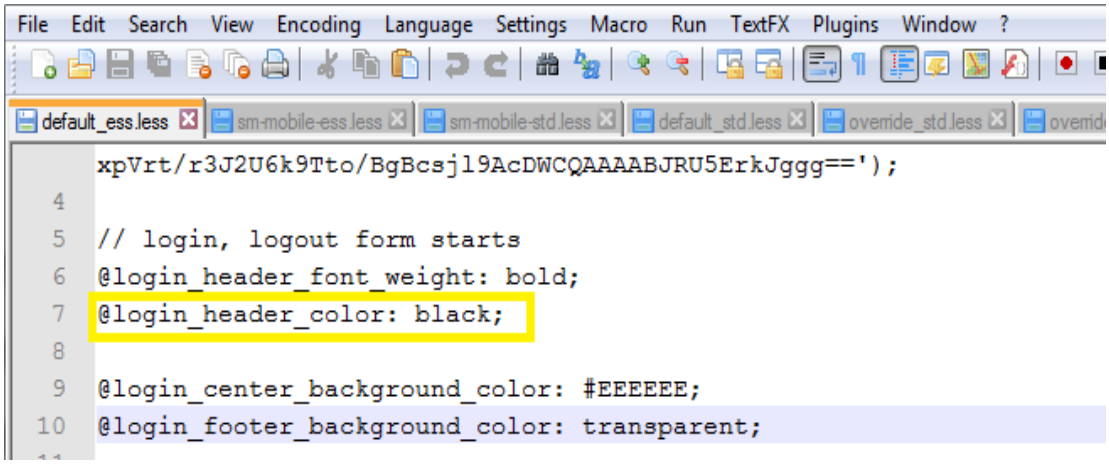
3. "Generate CSS files manually" on the next page
4. "Generate CSS files by Koala" on page 189
5. "Test generated CSS files" on page 191

Update LESS files

LESS extends CSS with dynamic behavior such as variables, mixins, operations and functions. Service Manager Mobile Applications is using LESS to simplify CSS customization and maintenance. For more information about LESS, visit the LESS official website.

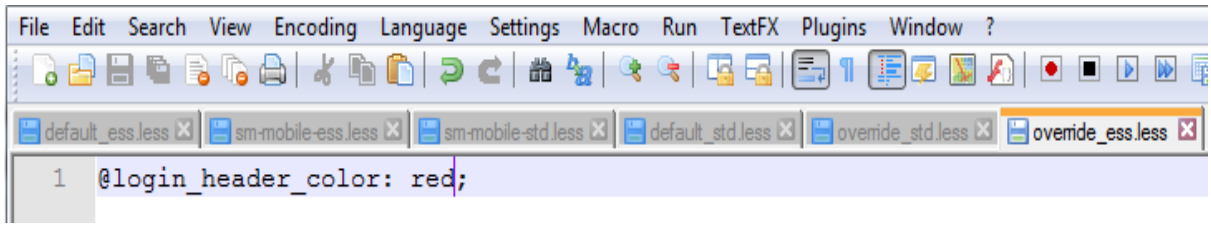
The styles of Mobile Applications web elements which can be customized are defined in default_ess.less and default_std.less in the <Tomcat installation directory>\webapps\<appname>\app\resources\css directory.

Refer to the following screenshot as an example.The text color of the default login header is defined by `@login_header_color`.



The styles can be overridden by the same variables defined in override_ess.less and override_std.less in the <Tomcat installation directory>\webapps\<appname>\app\resources\css directory.

To override the default value, you need to copy the variable from default_ess.less, paste it to override_ess.less, and then specify a new value for it.



> **Note:** Except for override_ess.less and override_std.less, the *.less files in the \app\resources\css directory should not be modified directly because these files might be overwritten during software upgrade.

Test Customized LESS files

To test the customized LESS files, follow these steps:

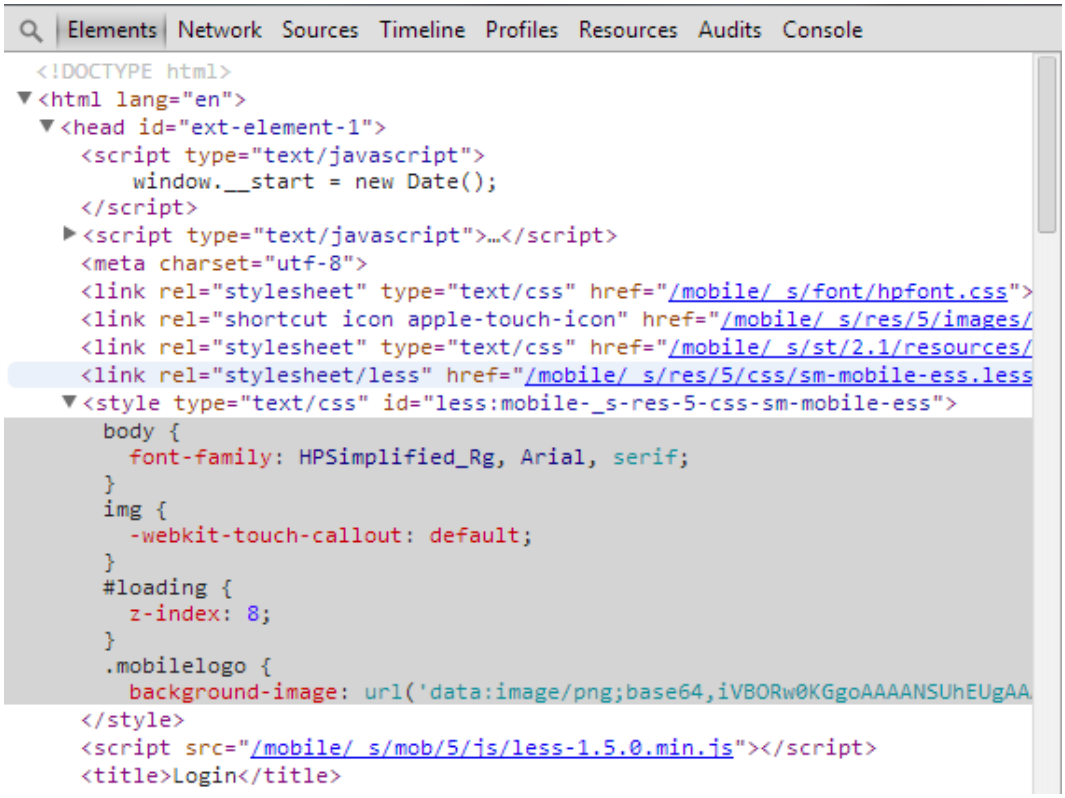
1. Browse to the <Tomcat installation directory>\webapps\<appname>\WEB-INF\classes\META-INF directory and open the app.properties file with a text editor.
2. Update `debug=false` to `debug=true`, save the file and restart Tomcat.
3. Refer to "Launching Service Manager Mobile Applications on your smartphone" on page 203 and launch the Mobile Applications employee self-service mode.
4. Check the styles are displayed as customized.
5. Refer to either "Generate CSS files manually" or "Generate CSS files by Koala" to generate CSS files according to your customized LESS files.

Generate CSS files manually

To generate CSS files manually, follow these steps:

1. Refer to "Launching Service Manager Mobile Applications on your smartphone" on page 203 and launch the Mobile Applications employee self-service mode.
2. In the **Elements** tab, search for `less:mobile-_s-res-5-css-sm-mobile-ess`.

   Refer to the following screenshot as an example:

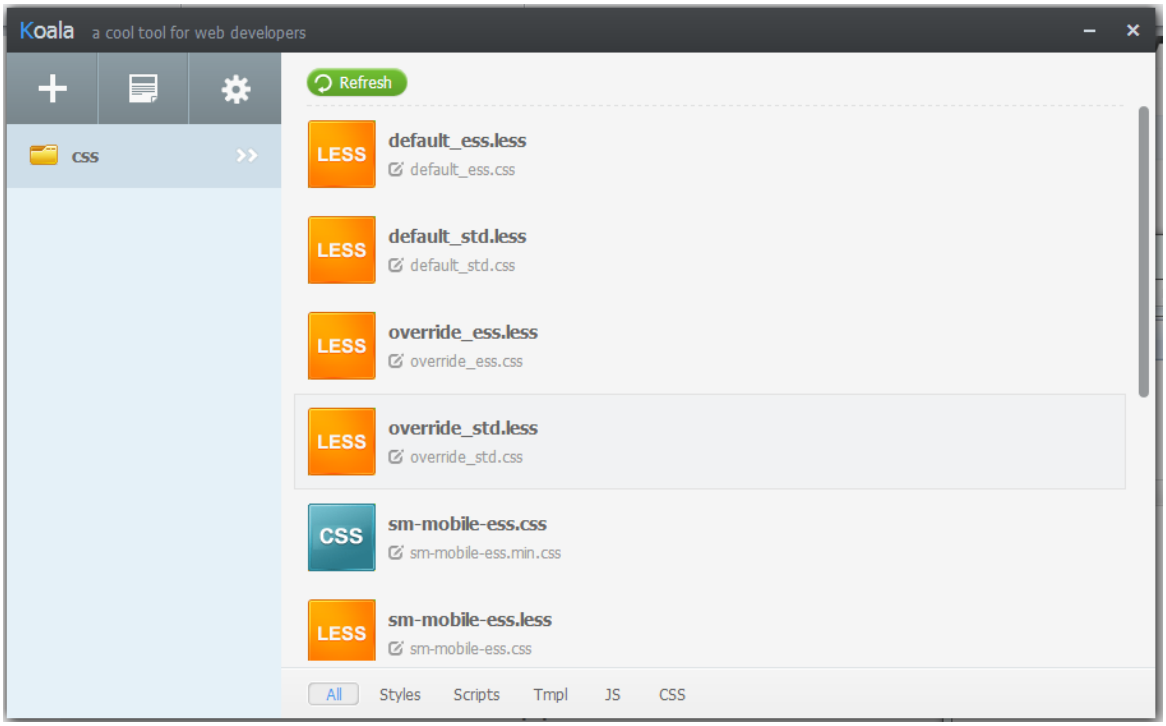


3. Copy the codes between `<style type="text/css" id="less:mobile-_s-res-5-css-sm-mobile-ess">` and `</style>`.
4. Browse to the <Tomcat installation directory>\webapps\<appname>\app\resources\css directory, replace the content of `sm-mobile-ess.css` with the codes copied in the previous step.
5. Save the CSS file.
6. Type `http(s)://<hostname>:<port>/<appname>/std/` in the Chrome address bar and then press **Enter** to launch the Mobile Applications standard mode.
7. In the **Elements** tab, search for `less:mobile-_s-res-5-css-sm-mobile-std`.
8. Continue to follow *step 3* through *step 5* to update the CSS file in the standard mode.

Generate CSS files by Koala

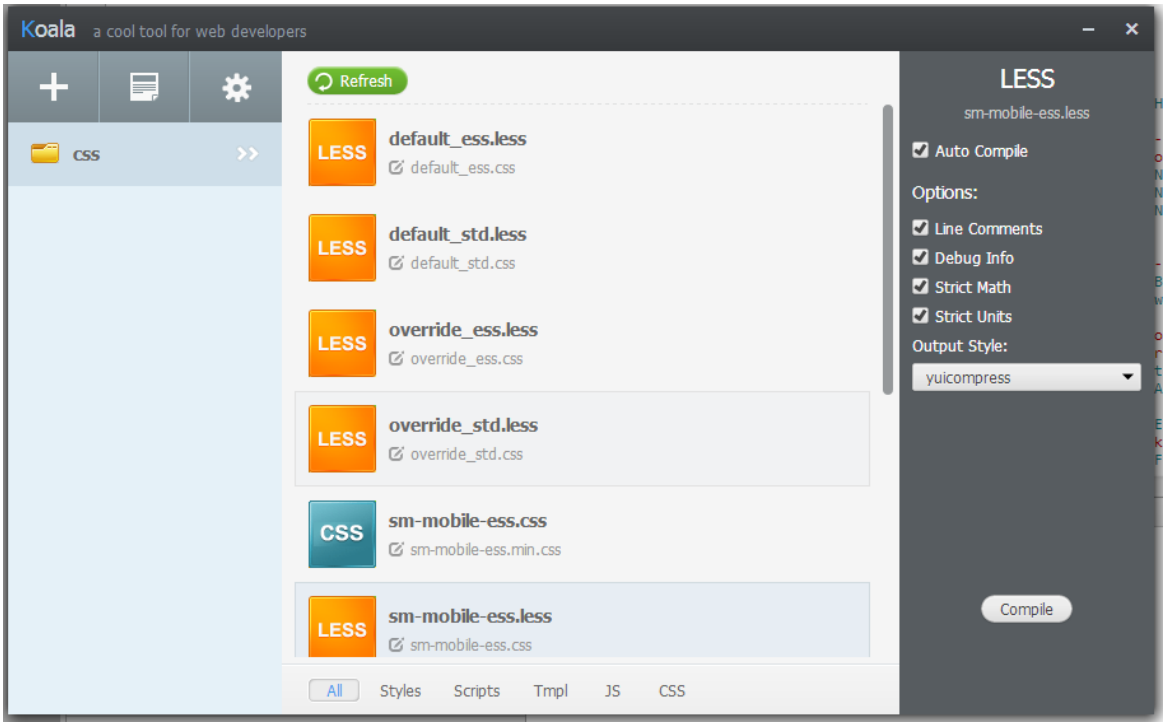
To generate CSS files by Koala, follow these steps:

1. Download Koala from http://koala-app.com and install this software on your computer.
2. Browse to the <Tomcat installation directory>\webapps\<appname>\app\resources\css directory and add the LESS folder to Koala by either drag-and-drop or click the **+** button in Koala UI.



3. After overwrite the variables in override_ess.less, use Koala to generate the CSS file.

   Click sm-mobile-ess.less, a panel will be displayed on the right. Click the **Compile** button to generate a CSS file with the name of sm-mobile-ess.css.

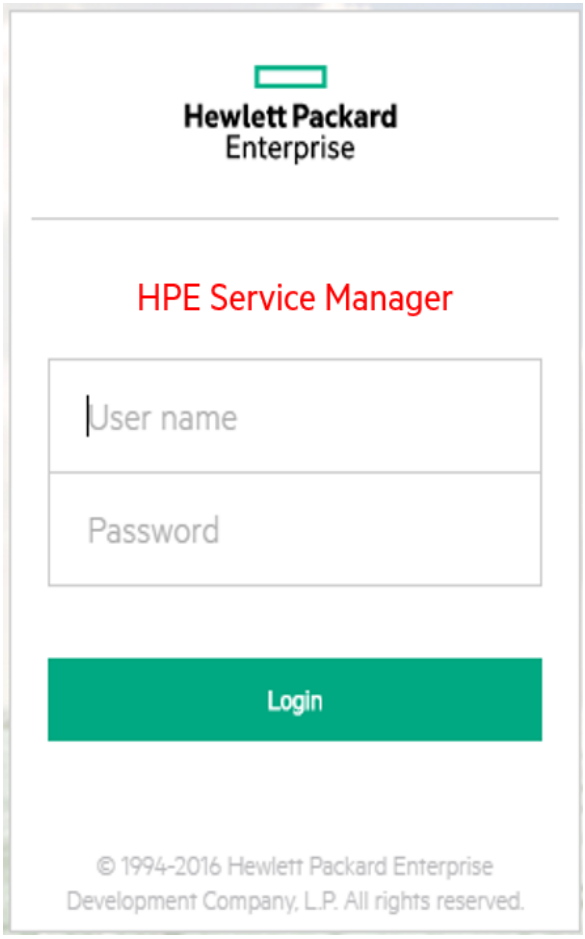


Test generated CSS files

To test the generates CSS files, follow these steps:

1. Browse to the <Tomcat installation directory>\webapps\<appname>\WEB-INF\classes\META-INF directory and open app.properties with a text editor.
2. Change debug mode to `false`.
3. Save and close this file.
4. Restart Tomcat and test Mobile Applications for both standard mode and employee self-service mode.

   For example, after overwrite the text color of login header from black to red, your login screen is displayed as follow:



If you customization is not correctly displayed, clear the browser cache and refresh the browser window.

Protecting communications between Mobile Applications and the Service Manager server

To protect communications between Mobile Applications and the HPE Service Manager server, you can perform the following tasks:

- "Set up Secure Sockets Layer (SSL)" on the next page
- "Set up trusted sign-on (TSO)" on page 197
- "Set up Lightweight Single Sign-On (LW-SSO)" on page 199

Set up Secure Sockets Layer (SSL)

HPE Service Manager supports Secure Hypertext Transfer Protocol (HTTPS), which encrypts and decrypts message requests and responses. Service Manager uses Secure Sockets Layer (SSL) for encryption only and relies on the server to authenticate each operator's user name and password. Service Manager supports SSL for the following connections:

- SSL on the Service Manager server to encrypt all communications between clients and the server
- SSL on the Mobile Applications client to verify the client's identity and limit server connections to these identified clients

For detailed information about how to enable SSL and SSO in Service Manager, refer to the *HPE Service Manager Help Center* and the *Setting up Single Sign-on in Service Manager* knowledge article.

Enable SSL on the Service Manager server

Service Manager clients send the operator's user name and password in each request as part of an HTTP Basic Authorization header. In order to protect these operators' user names and passwords, you can enable SSL on the Service Manager server.

Enabling SSL on the Service Manager server includes three major steps:

1. Purchase a certificate for the Service Manager server from a certificate authority, or create a certificate by yourself.
2. Create a server keystore. For detailed steps, refer to the Setting up Single Sign-on in Service Manager knowledge article.
3. Add SSL parameters to the sm.ini file.

> **Note:** Ignore the SSO parameters in the table at this point.

Enable SSL on the Mobile Applications client

In order to restrict access to the server to only clients that are known and identified by the server, you can enable SSL on Service Manager clients. Enabling SSL on clients requires creating or purchasing signed certificates for each Service Manager client. Service Manager Mobile Applications can share a

single signed certificate for all handset connections. If you enable SSL on the client, we recommend that you also enable SSL on the server to encrypt all communications between clients and the server.

To enable SSL on the Mobile Applications client, follow these steps:

1. Purchase a certificate for the Mobile Applications client host from the same certificate authority for the Service Manager server certificate, or create a certificate by yourself.
2. Create a client keystore. For detailed steps, refer to the Setting up Single Sign-on in Service Manager knowledge article.
3. Import the client certificate to a trusted clients keystore. For example, trustedclients.keystore.
4. Copy the trusted clients keystore (trustedclients.keystore) to the Service Manager server's RUN folder.
5. Open webapp-9.50.xxxx.war in an archive management program.
6. Copy the cacerts file to the WEB-INF directory.
7. Extract the web.properties file from the WEB-INF directory to your local system, and then open this file in a text editor.
8. Locate the following codes and configure the parameters as follow:

```
endpoint=https://full.qualified.domain.name:13443/SM/ui

cacerts=
keystore=
keystorePassword=
```

Required parameters for Mobile Applications client SSL configurations

Parameter	Default value	Description
endpoint	`https://full.qualified.domain.name:13443/SM/ui`	Change `full.qualified.domain.name` to the domain name of your Service Manager server. Change `13443` to your SSL port number.
cacerts	The default value is null.	Add the name of your cacerts file.
keystore	The default value is null.	Add the name of the keystore file.
keystorePassword	The default value is null.	Add the password of the

Required parameters for Mobile Applications client SSL configurations , continued

Parameter	Default value	Description
		keystore file. HPE recommends to add a strong password for the keystore. After you restart the Mobile Applications client, the keystore password is encrypted and the original `keystorePassword=` code is automatically updated to `*keystorePassword=<encrypted string>`. **Note:** The preceding asterisk (*) implies that the keystore password is encrypted. To change the password, remove the asterisk and replace the encrypted string with the new password.

9. Save the file and add the updated file back to the WEB-INF directory of the webapp-9.50.xxxx.war archive.
10. Restart the Service Manager Mobile Applications client.

Set up SSL between the smartphone browser and Mobile Applications

You can set up SSL to allow smartphone browsers and web servers to communicate over a secure connection. The data being sent is encrypted by one side, and decrypted by the other side before processing. This is a two-way process, meaning that both the server and the browser encrypt all traffic before sending out the data.

After SSL is set up on the web servers, browsers which support secure flag only send cookies with the secure flag when the request is going to an HTTPS page, that is, the browser does not send a cookie with the secure flag set over an unencrypted HTTP request.

You need to set up SSL on the web server or web application server where the Mobile Applications client is deployed, and update the port number mapping for the Mobile Applications client as necessary.

Set up SSL on you web server

For details, refer to the documentation of your web server.

> **Note:** It is recommended to enable HTTPOnly and Secure cookies on your web application server to help prevent malicious JavaScript injection and make the browser (or other http clients) only send cookies over SSL connections. For more information, see https://softwaresupport.hpe.com/km/KM02233778.

Set up SSL on Tomcat

Configuring Tomcat to use SSL is only necessary when Tomcat is run as a stand-alone web server. When Tomcat is primarily run as a Servlet/JSP container behind another web server, such as Apache or Microsoft IIS, it is necessary to configure the primary web server to handle the SSL connections from users. Typically, this server negotiates all SSL-related functionality, and then pass on any requests destined for the Tomcat container only after decrypting those requests. Likewise, Tomcat returns cleartext responses that are encrypted before being returned to the user's browser. In this case, Tomcat knows that communications between the primary web server and the client are taking place over a secure connection, but it does not participate in the encryption and decryption processes.

For information about how to set up SSL on Tomcat, refer to *Apache Tomcat SSL Configuration HOW-TO* document.

> **Note:** Since you have already got your certificates for the server as described in the previous step in the "Enable SSL on the Mobile Applications client" section, you only need to perform the steps in the **Edit the Tomcat Configuration File** section in Apache Tomcat SSL Configuration HOW-TO document.

Set up SSL on WebSphere 8.5.5

You can set the Secure flag within the WebSphere Application Server administrative interface. The **Restrict cookies to HTTPS Sessions** check box is available through the WebSphere Admin Console: **Application servers** > **[Your server]** > **Session management** > **Enable Cookies link**. For details, refer to the WebSphere 8.5.5 SSL configuration documentation.

Update the port number mapping for the Mobile Applications client

To update the port number mapping for the Mobile Applications client, follow these steps:

1. Go to Tomcat webapps directory of Mobile Applications.
2. Open WEB-INF\spring\security.xml with a text editor.

3. Locate the following codes, and then update the default security ports as necessary.

```
<security:http auto-config='true'>
        <security:port-mappings>
            <security:port-mapping http="8080" https="8443"/>
        </security:port-mappings>
        <security:intercept-url pattern="/**"  requires-channel="https"/>
 </security:http>
```

> **Note:** Remember to update the port number to the same as the configuration in your web server or web application server.

4. Save the changes.

Set up trusted sign-on (TSO)

Trusted sign-on (TSO) or Single sign-on is an optional Mobile Applications configuration that relies on a working SSL configuration, and integration with a trusted authentication source such as CA SiteMinder, IBM Webseal, and Integrated Windows Authentication. It also requires a web server to accept the pre-authenticated HTTP header information from your authentication source.

For more information, refer to Setting up Single Sign-on in Service Manager.

When you enable trusted sign-on (TSO), Mobile Applications will used the username of the user represented by the Principal to bypass the HPE Service Manager log-on screen, and then enter the application directly.

Enable TSO on the Service Manager server

In the sm.ini file, add the following parameter:

```
trustedsignon:1
```

For detailed information, refer to Setting up Single Sign-on in Service Manager.

Enable TSO on the Mobile Applications client

To enable TSO on the Mobile Applications client, follow these steps:

1. Open webapp-9.50.xxxx.war in an archive management program.
2. Extract the web.properties file from the WEB-INF directory to your local system, and then open this file in a text editor.
3. Locate the `isCustomAuthenticationUsed` script and set the value to `false`:

   ```
   # Set false to enable Trusted Sign-on
   isCustomAuthenticationUsed=false
   ```

4. Save the file and add the updated file back to the WEB-INF directory of the webapp-9.50.xxxx.war archive.
5. Extract the security.xml file from the WEB-INF/spring directory to your local system, and then open this file in a text editor.
6. Locate the following scripts:

   ```
   <!-- <security:custom-filter ref="preAuthenticationFilter" after="SECURITY_
   CONTEXT_FILTER"/>
       <security:custom-filter ref="lwSsoFilter" before="BASIC_AUTH_FILTER"/>
       <security:custom-filter ref="springSecurity2lwssoIntegrationFilter"
   position="LAST"/> -->
   ```

   Uncomment the first line as follows to enable TSO:

   ```
   <security:custom-filter ref="preAuthenticationFilter" after="SECURITY_CONTEXT_
   FILTER"/>
       <!--  <security:custom-filter ref="lwSsoFilter" before="BASIC_AUTH_
   FILTER"/>
       <security:custom-filter ref="springSecurity2lwssoIntegrationFilter"
   position="LAST"/> -->
   ```

   Or,

   For HTTP header pre-authentication, locate the following scripts and uncomment it:

   ```
   <!--<security:custom-filter ref="httpHeaderPreAuthenticationFilter"
   after="SECURITY_CONTEXT_FILTER"/>-->
   ```

7. Locate the httpHeaderPreAuthenticationFilter bean definition, and then at least change the principalRequestHeader setting, corresponding to the Header your Identity Management solution uses. For Webseal, iv-user is used as the value of principalRequestHeader, Siteminder often uses sm_user or sm_universalid. Note that this setting is case sensitive.
8. Save the file and add the updated file back to the WEB-INF/spring directory of the webapp-9.50.xxxx.war archive.
9. Configure the deployment environment to support the mobile system to receive the customized user information for authentication.

Set up Lightweight Single Sign-On (LW-SSO)

If Lightweight Single Sign-On (LW-SSO) is enabled on both the HPE Service Manager server and the Mobile Applications, Service Manager authentication will be bypassed if you have logged into another web application which also has LW-SSO enabled. The detailed bypass critieria includes both the protected domain/IP/DNS name and the initial LW-SSO string.

Enable LW-SSO on the Service Manager server

For detailed information about how to enable LW-SSO on Service Manager server, refer to the *HPE Service Manager 9.50 Help Center*.

Enable LW-SSO on the Mobile Applications client

To enable LW-SSO on the Mobile Applicationsclient, follow these steps:

1. Open webapp-9.50.xxxx.war in an archive management program.
2. Extract the security.xml file from the WEB-INF/spring directory to your local system, and then open this file in a text editor.
3. Locate the following scripts:

   ```
   <!-- <security:custom-filter ref="preAuthenticationFilter" after="SECURITY_
   CONTEXT_FILTER"/>
       <security:custom-filter ref="lwSsoFilter" before="BASIC_AUTH_FILTER"/>
       <security:custom-filter ref="springSecurity2lwssoIntegrationFilter"
   position="LAST"/> -->
   ```

   Uncomment the second line and the third line as follows to enable LW-SSO:

   ```
   <!-- <security:custom-filter ref="preAuthenticationFilter" after="SECURITY_
   CONTEXT_FILTER"/> -->
       <security:custom-filter ref="lwSsoFilter" before="BASIC_AUTH_FILTER"/>
       <security:custom-filter ref="springSecurity2lwssoIntegrationFilter"
   position="LAST"/>
   ```

4. Save the file and add the updated file back to the WEB-INF/spring directory of the webapp-9.50.xxxx.war archive.
5. Extract the lwssofmconf.xml file from the WEB-INF/classes directory to your local system, and then open this file in a text editor.

6. Configure the boldface parameters as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config
    xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/2.0">
    <enableLWSSO enableLWSSOFramework="true" enableCookieCreation="true"
cookieCreationType="LWSSO" enableSAML2Support="false"/>
    <webui>
        <validation>
            <in-ui-lwsso>
                <lwssoValidation  id="ID000001">
                    <domain>example.com</domain>
                    <crypto cipherType="symmetricBlockCipher"
                        engineName="AES" paddingModeName="CBC" keySize="256"
                        encodingMode="Base64Url"
                        initString="Please put your string here"></crypto>
                </lwssoValidation>
            </in-ui-lwsso>
        </validation>

        <creation>

            <lwssoCreationRef id="ID000002">
                <lwssoValidationRef refid="ID000001"/>
                <expirationPeriod>60</expirationPeriod>
            </lwssoCreationRef>

        </creation>

        <logoutURLs>
            <url>.*/std/logout</url>
            <url>.*/std/goodbye</url>
        </logoutURLs>

        <multiDomain>
            <trustedHosts>
               <!-- <DNSDomain>companydomain1.com</DNSDomain>
                <DNSDomain>companydomain2.com</DNSDomain>
                <NetBiosName>myserver1</NetBiosName>
                <NetBiosName>myserver2</NetBiosName>
                <IP>192.168.12.13</IP>
                <IP>192.168.12.14</IP>
                <FQDN>myserver1.companydomain1.com</FQDN>
                <FQDN>myserver2.companydomain2.com</FQDN>  -->
            </trustedHosts>
        </multiDomain>
```

```
    </webui>
</lwsso-config>
```

Required parameters for Mobile Applications client LW-SSO configurations

Parameter	Default value	Description
enableLWSSOFramework	`false`	Change this value to `true` to enable the LW-SSO framework.
domain	`example.com`	Change `example.com` to the domain name of the server host where you deploy your Mobile Applications client.
initString	`Please put your string here`	Enter your initial string. This initial string must be same as the initString value in the Service Manager LW-SSO configuration (minimum length: 12 characters). For example, smintegrationlwsso.

> **Note:** Beginning from the `<creation>` section to the end of the lwssofmconf.xml file, the variables are subject to change according to your actual deployment.

7. Save the file and add the updated file back to the WEB-INF/classes directory of the webapp-9.50.xxxx.war archive.

Work with Service Manager Mobile Applications

This chapter provides details about how to work with Service Manager Mobile Applications.

This chapter includes:

Preparing to launch Service Manager Mobile Applications on your smartphone

To prepare for launching Service Manager Mobile Applications on your smartphone, make sure:

1. Your touchscreen smartphone meets the requirements that are described in the *Service Manager Support Matrix*. For details, see HPE Support Matrices.
2. Your smartphone browser conforms to the following configurations:
   - Cookies are enabled.
   - JavaScript is enabled.
   - Pop-ups are enabled. At a minimum, add the Service Manager Mobile Applications host name to the pop-up exception list.
3. Your System Administrator has provided you with the web URL needed to access the Service Manager server from the Mobile Applications.

   Power user view: http://<*servername*>:<*portnumber*>/<*appname*>/std/ (/std/ can be omitted)

   Self-service user view: http://<*servername*>:<*portnumber*>/<*appname*>/ess/ (/ess/ cannot be omitted)
4. You have a valid Service Manager username and password.

Launching Service Manager Mobile Applications on your smartphone

User role: IT Operator

To launch Service Manager Mobile Applications on your smartphone, follow these steps:

1. In the web browser on your smartphone, type the Service Manager Mobile Applications web URL provided by your System Administrator. The Login page opens.
2. On the Login page, type your user name and password. The user name is auto-filled in the login screen the next time you log in.
3. Tap the **Language** field and scroll down to select your preferred language from the list, and then tap **Done**. The language defaults to your settings on Service Manager.

> **Note:**
> - Service Manager 9.50 Mobile Applications does not support right-to-left displayed languages such as Arabic and Hebrew.
> - Available languages are retrieved from the Service Manager server. Only when your Service Manager server has a language pack installed, the corresponding language appears in the language selection list.
> - If you clear your browser cookies from the smartphone, you need to type your user name and select the preferred language again the next time you log in.

4. Tap **Login** to log on to Mobile Applications.

> **Note:** Service Manager Mobile Applications supports multi-tenancy mode.

Using Service Manager Mobile Applications in power user view

The Service Manager Mobile Applications power user view is intended for Service Desk technicians, managers, and provides various views for the following tasks:

Understand the views within Service Manager Mobile Applications

After you logged in to Service Manager Mobile Applications, the default view is displayed depending on your user role. Service Manager Mobile Applications provides the following default views to access individual and group assignments and enables you to address any critical and pending issues that need immediate attention. If you are a Change Approver, you will also see change requests waiting for your approval.

Service Manager Mobile Applications Default Modules and Views

Module	View
Incident	• Assigned to Me • Assigned to My Groups
Change	• Awaiting My Approval • Assigned to My Groups
Interaction	• All My Interaction • Awaiting Approval
Approval[1]	• My Pending Approvals • My Pending Delegated Approvals

[1]As of version 9.40, Mobile Applications provides additional approvals for time periods and requests (for Service Manager Codeless).

List view

Being the default home page after you log on to Service Manager Mobile Applications, the List view enables you to navigate through lists of Incidents and Change requests. In the List view, you can perform the following tasks:

- Switch between different modules (Incident, Change, Interaction and Approval).
- Switch between different list views (For example, Assigned to Me, Assigned to My Groups, and so on).
- Scroll vertically through a list of records.
- Search for specific incidents, change requests and interactions by record ID.

Common tasks in the List view

Refer to the following content for some common user tasks in the List view.

- **To switch between different modules:**

  Tap the Module icon at the top and select other categories from the list. The default categories includes **Incident**, **Change** and so on.

- **To switch between different list views:**

  Refer to the Incident module as an example. Tap **Assigned to My Groups** at the top and scroll down to select **Assigned to Me** and so on from the list.

  > **Tip:** For more information about how to add views on Mobile Applications client, see "Add a view for Mobile Applications" on page 181.

- **To access the Detail view of a record:**

  When navigating through the records list, tap a record to access its Detail view.

- **To search for specific incidents and change requests by record ID:**

  a. Tap the Magnifier icon at the top. A Search field opens.

  b. In the Search field, type the `IM` or `C` prefix with ID of the incident record or change request. For example: `IM10002` or `C10003`.

  c. Tap **Enter**. The specific incident record or change request opens in the Detail view.

  > **Note:**
  > - When using the search function, make sure the prefix of the incident record or change request aligns with those in your Service Manager environment. For example, `C` is the prefix for a change request. For more information about how to configure the prefix of an incident record or a change request, see "Configure the prefix of a record" on page 179.

> - Service Manager Mobile Applications supports wildcards in the Search field. If you type `IM1000*` and then tap **Enter**, the multiple search results will be displayed as a list of Incident records.

- **Tap the Ellipsis icon at the top** and select corresponding option in the list opened to:
  - View or clear system messages for the current user
  - Log out of the mobile session
- **Tap the floating action bar** and select corresponding option in the list opened to:
  - Refresh the current page
  - Sort the records in the List View

Detail view

The Detail record view enables you to view or update the details of a record. In the Detail view, you can perform the following tasks:

- Browse the summary information and the updates of a record.
- Update the editable fields of a record (for example, Description, Status, Affected Service/CI).
- Reassign a record (update the Assignee and Assignment Group).
- Use the click-to-dial functionality and the click-to-email functionality. For example, if a field engineer wants to notify a customer that he is going to stop by, he can drill into the contact information of a record and use the single-click method to call or email the customer.

Common tasks in the Detail view

Refer to the following content for some common user tasks in the Detail view.

- **To access the List view of a record:**

  When navigating through detailed records, you can tap **Back** to go back to the List view.
- **Tap the tabs** at the top to display the detailed information of a record (for example, Categorization and Assignment, Related Records, Attachments, and so on).

> **Note:** The Related Records tab is not available in the power user view in Service Manager 9.50 Classic.

- **Tap the Fill icon** to update the editable fields of a record (for example, Status, Affected Service/CI, Assignee/Assignment Group).
- **Tap the bulb icon** in the contact information of a record, and then tap the telephone number to use the click-to-dial functionality. The dial dialog box will open.
- **Tap the bulb icon** in the contact information of a record, and then tap the email address to use the click-to-email functionality. The email application embedded in your smartphone opens.
- **Tap the Ellipsis icon at the top** and select corresponding option in the list opened to:
  - View or clear system messages for the current user.
  - Log out of the mobile session.
- **Tap the floating action bar** to display the options that you can perform on the current record.

Manage user interactions

After a user contact with the Service Desk is logged as an interaction, User Interaction Management provides the Service Desk Agents the ability to perform the following tasks from their smartphones:

- Browse and review interactions.
- Approve, deny or close an interaction.
- Update interactions. For example, a field engineer can update the details and add an activity (or journal entry) update to an interaction record.
- Approve or deny a Service Catalog request.

Update an open interaction

User role: Service Desk Agent

To update an open Service Desk interaction, follow these steps:

1. Tap the Service Desk interaction record you want to update. The Detail view of this record opens.
2. In the **Interaction Details** tab, update the request details as needed.
3. Tap the **Updates** tab.
4. In the **New Update Type** field, scroll up or down to select a type, and then tap **Done**.

5. In the **New Update** field, add the details for the new activity (or journal entry).
6. Tap **Save** from the action bar to save the record.

The details of the new activity entry will become available for customer viewing on your customer support portal.

Approve or deny an interaction

User role: Service Desk Agent

When an order is submitted from Service Desk, Service Manager automatically creates an interaction that, based on approval requirements, may have to be approved before its fulfillment or to be denied.

To process an interaction, follow these steps:

1. Tap a Service Desk interaction record from the **Awaiting Approvals** view. The Detail view of this record opens.
2. Review the Service Desk interaction and determine how you will process the approval interaction.
3. To approve an Service Desk interaction, tap **Approve** from the Ellipsis icon options.

   The record is now approved and disappear from the view list.
4. To deny an Service Desk interaction, follow these steps:
   a. Tap **Deny** from the action bar.
   b. Type the reason you are denying the request, and then tap **Save**.

   The record is now denied and disappears from the view list.

Close an interaction

User role: Service Desk Agent

You can close an existing Service Desk interaction if the user accepts the proposed solution. If you or the user disagree with the proposed solution, you need to resubmit the related incident for further investigation.

To close an existing Service Desk interaction, follow these steps:

1. Tap the Service Desk interaction record you want to close. The Detail view of this record opens.
2. Tap the Fill icon in the **Contact** field to determine which user will be notified of the solution.

3. If necessary, update the **Notify By** field to determine how the user will be notified.
4. Tap on the Fill icon in the **Closure Code** field to select a closure code.
5. Type the solution in the **Solution** field.
6. Tap **Close Interaction** from the action bar. The status of this interaction record changes to Closed.

Approve or deny a Service Catalog request

User role: Service Catalog approver

When an order is submitted from Service Catalog, HPE Service Manager automatically creates an interaction that, based on approval requirements, may have to be approved before its fulfillment or to be denied.

To process a Service Catalog request, follow these steps:

1. Tap a request record from the My Pending Approvals view. The Detail view of this record opens.
2. Review the request and determine how you will process the approval request.
3. To approve a Service Catalog request, tap **Approve** from the action bar.

   The record is now approved and disappear from the view list.

   > **Note:** You can also approve delegated approvals from the **My Pending Delegated Approvals** view.

4. To deny a Service Catalog request, follow these steps:
   a. Tap **Deny** from the action bar.
   b. Type the reason you are denying the request, and then tap **Save**.

The record is now denied and disappear from the view list.

Manage incidents

When incidents are escalated from Service Desk interactions, opened by support staff, or reported by event monitoring tools, Incident Management provides the Incident Management staff the ability to perform the following tasks from their smartphones:

- Browse and review incidents.
- Assign or reassign an incident.
- Investigate incidents.
- Update incidents. For example, a field engineer can add an activity (or journal entry) update to an incident record and set the customer-visible flag to make the update available for customer viewing on the customer support portal.
- Resolve or close a ticket. When a field engineer attempts to resolve or close an incident, HPE Service Manager determines the business logic and displays Resolve or Close accordingly.

Set the customer-visible flag for an incident's activity

User role: IT Operator

When you want to publish the activity (or journal entry) details of an incident for customer viewing, you can set the customer-visible flag in a new activity entry.

To set the customer-visible flag in a new activity (or journal entry) entry, follow these steps:

1. Tap the incident record you want to resolve. The Detail view of this record opens.
2. Tap the **Updates** tab.
3. In the **New Update Type** field, scroll up or down to select a type, and then tap **Done**.
4. Tap to highlight the check mark in the **Visible to Customer** field.
5. In the New Update field, add the details for the new activity (or journal entry).
6. Tap **Save** from the action bar to save the record.

The details of the new activity entry will become available for customer viewing on your customer support portal.

Reassign an incident

User role:Incident Analyst, Incident Coordinator, Incident Manager

At times you will need to reassign incident records when an Incident Analyst is unavailable.

To resolve an incident, follow these steps:

1. Tap the incident record you want to resolve. The Detail view of this record opens.
2. Tap the Fill icon in the **Assignee** field, and then select an operator from the list of names to reassign the incident to that person.
3. Tap **Save** from the action bar to save the record.

Resolve an incident

User role:Incident Analyst, Incident Coordinator, Incident Manager

To resolve an incident, follow these steps:

1. Tap the incident record you want to resolve. The Detail view of this record opens.
2. Tap the arrow icon in the **Status** field, and then tap **Resolved** to close the incident record.
3. Tap the Fill icon in the **Closure Code** field to select a closure code.
4. Type the solution in the Solution field.
5. Tap **Close Incident** from the action bar. The status of this incident record changes to Closed.

Manage changes

When a change request is logged, the Change Analyst assesses the change request, implements a plan for delivering the change, and then notifies the Change Coordinator as to the impact of the change. The change request is then submitted for Change Approver, or Change Advisory Board (CAB)'s approval. Service Manager Mobile Applications provide the Change Management staff the ability to perform the following tasks from their smartphones:

- Review change requests.
- Approve or deny changes.
- Coordinate change implementation.
- Handle emergency change requests.
- Assign or reassign change requests.
- Add activity (or journal entry) entries.
- Review change requests.

An example of a change approver's possible actions for a change record include approving or denying change requests. To deny a pending change request, a Change Approver may do the following:

- Drill down into a single record.
- Deny the ticket.
- In the Update field, type detailed notes about the denied request.

Users can also drill down to the details of a field within a record. For example, if a Change Management staff wants to add an activity (or journal entry) update to a change request, he/she nay do the following:

- Search for the change record.
- Drill down into the record's activities.
- Add the necessary activity update.
- Make any other necessary changes.

Set the customer-visible flag for a change's activity

User role: All users

When you want to publish the activity (or journal entry) details of a change for customer viewing, you can set the customer-visible flag in a new activity entry.

To set the customer-visible flag in a new activity (or journal entry) entry, follow these steps:

1. Tap the change record you want to resolve. The Detail view of this record opens.
2. Tap the **Activities** tab.
3. In the **New Update Type** field, scroll up or down to select a type, and then tap **Done**.
4. Tap to highlight the check mark for the **Visible to Customer** field.
5. In the **New Update** field, add the details for the new activity (or journal entry).
6. Tap **Save** from the action bar to save the record.

The details of the new activity entry will become available for customer viewing on your customer support portal.

Approve, deny or retract a change

User role: Change Approver

You can approve or deny a change that is pending approval only if you are a member of the necessary approval group and you are assigned the appropriate Change Management user profile. You can also retract a change that has been previously approved or denied, if you are unwilling to commit resources or know of technical incidents that affect the request.

To process a change approval request, follow these steps:

1. Tap a change record from the **Awaiting My Approval** view. The Detail view of this record opens.
2. Review the change information and determine how you will process the approval request.
3. To approve a change, tap **Approve** from the action bar.

   HPE Service Manager changes the Approval Status to approved, and the Change Manager updates the change and passes it to the Change Coordinator for implementation.
4. To deny a change, follow these steps:
   a. Tap **Deny** from the action bar.
   b. Type the reason you are denying the change, and then tap **Save**.

   Service Manager changes the Approval Status to denied, and no further approvals are possible until the denial is retracted.
5. To retract a change, follow these steps:
   a. Tap **Retract** from the action bar.
   b. Type the reason you are retracting the change, and then tap **Save**.

   Service Manager changes the Approval Status to pending, and the change request requires a new approval cycle to progress.

Using Service Manager Mobile Applications in self-service user view

The Service Manager Mobile Applications self-service user view is intended for end-users as an entry point to Service Desk and provides a simplified Service Desk interface for users to perform the following tasks:

- "Search the knowledge base" on the next page
- "Submit a self-service request" on the next page
- "Submit a smart request" on page 215

- "View opened and closed tickets" on page 216
- "View, approve, or deny pending approval requests" on page 216

Search the knowledge base

User role: IT Operator

To search the knowledge base for your questions, follow these steps:

1. Type your issue, and then tap the magnifier icon to search the knowledge base.

   > **Note:** The maximum length of the query key words string is limited to 1024 characters. Any query string longer than 1024 characters will be truncated to 1024 characters.

2. Tap the result record and view the knowledge article. You can tap **Cancel** on the bottom to return to the search results.
3. If you like an knowledge article, tap  .
4. To add feedback to the knowledge article, tap **Add Feedback**.

Perform Smart Search

After you have purchased a Smart Analytics module license and enabled Smart Analytics in Service Manager, Service Manager Mobile Applications supports Smart Search to perform advanced cross-module search actions in Service Manager resources (Knowledge Base articles and attachments) and external resources (SharePoint resources and static web pages). Meanwhile, Smart Search can perform a spell check to return meaningful results. For example, if you search for "offica," the search result will return records that include the term "office" if there is no exact result for "offica."

You need to set up and verify the server connectivity for multiple servers and connectors before you can use the Smart Search. For detailed information to configure and monitor the connectors and servers, refer to the related topics from *Service Manager Help Center*.

For detailed steps about how to perform Smart Search, see "Search the knowledge base" above.

Submit a self-service request

User role: IT Operator

If you cannot find the knowledge article to address your issue, you can also submit a self-service request.

To submit a self-service request, follow these steps:

1. Tap **Submit a Request** on the bottom of the screen. You can also tap the menu icon ≡, and then tap **Submit a Request** in the menu.
2. Type the required information for a support ticket, including title, description and urgency.
3. Tap + to attach a file as necessary. The supported file types including images (*.jpg, *.png, *.tiff and *.bmp) and PDF.

   > **Note:** Attachment is not supported on BlackBerry 6.x, 7.0 and 7.1 devices.

4. Tap **Submit** to submit the request.

Submit a smart request

User role: IT Operator

If you have installed and enabled HPE Service Manager Smart Analytics, **Submit a Smart Request** is automatically added to leverage the power of the Smart Ticket feature. You can tap **Submit a Smart Request** to open a new, simplified request form that only requires “description” or “attachment” to submit a request, which simplifies the process of submitting the ESS support requests.

To submit a smart request, follow these steps:

1. Tap **Submit a Request** on the bottom of the screen. You can also tap the menu icon ≡, and then tap **Submit a Smart Request** in the menu.
2. Tap + to attach an image file. For example, a screenshot of the error message.
3. (Optional) Type the comment for your request.
4. Tap **Submit** to submit the request.

Service Manager Smart Analytics will analyze your attached image file, fill in the necessary information automatically, and then generate the interaction directly.

> **Note: Submit a Smart Request** is visible to self-service users only when Service Manager Smart Analytics is enabled. However, this option is visible to the administrator no matter Smart Analytics is enabled or not.

View opened and closed tickets

User role: IT Operator

To view your opened and closed tickets, follow these steps:

1. Tap **My Closed Ticket** or **My Opened Ticket** to view your submitted tickets.
2. Tap the record to view the content of a ticket.
3. Scroll down to the bottom of the screen to see a list of the related records.
4. You can update, close or resubmit the ticket by tap the buttons on the bottom of the screen.

View, approve, or deny pending approval requests

User role: IT Operator

Users with the self-service Approval menu is allowed to view, approve, or deny pending approval requests.

To view, approve, or deny pending approval requests, follow these steps:

1. Tap the menu icon  and then tap **Pending Approval** to view your pending approvals.
2. Tap one record and then tap **View**, **Approve** or **Deny**.
3. If there are more than 10 pending approvals, tap the **More** button to view the records on the next page.

Appendix A: Mobile Applications Form Widgets

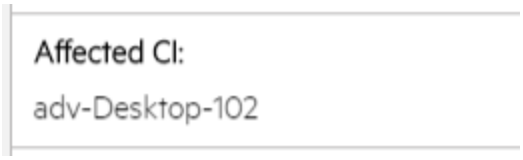
This chapter provides detailed information about the widgets on HPE Service Manager Mobile Applications forms.

This chapter includes:

Label control

Use this control to add a label. A label is a single line of text you can use to give titles to forms, give labels to objects within the form, or otherwise place text on the form.

Refer to the following screenshot as an example of the label control widget on a Mobile Applications form:



Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Caption	(Required) Specify a text caption for the object.
Input	(Optional) Specify the database field or variable to associate with this control. When input is specified, the Label will be displayed as a read-only Text.
Label For	(Optional) Specify the widget which the label belongs to.

Note: A label which is neither referred by any field or variable nor belongs to any other widget will not be displayed on a Mobile Applications form.

Text control

Use this control to add a text box that displays the contents of a text field and conditionally enables users to enter or modify its contents.

Refer to the following screenshot as an example of the text control widget on a Mobile Applications form:

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object. This name is also used by the Label For property to specify the label of this widget.
Input	Specify the database field or variable to associate with this control.

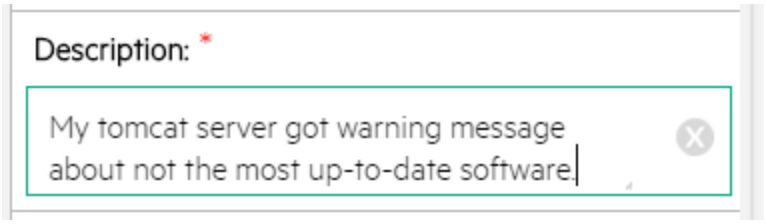
Property	Usage
Read-Only	Select this option to disable editing capabilities and provide only viewing access to the field.
Mandatory	Setting Mandatory to **Yes** by selecting the check box indicates that the field is required and therefore an asterisk indicating a required field is displayed. This is a visible change only. To make the field mandatory for any form it appears on, use the System Definition Utility. To make the field mandatory for a small number of forms only, use Format Control.

> **Note:** If the text is too long for a mobile device to display in one line, use a Text area control instead.

Text area control

Use this control to add a text area that displays the contents of a text field and conditionally enables users to input several lines of data. This object contains scroll bars and allows text wrapping.

Refer to the following screenshot as an example of the text area control widget on a Mobile Applications form:



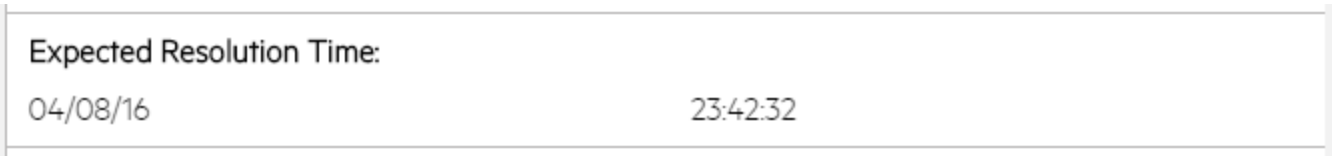
Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object. This name is also used by the Label For property to specify the label of this widget.
Input	Specify the database field or variable to associate with this control.
Read-Only	Select this option to disable editing capabilities and provide only viewing access to the field.
Mandatory	Select this option so that a red asterisk indicating a required field is displayed. This is a visible change only. • To make the field mandatory for any form it appears on, use the System Definition

Property	Usage
	Utility. • To make the field mandatory for a small number of forms only, use Format Control.

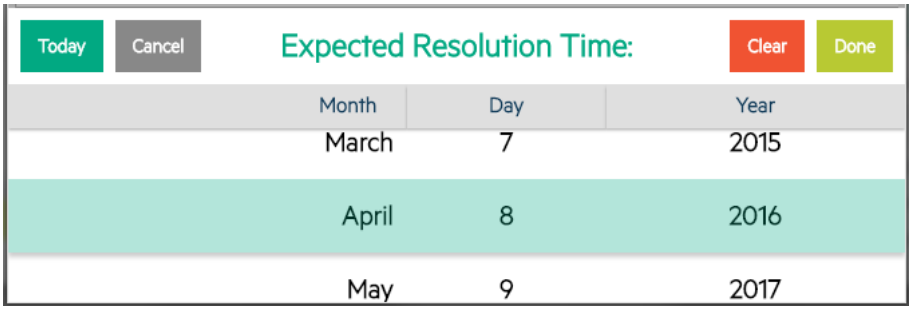
Date control

Use this control to add a text box that displays and enables users to update the contents of a date field.

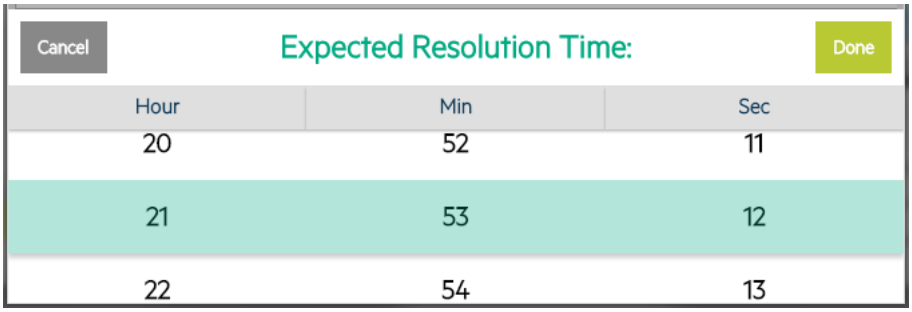
Refer to the following screenshot as an example of the date control widget on a Mobile Applications form:



Refer to the following screenshot as an example of the date selector on a Mobile Applications form:



Refer to the following screenshot as an example of the time selector on a Mobile Applications form:



Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen.

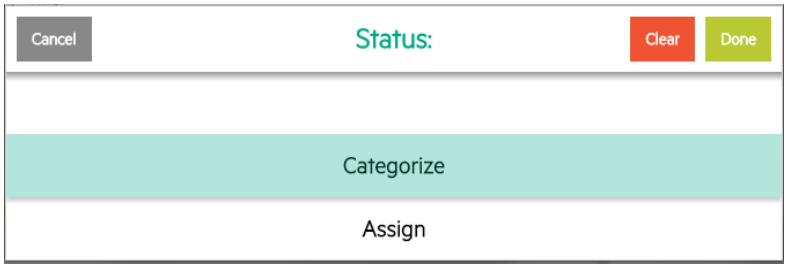
Property	Usage
	This name is used by external applications, such as RAD, to dynamically change the properties of the object. This name is also used by the Label For property to specify the label of this widget.
Input	Specify the database field or variable to associate with this control.
Read-Only	Select this option to disable editing capabilities and provide only viewing access to the field.
Mandatory	Select this option so that a red asterisk indicating a required field is displayed. This is a visible change only. • To make the field mandatory for any form it appears on, use the System Definition Utility. • To make the field mandatory for a small number of forms only, use Format Control.

Combo Box control

Use this control to add a Combo Box that enables users to click a button and select from a drop-down list. The items in the list are associated with a database field or variable. Users can also type in a value if the check box in the Select Only property is cleared (set to false).

Refer to the following screenshot as an example of the Combo Box control widget on a Mobile Applications form:

Refer to the following screenshot as an example of the Combo Box selector on a Mobile Applications form:



Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object. This name is also used by the Label For property to specify the label of this widget.
Input	Specify the database field or variable to associate with this control.
Read-Only	Select this option to disable editing capabilities and provide only viewing access to the field. Give read–only fields a tab–stop value of –1 to prevent users from tabbing into them.
Mandatory	Select this option so that a red asterisk indicating a required field is displayed. This is a visible change only. • To make the field mandatory for any form it appears on, use the System Definition Utility. • To make the field mandatory for a small number of forms only, use Format Control.
Value List	In conjunction with the Input property, defines how the Display List values are identified in the database. Value and Display Lists are entered using the Edit List dialog box. You can enter hard coded entries for each list, or you can supply a variable as the first and only entry. The run time values of the variable are used to populate these lists. **Note:** When defining Value List and Display List properties, you should avoid using the following reserved characters: • semicolon (;) • tab key • newline (carriage return) • form feed • backspace • equal sign (=) **Caution:** Do not use keys (such as backspace). The system cannot process their ASCII representation entries correctly, which may lead to unpredictable results.
Display List	Specify the values that appear in the drop-down list at run time. There must be a one–to–one correspondence between the values for Value List and for Display List. If the Display List is the only populated property, the display values are written to the database. **Note:** When defining Value List and Display List properties, you should avoid using the following reserved characters: • semicolon (;)

Property	Usage
	• tab key • newline (carriage return) • form feed • backspace • equal sign (=) **Caution:** Do not use keys (such as backspace). The system cannot process their ASCII representation entries correctly, which may lead to unpredictable results.

Note: Combo box is always select-only on HPE Service Manager Mobile Applications.

Comfill control

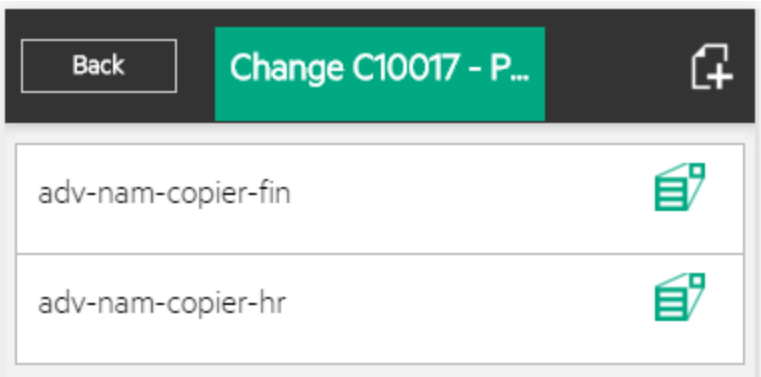
Use this control to add a combination Combo Box and Fill button. Comfill has all the properties of a Combo Box, plus the capability for Fill button. You can select which comfill buttons to display. For example, to display just a Fill button, set the Third Button Visible property to true by selecting the check box and set the Combo Button Visible property to false, by clearing the checkbox.

Note: As of Service Manager 9.41, the display name of a CI can be displayed in comfill for mobility. You can fill a CI by its display name.

Refer to the following screenshot as an example of the non-array comfill widget with popup form enabled on a Mobile Applications form:

Refer to the following screenshot as an example of the array comfill widget on a Mobile Applications form:

Refer to the following screenshot as an example of the array comfill widget after clicking:



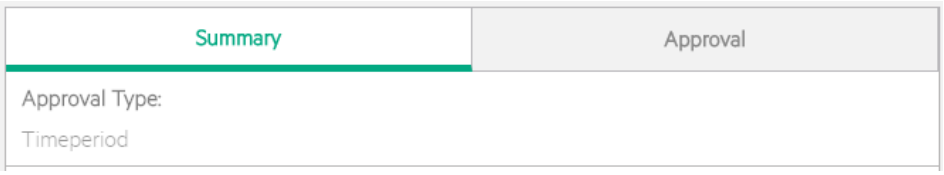
Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object. This name is also used by the Label For property to specify the label of this widget.
Input	Specify the database field or variable to associate with this control.
Read-Only	Select this option to disable editing capabilities and provide only viewing access to the field.
Mandatory	Select this option so that a red asterisk indicating a required field is displayed. This is a visible change only. • To make the field mandatory for any form it appears on, use the System Definition Utility. • To make the field mandatory for a small number of forms only, use Format Control.
Array Length	Specify the size of the scrolling region used to view array entries. A scroll bar appears beside the fields to allow users to view the array entries. • If a field is assigned an Array Length of 5, the form stacks five fields vertically to allow users to view the five array entries. • If Array Length is set to -1, the form dynamically creates as many fields as there are entries in the array. • If the Input data type is scalar, only a single text box appears. **Note:** The screen object must be associated with an array data structure. The default is 0, which means one vertical line of information appears.
Value List	In conjunction with the Input property, defines how the Display List values are identified in the database. Value and Display Lists are entered using the Edit List dialog box. You can enter hard coded entries for each list, or you can supply a variable as the first and only entry. The run time values of the variable are used to populate these lists.

Property	Usage
Display List	Specify the values that appear in the drop-down list at run time. There must be a one–to–one correspondence between the values for Value List and for Display List. If the Display List is the only populated property, the display values are written to the database.
Combo Button Visible	Select this option to make the Combo Button visible when the form opens. **Note:** When this property is enabled, the Fill Button Visible property is no longer effective.
Fill Button ID	Specify a Control ID to transmit when clicked.
Fill Button Visible	Select this option to make the Fill Button visible when the form opens.
Popup Subform Format	Specify the form to display.
Popup Subform Input	Specify the database field or variable to associate with this control.
Popup Subform Enabled	Select this option to enable the Popup Subform for this control.

Group control

Use this control to add a container that enables you to logically group associated items. In the Windows client the Group has a rectangular border with a text label at the top.

Refer to the following screenshot as an example of the group control widget on a Mobile Applications form:



Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen.

Property	Usage
	This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Caption	(Required) Specify a text caption for the object.

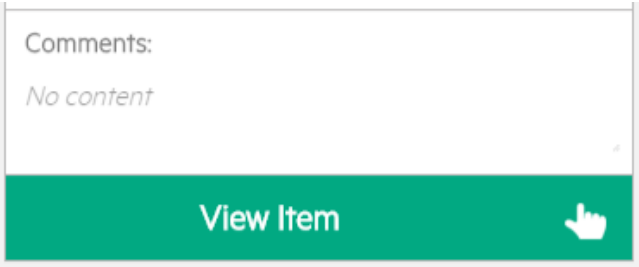
Note:

- Do not nest field groups.
- For usability and performance issues, do not include more than ten fields in a group.
- If there is one field group defined on a form at a minimum, the widgets which are not included in this group will not be displayed on a Mobile Applications form.

Button control

Use this control to add an input field that displays and enables users to update the contents of a numeric field and offers spinner buttons to increase or decrease a value.

Refer to the following screenshot as an example of the button control widget on a Mobile Applications form:



Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Caption	Specify a text caption for the object.
Button ID	Specify a numeric identification that specifies a Control ID to transmit when clicked.

Check box control

Use this control to add a check box that displays and enables users to update the contents of a Boolean (logical) field, which can evaluate to true, false, unknown, or null.

Refer to the following screenshot as an example of the check box control widget on a Mobile Applications form:

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Caption	Specify a text caption for the object.
Input	Specify the database field or variable to associate with this control.
Read-Only	Select this option to disable editing capabilities and provide only viewing access to the field. Give read–only fields a tab–stop value of –1 to prevent users from tabbing into them.

Attachments control

Use this control to add a box into which users can place non-Service Manager documents (For example, from Microsoft Word or Microsoft Excel).

To place an attachment container on a form, click **Attachments**, and then click the form.

Refer to the following screenshot as an example of the Attachments control widget on a Mobile Applications form:

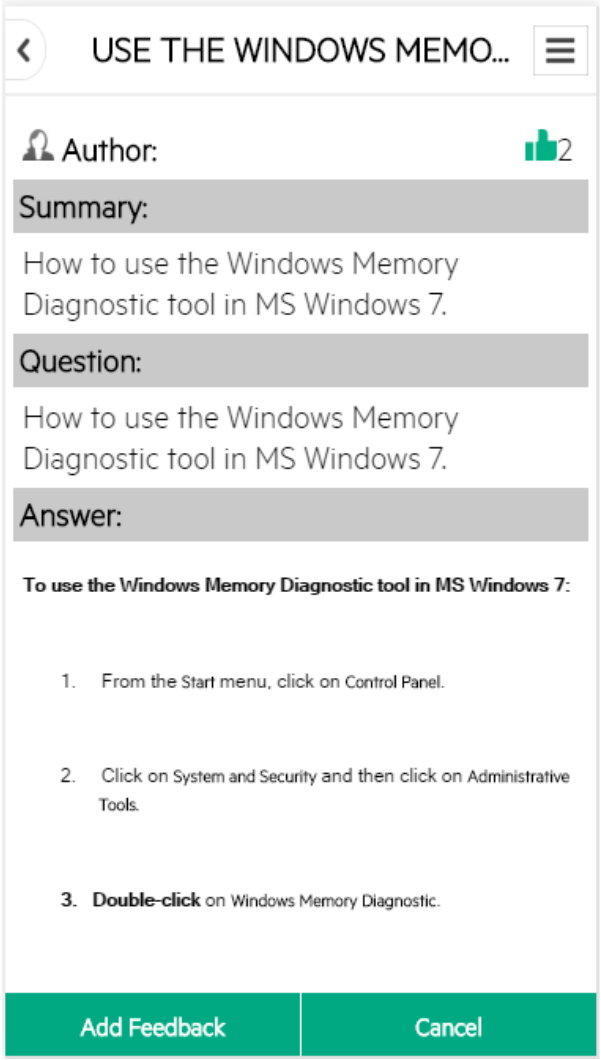
Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This identifier is used by external applications, such as RAD, to dynamically change the properties of the object.
Visible	Select this option to make the object visible on the form. Clear the check box to hide the object from view on the form.
Read-Only	Disable the editing capability of the control. Users can only view the attached documents when this option is selected. To prevent users from using the Tab key to enter the control, you can assign the value of -1 to the Read-Only field.
Maximum Attachment Size	Specify the maximum size of an attachment, in bytes. **Note:** Size limits defined in the Maximum Attachment Size field in a user's operator record override the size limit specified in the Company record. A non-zero value overrides any values specified in the Company or Operator record.
Total Attachment Size	Specify the maximum amount of memory (in bytes) that all attachments in a form can use. The total size of all attachments must be lower than this threshold or the form no longer accepts additional attachments.
Maximum Attachments Allowed	Select whether you want to allow one or any number of attachments. **Known issue**: This property is not supported in Mobile Applications.

HTML Viewer control

Use this control to add an HTML Viewer that enables users to view the HTML created by using the HTML Editor.

To place an HTML Viewer on a form, click **HTML Viewer**, and then click the form. Be sure to put the name of the database field or variable that you want to associate with this control into the Input property.

Refer to the following screenshot as an example of the HTML Viewer control widget on a Mobile Applications form:

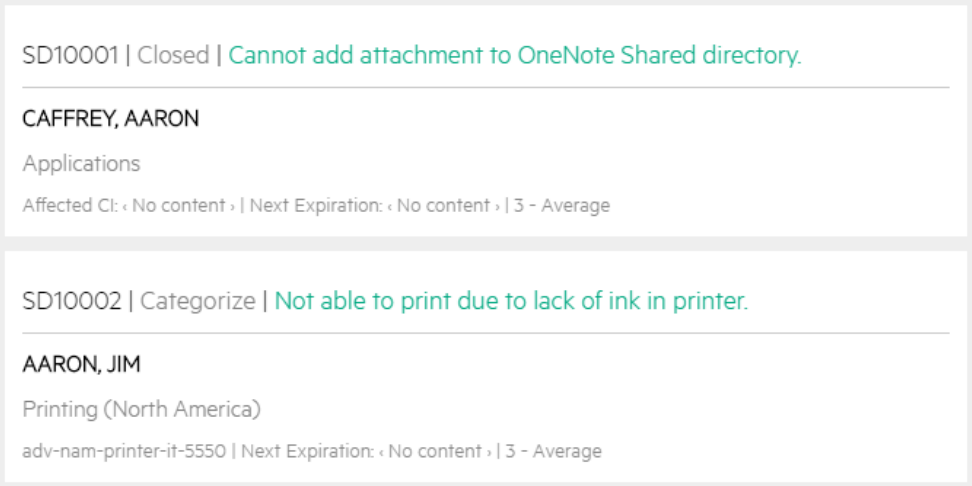


Property	Usage
Input	Specify the database field or variable to associate with this control.
Name	(Optional) Specify a unique identifier for the object on the screen.
Visible	Make the object visible or invisible on the form. Selecting the check box makes the object visible and clearing the check box makes it invisible.

Table control

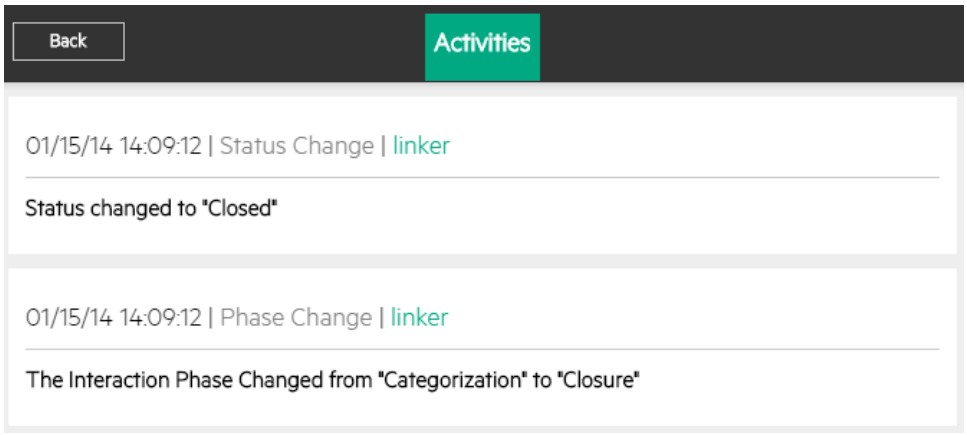
Use this control to add a table that displays one or more columns of data in a scrollable pane. The tables you create in the Form Designer appear as a rectangular region subdivided by rows and columns. The look and feel mimics tables in Microsoft Windows applications like Excel.

Refer to the following screenshot as an example of the table control widget in List view:



Refer to the following screenshot as an example of the table control widget in Detail view:

Refer to the following screenshot as an example of the table control widget after clicking:



Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This field is required if you enable the Multiple Selection property. This name is used by external applications, such as RAD, to dynamically change the properties of the object. This name is also used by the “Label For” property to specify the label of this widget.
Read-Only	Always read-only.
Columns	Specify a list of columns in the table.

Table column control

Use this control to add a column to an existing table.

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Caption	Specify a text caption for the object.
Input	Specify the database field or variable to associate with this control.
Field	In the case where the array specified in the input property is an array of structure, it specifies the field in the structure for this object.
Display List	Specify the values that appear in the drop-down list at run time. There must be a one–to–one correspondence between the values for Value List and for Display List. If the Display List is the only populated property, the display values are what were written to the

Property	Usage
	database.
Read-Only	Always read-only.

Subform control

Use this control to display a subform on another form.

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Format	Specify the form to display. Be sure you type the exact form name.
Virtual Join	Select this option to associate virtual join run time processing with the subform object. Clear the check box to use a same-file join.
Display Using Table	Select this option to display the subform in table format.
Input	Specify the database field or variable to associate with this control.

Dynamic Form control

Use this control to add a dynamic form that becomes visible when populated by XML from a RAD application or JavaScript. The aspect and content of the dynamic form depend on the XML.

To place a dynamic form on a form, click **Dynamic Form** and then click the form.

Be sure to put the name of the database field or variable that you want to associate with this control into the Input property.

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Visible	Select this option to make the object visible on the form. Clear the check box to hide the object from view on the form.

Property	Usage
Read-Only	In this release, we does not support change user options from mobile. All the contents inside the dynamic form will be read-only.
Input	Specify the database field or variable to associate with this control.

Notebook control

Use this control to subdivide the contents of a screen into logical groups or categories. Notebooks provide an aesthetic way of organizing large amounts of data into small spaces.

Click to the right of the last tab on the notebook to open the notebook properties. Click the tab and then the blank area below the tab to open the notebook tab properties.

To place a notebook on a form, click **Notebook** and then click the form.

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Visible	Select this option to make the object visible on the form. Clear the check box to hide the object from view on the form.

Notebook tab control

Use this control to add a tab to an existing notebook. Navigate to each page of the notebook by selecting its tab.

Click to the right of the last tab on the notebook to open the notebook's properties. Click the **notebook** tab and then the blank area below the tab to open the notebook tab's properties.

Property	Usage
Name	(Optional) Specify a unique identifier for the object on the screen. This name is used by external applications, such as RAD, to dynamically change the properties of the object.
Caption	(Required) Specify a text caption for the object.
Visible	Select this option to make the object visible on the form. Clear the check box to hide the object from view on the form.

Appendix B: Mobile Applications for HPE Service Manager Process Designer

Multiple Mobile Applications forms are designed for HPE Service Manager 9.50 Codeless. Refer to the following table for detail.

Mobile Application forms designed for PD

Module	Workflow	Phase	Display Option/Action/Transation	Forms for Mobile Applications
Change	Emergency	E-CAB Approval	Approve, Deny, Retract and Save	chm.emergency.approval.mobile chm.subform.activity.mobile
	Standard	Authorization CAB	Approve, Deny, Retract and Save	chm.standard.approval.mobile
	Normal	T-CAB Approval D-CAB Approval	Approve, Deny, Retract and Save	chm.normal.dcab.approval.mobile chm.normal.tcab.approval.mobile
	Change Proposal	Authorization CAB	Approve, Deny, Retract and Save	chm.proposal.tcab.approval.mobile
Incident	Incident	Categorization Investigation Review Recovery	Save and Close	im.incident.categorization.mobile im.incident.investigation.mobile im.incident.recovery.mobile im.incident.review.mobile

Mobile Application forms designed for PD, continued

Module	Workflow	Phase	Display Option/Action/Transation	Forms for Mobile Applications
		Closure		im.incident.closure.mobile im.incident.close.mobile
Interaction	Service Catalog	Categorization Work In Progress Review Closure	Approve, Deny, Retract, Update and Close	sd.interaction.svc.categorization.mobile sd.interaction.svc.workinprogress.mobile sd.interaction.svc.review.mobile sd.interaction.svc.closure.mobile
	Service Desk	Categorization Work In Progress Review Closure	Update, Close	sd.interaction.categorization.mobile sd.interaction.closure.mobile sd.interaction.workinprogress.mobile sd.interaction.review.mobile sd.interaction.subform.detail.mobile
	Streamlined Complaint or Compliment	Open In Progress Close Canceled	Update, Close	sd.streamlined.detail.mobile sd.streamlined.closure.mobile
	Streamlined Service Catalog	Open Pending Approval Work In	Approve, Deny, Retract, Update and Close	sd.streamlined.svc.detail.mobil sd.streamlined.svc.closure.mobile

Mobile Application forms designed for PD, continued

Module	Workflow	Phase	Display Option/Action/Transation	Forms for Mobile Applications
		Progress Close Canceled		
	Streamlined Service Desk	Open Work In Progress Close Canceled	Update, Close	sd.streamlined.itil.detail.mobil sd.streamlined.itil.closure.mobile
Request	Request	Authorization	Approve, Deny	rm.request.authorization.mobile rm.request.fullfillment.subform.detail.mobile

Note: Being widely used in PD forms, the Dynamic View Dependencies (DVD) conditions for widgets are not supported by Mobile Applications. On Mobile Applications client, errors may occur when you are updating a record which uses PD forms with DVD conditions. The errors include blank title on the Related Records tab, some invisible fields in HPE Service Manager become visible on Mobile Applications client, and so on. We recommend that you to use customized forms on Mobile Applications client and avoid the DVD conditions.

PD Change module

A typical usage of your Mobile Applications is to approve or deny a change on the smartphone regardless of the change's category. Based on the phases and workflows introduced by PD, a series of chm.*.mobile sample forms are designed for Mobile Applications to address the Emergercy, Standard, Normal changes and the Change Proposals. For Normal or Standard changes, or Emergency changes in a phase other than E-CAB Approval , you need to define your own forms. Otherwise, the original PD forms will be exposed on Mobile Applications client.

You need to move the created Emergency change to the E-CAB Approval phase in HPE Service Manager before utilizing them on Mobile Applications client. For any Emergency change in the E-CAB Approval phase, Mobile Applications client displays Change Main, Updates, and Approval groups as corresponding tabs in the Detail view. You are able to approve, deny and update a change in this phase. In addition, you are also able to search for any approved or denied change by using global search and then retract the change.

PD Incident module

For a newly created incident in the Categorization phase, Incident Details, Categorization and Assignment, Major & Escalation, Activities, Proposed Solution and Related Records groups are displayed as corresponding tabs in the Detail view on Mobile Applications client. You are able to update the incident in this phase.

Change the incident's status to Work in Progress, the incident moves to the Investigation phase. You are able to update the incident in this phase.

After updating the proposed solutions and save the record, the incident moves to the Recovery phase. You are able to update and close the incident in this phase.

After changing the incident's status to Resolved, the incident moves to the Review phase. The Proposed Solution tab is renamed to Recovery Action and you are able to update and close the incident in this phase.

After closing the incident on Mobile Applications client, the incident moves to the Closure phase and all tabs become read-only.

PD Interaction module

If an interaction is ordered from the catalog or opened by Service Desk and includes pending request level approvals, it is read-only on Mobile Applications client before all approvals are approved. You are able to approve or deny the interaction in this phase. In addition, you are also able to search for any approved or denied interaction by using global search and then retract the interaction.

After approving all pending approvals, the interaction moves to the Work In Progress phase. You are able to update and withdraw the interaction in this phase.

After updating the proposed solutions and save the record, the interaction moves to the Review phase. You are able to update and close interaction in this phase.

After closing the interaction on Mobile Applications client, the interaction moves to the Closure phase and all tabs become read-only.

> **Note:** Streamlined Interaction is disabled by default in Service Manager 9.50. You need to manually enable it before accessing the interactions from the Mobile Applications client. After you adopted Streamlined Interaction, the workflow is slightly different after interaction approval. For more information, see *HPE Service Manager Help Center > Service Desk*.

Appendix C: Troubleshooting

This chapter provides troubleshooting information about HPE Service Manager Mobile Applications installation and configuration issues and provide solutions.

This chapter includes:

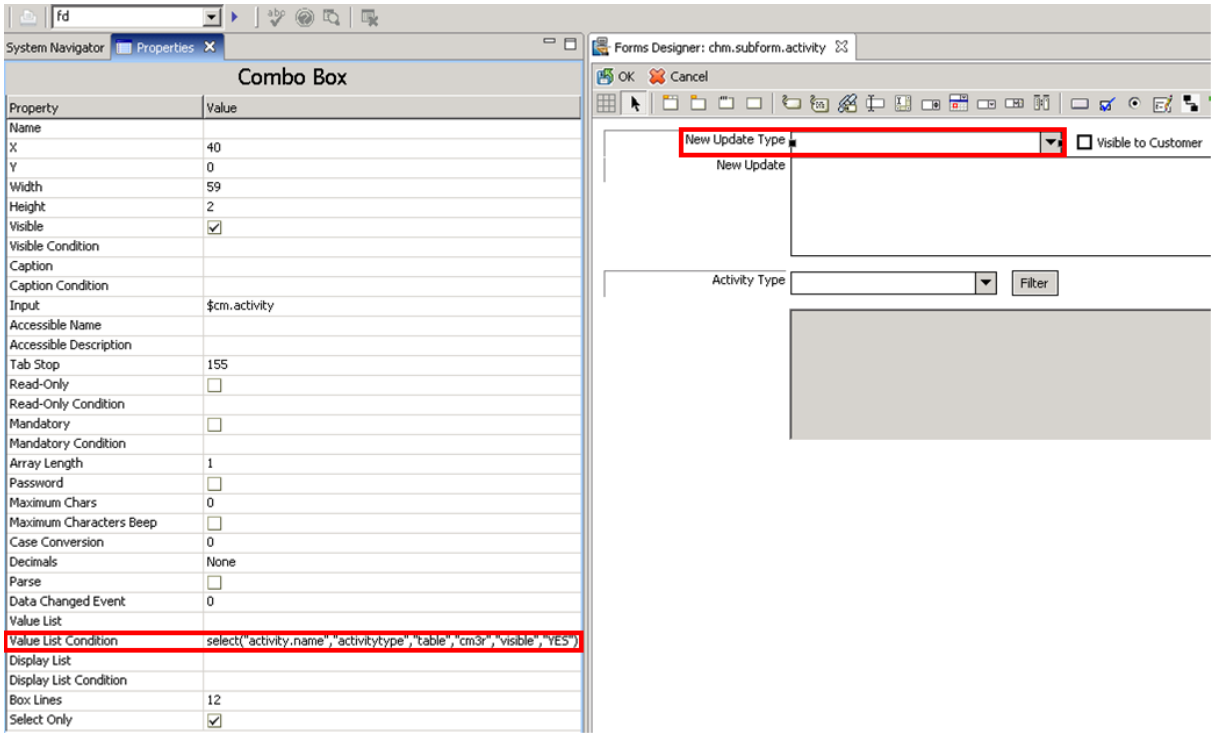
Widgets do not support Dynamic View Dependencies (DVD)

Issue

Some widgets on the forms do not support the Dynamic View Dependencies (DVD) feature of Forms Designer. How to solve this problem?

Solution

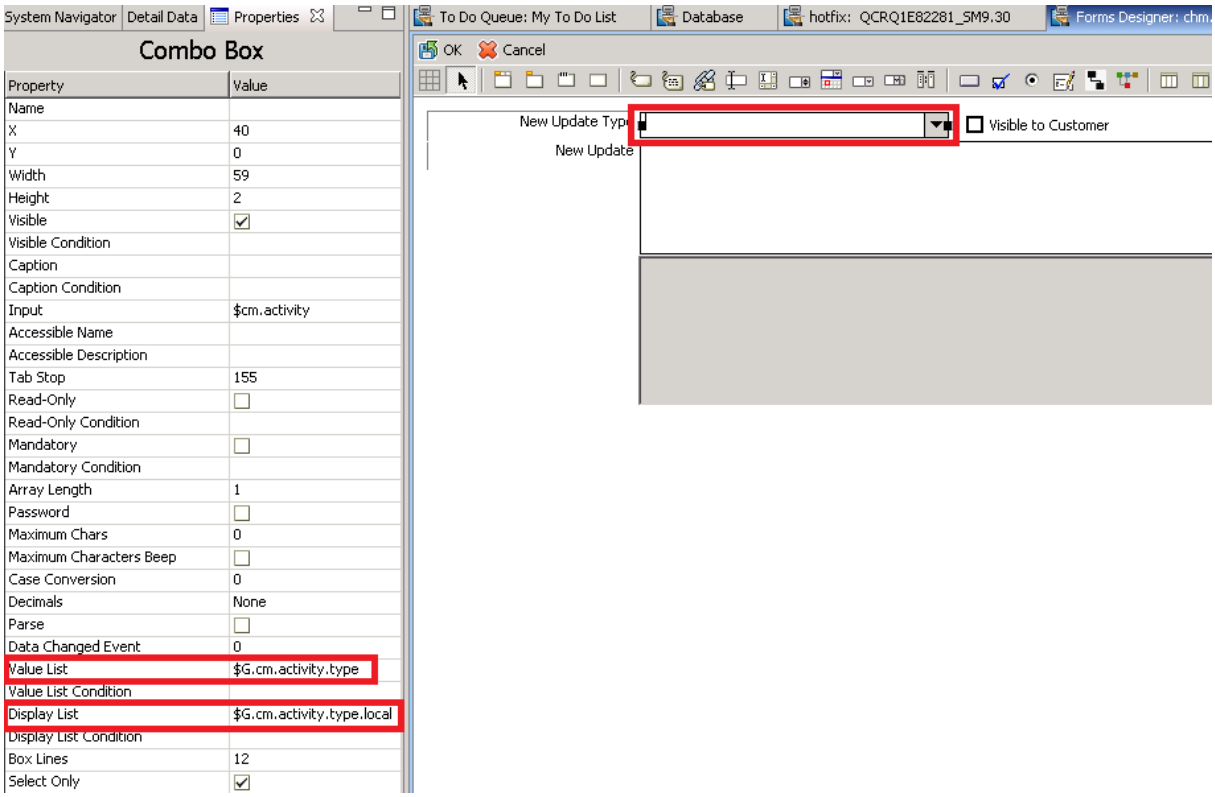
In the following example, the chm.subform.activity form has the **New Update Type** field using the DVD feature as illustrated below:



Since the current version of HPE Service Manager Mobile Applications does not support the DVD feature, change the properties of Value List, Value List Condition and Display List as below to avoid using the DVD feature:

Property	Old Value	New Value
Value List	Null	$G.cm.activity.type
Value List Condition	select ("activity.name","activitytype","table","cm3r","visible", "YES")	Null
Display List	Null	$G.cm.activity.type.local

Refer to the following screenshot as an example:


System Navigator
Detail Data
Properties
Combo Box
Property
Value
Name
X
40
Y
0
Width
59
Height
2
Visible
Visible Condition
Caption
Caption Condition
Input
$cm.activity
Accessible Name
Accessible Description
Tab Stop
155
Read-Only
Read-Only Condition
Mandatory
Mandatory Condition
Array Length
1
Password
Maximum Chars
0
Maximum Characters Beep
Case Conversion
0
Decimals
None
Parse
Data Changed Event
0
Value List
$G.cm.activity.type
Value List Condition
Display List
$G.cm.activity.type.local
Display List Condition
Box Lines
12
Select Only
To Do Queue: My To Do List
Database
hotfix: QCRQ1E82281_SM9.30
Forms Designer: chm
OK
Cancel
New Update Typ
New Update
Visible to Customer

Install and configure Smart Analytics

Built on Service Manager (SM) and using an OEM-licensed version of HPE IDOL, SM Smart Analytics heralds the debut of the "Big Data" edition of Service Manager.

Smart Analytics offers the following capabilities: Smart Ticket, Hot Topic Analytics, and Smart Search. For more information, search for "Smart Analytics overview" in the Service Manager Help Center.

As of Service Manager 9.41, you can choose to use either the IDOL Search Engine or the Solr Search Engine for Knowledge Management.

> **Note:** If you have purchased Service Manager Smart Analytics, you do not need to install the Solr Search Engine. Additionally, once you have enabled Smart Analytics, you cannot use Solr as the search engine any more.

Follow these instructions to install and configure Smart Analytics.

> **Note:** If you are upgrading your Smart Analytics from an earlier version to SM 9.50 Smart Analytics, search for "Upgrade Smart Analytics" in the Service Manager Help Center.

> **Note:** For information about how to administer Service Manager Smart Analytics, search for "Smart Analytics Administration" in the Service Manager Help Center.

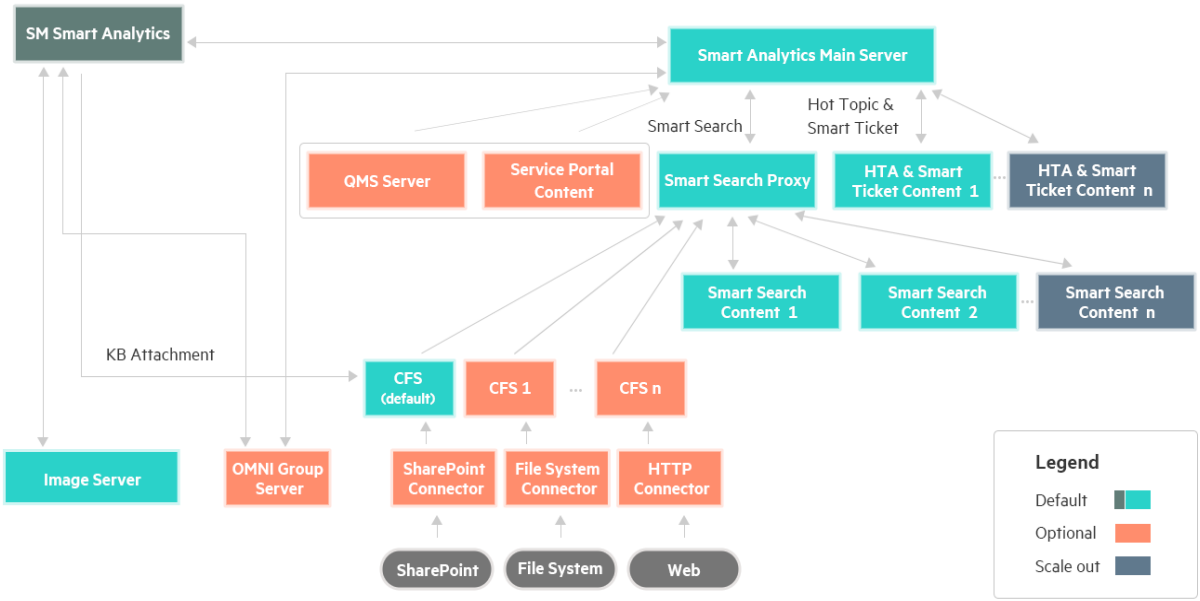
Install Smart Analytics

To install Smart Analytics, follow the instructions in these sections:

> **Note:** Before you install Service Manager 9.50 Smart Analytics, make sure that you have installed or upgraded to Service Manager 9.50 Applications.

Installation overview

Smart Analytics is powered by HPE IDOL. You need to prepare servers to deploy Smart Analytics. Check the information of Smart Analytics architecture as displayed in the following diagram before installation.



Smart Analytics deployment scenario

This section describes Smart Analytics installation options based on different deployment scenarios.

For small to medium enterprises with data volume smaller than 6 million records, Service Manager provides four templates to fit different needs:

- **Quick Install**

  If you do not need search file systems, web sites or SharePoint, you can choose **Quick Install** to deploy only necessary components for Smart Analytics on one server. When performing quick install, you can only configure the server ports, while service ports and index ports are automatically configured based on the server ports that you specify.

  > **Tip:** You can install corresponding connectors using the Customize template if you want to search external data sources in the future.

- **Basic for Smart Analytics**

  If you do not need search file systems, web sites or SharePoint, but need configure all ports, you can choose the **Basic for Smart Analytics** template in Advanced Install to deploy only necessary components for Smart Analytics on one server. When using **Basic for Smart Analytics**, you can manually configure the server ports, service ports and index ports.

  > **Tip:** You can install corresponding connectors using the Customize template if you want to search external data sources in the future.

- **All in One**

  If you would like to search file systems, web sites or SharePoint, and install all components on one server, you can choose the **All in One** template in Advanced Install. In this scenario, all Smart Analytics components will be installed. When using **All in one**, you can manually configure the server ports, service ports and index ports.

- **Basic for SM Service Portal**

  If you use Service Manager Service Portal as portal, you can choose the **Basic for SM Service Portal** template in Advanced Install to both necessary components for Smart Analytics and SM Service Portal will be installed. For more details, see "Set up Smart Analytics for Service Manager Service Portal" on page 278

For large enterprises with data volume larger than 6 million records, it is recommended that you install Smart Analytics on multiple servers using the **Customize** template in Advanced Install. For more information, see "Example: Deploying Smart Analytics on multiple servers" on page 269

Smart Analytics installer components

The following table lists the components available in Quick Installation and Advanced Installation respectively:

Installation type	Components included
Quick installation	• Smart Analytics Main Server • Smart Search Proxy server • One content server for Hot Topic Analytics and Smart Ticket • Two content servers for Smart Search • Default Connector Framework Server (for attachment index for Smart Search) • Image server for OCR
Advanced installation	• All components included in Quick Installation • Distributed Content Server • Distributed Image Server • CFS server • SharePoint Connector • HTTP Connector • File System Connector • OMNI Group Server • Portal Content • Query Manipulation Server **Note:** The Portal Content and Query Manipulation Server components are for Service Manager Service Portal only. Install these components only when you use Service Manager Service Portal.

Here is the description of the components for the Smart Analytics main server.

Component	Description
DIH (Distributed Index Handler)	Allows you to efficiently split and index extremely large quantities of data into multiple Smart Analytics content servers, in order to create a completely scalable solution that delivers high performance and high availability. It provides a flexible way of transparently batching, routing, and categorizing the indexing of internal and external content into Smart Analytics main server.
DAH (Distributed Action Handler)	Distributes actions to multiple child components of Smart Analytics main server. It enables you to scale your system in a linear manner, increasing the speed that runs actions and saving processing time.
Community	A Smart Analytics main server component that manages users and communities.

Component	Description
Agentstore	A Smart Analytics main server component that stores agents and categories.
Category	A Smart Analytics main server component that manages categorization and clustering
View	A Smart Analytics main server component that converts files in a repository to HTML formats for viewing in a Web browser.

Here is the description of the Smart Analytics connectors and protocol required for the installation.

Component	Description
OMNI Group Server	Communicates with SharePoint connector and LDAP to retrieve access permissions for your users. In this way, the access permissions can be applied to documents in the Smart Analytics main server. **Note:** LDAP - Lightweight Directory Access Protocol. A protocol that applications can use to retrieve information from a server. LDAP is used for directory services (such as corporate e-mail and telephone directories), and user authentication.
SharePoint Connector	Retrieves information from a Microsoft SharePoint repository, through the SharePoint web services. The connector can also retrieve information from an instance of SharePoint Online.
File System Connector	Retrieves various document types from file system so that the documents are available in smart search.
HTTP Connector	A powerful tool for retrieving documents from a web site. The HTTP Connector uses spiders to find web pages and to process the web pages for content and links to other web sites. HTTP Connector can retrieve various document types, including Web documents, Word, Excel, and PDF files.

Note: After you install a connector, you must configure the parameters for this connector from the corresponding .cfg file before you start the service. For a configuration example, see "Configure connectors" on page 293.

Default configuration for server ports

Server name	Default port number
HPE SM Smart Analytics main server port	9000

Server name	Default port number
Main content server port	10010
Smart Search Proxy server port	20010
First Smart Search content server port	30010
Second Smart Search content server port	30020
Image server port	18000
CFS server port	7000
OMNI group server port	5057
SharePoint connector port	36000
HTTP connector port	5678
File system connector port	1234
Query Manipulation Server port	16000
Portal Content server port	10020

To check ports occupied by Smart Analytics, search for "Get ports occupied by Smart Analytics" in the Service Manager Help Center.

> **Note:** For HPE SM Smart Analytics main server and Smart Search Proxy server, it is recommended you reserve the next 99 consecutive ports that follows the port you configured for the server. For example, if you specify the port number of Smart Analytics main server as 9000, then you need to reserve all the port numbers from 9000 to 9099.

System requirements

This section lists the hardware requirements and the supported operating systems for the Smart Analytics servers.

Hardware requirements

Quick installation

- 64 GB RAM (8 GB minimum)
- 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above)
- 500 GB disk

Advanced installation

About hardware requirements for typical install scenarios, please see table below.

Installation template	Hardware requirements
Basic for Smart Analytics	• 64 GB RAM (8 GB minimum) • 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above) • 500 GB disk
All in one	• 64 GB RAM (8 GB minimum) • 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above) • 700 GB disk
Basic for Service Portal	• 64 GB RAM (8 GB minimum) • 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above) • 600 GB disk
Distributed IDOL content server	• 4 GB RAM • A minimum of 2 dedicated CPU - XEON 3 GHz or above • 100 GB disk
Distributed image server	• 4 GB RAM • A minimum of 2 dedicated CPU - XEON 3 GHz or above • 100 GB disk
Customized scenarios	For the Smart Analytics proxy server (including

Installation template	Hardware requirements
	DIH, DAH, community, category, agentstore, view, and one second-level DIH and DAH), one Hot Topic Analytics content, and two sets of Smart Search content: • 64 GB RAM (8 GB minimum) • 8 Core (a minimum of 4 dedicated CPU - XEON 3 GHz or above) • 500 GB disk For each content or image server: • 4 GB RAM • A minimum of 2 dedicated CPU - XEON 3 GHz or above • 100 GB disk For each connector and CES and OMNI Group server: • 2 GB RAM • CPU - XEON 3 GHz or above • 20 GB disk

Note: For more information, see the *Service Manager Deployment Sizing Guide*, which is available on HPE Software Support Online (https://softwaresupport.hpe.com) as a white paper.

Supported operating systems

For the information about supported operating systems, see Service Manager 9.50 *Support Matrix*.

Install Smart Analytics on Windows

Before you install Smart Analytics, make sure that your servers meet the system requirements as specified in "System requirements" on page 247.

Caution: If you are re-installing content servers for a different Smart Analytics deployment architecture, do not manually add or remove Smart Search content servers in the IDOLServer.cfg

file when the installation is complete. Otherwise, you would encounter data loss when doing full index to index data.

To properly add or remove Smart Search content servers, see the Smart Analytics Administration section in the Service Manager Help Center.

Pre-install considerations

There are a number of key factors you should consider before deploying Smart Analytics:

- **Operating system** Smart Analytics supports Windows family and Linux operating system. It is recommended that all servers used utilize the same OS for easy of management.
- **Storage I/O performance**: Ideally, each SM Smart Analytics Component should have access to its own disk or partition, independently capable of 120 MB/s bandwidth and 180–200 IOPS (bandwidth being the more important metric).
- **Storage capacity**: Due to bandwidth bottlenecks of conventional HDDs, it is recommended that the size of the partitions utilized for each SM Smart Analytics Component should not exceed 300 GB.
- **Network** To properly interface with data repositories, Smart Analytics requires high-speed network access to the data repositories. In practice, this is accomplished by placing connectors physically “close” to the original data sources.

Install

To install Smart Analytics on a Windows-based system, follow these steps:

1. Obtain the Smart Analytics installer for Windows.
2. Unpack the .zip file and then double-click the setup application (`setupSmartAnalyticsWindowsX64.exe`).
3. The HPE SM 9.50 SmartAnalytics Setup wizard opens. Read the introduction, and then click **Next**.
4. Read the License Agreement. To continue the installation, select **I accept the terms of the License Agreement**, and then click **Next**.
5. Select **New Installation**, and then click **Next**.

6. Choose an installation folder, and then click **Next**. The default installation folder is `C:\Program Files(x86)\HPE\Service Manager 9.50\SmartAnalytics`.
7. Select **Quick Install** or **Advanced Install** as your installation type, and then click **Next**.
8. Continue with the corresponding installation steps.

   Quick Install

   Quick Install deploys the minimum required components to perform Smart Analytics on Service Manager internal data only. It sets default configurations, and no extra data source connectors are installed.

   To perform quick installation of Smart Analytics on Windows, continue with these steps:

   a. Select **Quick Install** as the installation type, and then click **Next**.
   b. Specify the IP address of your Service Manager Server, and then click **Next**.

      You need to specify the IP addresses (or host names) of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. Use commas to separate multiple addresses (do not use a space before or after a comma).

      > **Note:**
      > - Service Manager Server uses load balance, therefore, all slave Service Manager addresses should be specified in this step.
      > - Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

   c. Follow the configuration steps to configure ports for these servers. Click **Next** after each step.
      - HPE SM Smart Analytics main server
      - Main Content Server
      - Smart Search Proxy Server
      - Smart Search Content Server1
      - Smart Search Content Server2
      - Image Server
      - CFS Server
   d. Check the pre-installation summary. If you want to change your configuration, click **Previous**. Otherwise, click **Install** to start the installation.
   e. Wait for the installation to complete

Advanced Install

Advanced Install provides multiple installation templates, each including a group of server components and connectors. You can deploy components by selecting different installation templates for different scenarios.

To perform advanced installation of Smart Analytics on Windows, continue with these steps:

a. Select **Advanced Install** as the installation type, and then click **Next**.

b. Specify the IP address of your Service Manager Server.

You need to specify the IP addresses of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. Use commas to separate multiple addresses (do not use a space before or after a comma).

> **Note:**
>
> - Service Manager Server uses load balance, therefore, all slave Service Manager addresses should be specified in this step.
> - Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

c. Choose an installation template, and then click **Next**. To customize your installation, select the **Customize** template to choose from the available components.

Service Manager provides six out-of-box installation templates.

Installation template	Components included	Description
Basic for Smart Analytics	• Proxy Server Components (including DIH, DAH, community, category, agentstore, view, one second-level DIH and DAH, one main content server and two Smart Search content servers) • Image Server • CFS Server	Deploys the minimum required components to perform Smart Alalytics on Service Manager internal data only. No extra data source connectors are installed.
All in one	• Proxy server components (including DIH, DAH, community, category, agentstore, view, one	Deploys all components in one physical machine. In this way, you can use the full Smart Analytics functionality on both

Installation template	Components included	Description
	second-level DIH and DAH, one main content server and two Smart Search content servers) • Image Server • CFS Server • OMNI Group Server • SharePoint Connector • HTTP Connector • File System Connector	Service Manager without a large volume of data.
Basic for SM Service Portal	• Proxy Server Components (including DIH, DAH, community, category, agentstore, view, one second-level DIH and DAH, one main content server and two Smart Search content servers) • Image Server • CFS Server • Portal Content • Query Manipulation Server	Deploys the required components to support IDOL on Service Manager Service Portal. For more information, see "Set up Smart Analytics for Service Manager Service Portal" on page 278.
Distributed IDOL content server	Content Server	Installs remote or additional content servers to handle more data.
Distributed image server	• Image Server • Image Proxy Server	By default, one image server is included in the basic installation to handle OCR process. If there are too many image processing requests, you can deploy a distributed image server.
Customize	No pre-set components	Install any component based on your customized requirements. **Note:** Do not select

Installation template	Components included	Description
		Portal Content and **Query Manipulation Server** unless you plan to run Service Portal.

Note: If you plan to install the content servers and the proxy server on different machines, it is recommended that you install the content servers first. Because without content server installed and started, the proxy server cannot start and the OOB data cannot be imported. For detailed steps of installing Smart Analytics components on different machines, see "Example: Deploying Smart Analytics on multiple servers" on page 269

d. Specify the IP addresses of the remote machines on which you have installed or will install Smart Analytics components such as content servers, CFS servers and connectors, and then click **Next**.

e. Follow the configuration steps to configure the components you selected. Click **Next** after each configuration step.

If you did not select Main Content, Smart Search Content 1 or Smart Search Content2 in the installation template as described in step c, the installer displays configuration pages for you to specify the IPs and ports of the remote servers on which you have installed or will install these contents servers.

If you do not specify IPs and ports for remote content servers on the configuration pages, or you want to change your settings after installation, you need to manually edit the IPs and Ports in the following configuration files and corresponding sections:

File	Configurations
<*Smart Analytics Installation*>/IDOL/IDOLServer.cfg	[Service] …… ServiceStatusClients=…,<Remote Main Content Server IP> ServiceControlClients=…,<Remote Main Content Server IP> …… [Server]

File	Configurations
	…… QueryClients=…,<Remote Main Content Server IP> AdminClients=…,<Remote Main Content Server IP> IndexClients=…,<Remote Main Content Server IP> …… [IDOLServer1] …… Host=<Remote Main Content Server IP> Port=<Remote Main Content Server Port> ……
<*Smart Analytics Installation*> /level2proxy/IDOLServer.cfg	[Service] …… ServiceStatusClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> ServiceControlClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> …… [Server] …… QueryClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> AdminClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> IndexClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> …… [DistributionIDOLServers]

File	Configurations
	Number=2 [IDOLServer<0>] Host=<First Remote Smart Search Content Server IP> Port=<First Remote Smart Search Content Server Port> …… [IDOLServer<1>] Host=<Second Remote Smart Search Content Server IP> Port=<Second Remote Smart Search Content Server Port>

Some useful information for configuration:

- **Configure Smart Search Proxy Server** > **Replicas** : Specifies the number of identical copies of each document to index. This is configured in the level2proxy\IDOLServer.cfg file.

  The default value is set to **0**, which means that there is only one copy of each document for Smart Search. If you set the number as 1, it means that there will be two mirrored copies of the document in your Smart Search content servers.

  In Smart Search proxy level, content is distributed between virtual nodes, which the DIH assigns to its child servers. When you configure replicas, DIH copies the documents in a particular virtual node to two or more child servers. This method ensures there are two mirrored copies of the document in your system without you having to set up specifically mirrored child servers.

  > **Note:** The number of copies (that is, the value of Replicas plus one) must be no more than the number of child servers. If you create more copies than existing Smart Search child servers, DIH does not start.

- **Configure SharePoint Connector** > **SharePoint URL Type**:
  - To retrieve all content databases and site collections, set the value of this parameter to **WebApplication**. Set the value of the SharepointUrl parameter to the URL of the web application. You cannot use this value with SharePoint Online.

- To retrieve only one site collection, set the value of this parameter to **SiteCollection**. Set the value of the SharepointUrl parameter as the URL of the site collection.

- **Configure LDAP Repository** (for OMNI Group server):
  - LDAP User Base: the base DN or top level of the directory tree you want to search for users. This indicates where in the LDAP directory tree you want to begin the search.
  - LDAPGroupBase: the base DN or top level of the directory tree you want to search for groups. This indicates where in the LDAP directory tree you want to begin the search.
  - (Optional) UserFilter: the query you want to use to retrieve the set of users you want to store in the group server. For example, `UserFilter=(objectClass=hpeEmployee)`.
  - (Optional) GroupFilter: you can use GroupFilter to set the filter that is passed to the LDAP server to request a list of groups. For example, `GroupFilter=(objectClass=hpeGroup)`.

f. Check the pre-installation summary. If you want to change your configuration, click **Previous**. Otherwise, click **Install** to start the installation.

g. Wait for the installation to complete.

9. The Start Service page opens when the installation is complete. If you want to start the services now, select **Yes** and then click **Next**. Otherwise, select **No** and then click **Next**

> **Note:** HPE recommends you to start the services manually after you configure the .cfg files for each connector.

10. If you selected **Yes** in step 8, the Import OOB Data page opens. If you want to import the out-of-box data now, select **Yes** and then click **Next**. Otherwise, select **No** and then click **Next**.

> **Note:** Importing the out-of-box data will erase the previous data for Hot Topic Analytics.
>
> You can also import the out-of-box data at any time after the installation, by running the <*Smart Analytics Installation*>/OOBData/oobdata.cmd file.

11. Wait a few minutes for the installer to finish starting the services and importing the OOB data, and then click **Done**.

> **Note:**
>
> - Make sure that all the required components are started. If not, you need to start the corresponding component manually.
> - Under some circumstances, users are unable to connect to the main server in Service Manager while the status of HPE SM Smart Analytics Main Server shows **Started** in the

> Services snap-in. You can check `<Smart Analytics Installation>/IDOL/logs/application.log` to see if agentstore was started. If not, restart the HPE SM Smart Analytics Main Server service to troubleshoot the problem.

Post-install actions

After installation, you can modify the following configuration files to change the previous settings:

- Smart Analytics main server: <*Smart Analytics Installation*>/IDOL/IDOLServer.cfg
- Image server: <*Smart Analytics Installation*>/ImageServer#/ImageServer#.cfg
- Image proxy server: <*Smart Analytics Installation*>/ImageProxyServer/dah.cfg

  This is only required if you have installed multiple image servers in the distributed mode.
- Content server: <*Smart Analytics Installation*>/Content#/Content#.cfg
- CFS server: <*Smart Analytics Installation*>/CFS/CFS.cfg
- SharePoint connector: <*Smart Analytics Installation*>/SharepointRemoteConnector/SharepointRemoteConnector.cfg
- OMNI group server: <*Smart Analytics Installation*>/OmniGroupServer/OmniGroupServer.cfg
- HTTP connector: <*Smart Analytics Installation*>/HTTPConnector/httpconnector.cfg
- File system connector: <*Smart Analytics Installation*>/FileSystemConnector/filesystemconnector.cfg
- Portal content: <*Smart Analytics Installation*>/Content-SMSP/Content-SMSP.cfg
- Query Manipulation Server: <*Smart Analytics Installation*>/QMS/QMS.cfg

> **Note:** If you installed any connectors, you may need edit their configuration files manually. For more information, see "Configure connectors" on page 293.

Restart the corresponding components after you modify the related configuration files.

> **Tip:** If you want to uninstall SM Smart Analytics, see "Uninstall Smart Analytics" on page 307.

Install Smart Analytics on Linux

Before you install Smart Analytics, make sure that your servers meet the system requirements as specified in "System requirements" on page 247.

> **Caution:** If you are re-installing content servers for a different Smart Analytics deployment architecture, do not manually add or remove Smart Search content servers in the IDOLServer.cfg file when the installation is complete. Otherwise, you would encounter data loss when doing full index to index data.
>
> To properly add or remove Smart Search content servers, search for "Add a content server for Smart Search" and "Remove a content server for Smart Search" in the Service Manager Help Center.

Pre-install considerations

There are a number of key factors you should consider before deploying Smart Analytics:

- **Operating system** Smart Analytics supports Windows family and Linux operating system. It is recommended that all servers used utilize the same OS for easy of management.
- **Storage I/O performance**: Ideally, each IDOL engine should have access to its own disk or partition, independently capable of 120 MB/s bandwidth and 180–200 IOPS (bandwidth being the more important metric).
- **Storage capacity**: Due to bandwidth bottlenecks of conventional HDDs, it is recommended that the size of the partitions utilized for the IDOL services should not exceed 300 GB.
- **Network** To properly interface with data repositories, Smart Analytics requires high-speed network access to the data repositories. In practice, this is accomplished by placing connectors physically “close” to the original data sources.

Install

To install or re-install the SM Smart Analytics servers on a Linux-based system, follow these steps:

1. Obtain the SM Smart Analytics installer for Linux .
2. Unpack the .zip file and then execute the binary file (`setupSmartAnalyticsLinuxX64.bin`) from the command line on the Linux server.
3. Read the introduction, and then press **Enter**.
4. Read the License Agreement, and then press **Enter** repeatedly until you see **DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENTS? (Y/N)**.
5. Type **Y**, and then press **Enter**.
6. Select **New Installation**, and then press **Enter**.
7. Specify an installation folder, and then press **Enter**. The default installation folder is `/opt/HPE/ServiceManager9.50/SmartAnalytics`.
8. Select **Quick Install** or **Advanced Install** as your installation type, and then press **Enter**.
9. Continue with the corresponding installation steps.

   Quick Install

   Quick Install deploys the minimum required components to perform Smart Analytics on Service Manager internal data only. It sets default configurations, and no extra data source connectors are installed.

   To perform quick installation of Smart Analytics on Linux, continue with these steps:

   a. Specify the IP address of your Service Manager Server, and then press **Enter**.

      You need to specify the IP addresses of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. Use commas to separate multiple addresses (do not use a space before or after a comma).

      > **Note:**
      >
      > - Service Manager Server uses load balance, therefore, all slave Service Manager addresses should be specified in this step.
      > - Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

   b. Follow the configuration steps to configure ports for these servers. Press **Enter** after each step.

      - HPE SM Smart Analytics main server
      - Main Content Server

- Smart Search Proxy Server
- Smart Search Content Server1
- Smart Search Content Server2
- Image Server
- CFS Server

c. Check the pre-installation summary, and then press **Enter**.

d. Wait for the installation to complete.

Advanced Install

Advanced Install provides multiple installation templates, each including a group of server components and connectors. You can deploy components by selecting different installation templates for different scenarios.

To perform advanced installation of Smart Analytics on Linux, continue with these steps:

a. Specify the IP address of your Service Manager Server.

You need to specify the IP addresses of the Service Manager servers that are permitted to send administrative and query actions to the Smart Analytics servers. Use commas to separate multiple addresses (do not use a space before or after a comma).

> **Note:**
>
> - Service Manager Server uses load balance, therefore, all slave Service Manager addresses should be specified in this step.
> - Please use a valid FQDN or IP address for the server address. Do not use the localhost or 127.0.0.1.

b. Choose an installation template, and then press **Enter**. To customize your installation, select the **Customize** template to choose from the available components.

Service Manager provides six out-of-box installation templates.

Installation template	Components included	Description
Basic for Smart Analytics	• Proxy Server Components (including DIH, DAH, community, category, agentstore, view,	Deploys the minimum required components to perform Smart Alalytics on Service Manager internal data only. No extra data source connectors are installed.

Installation template	Components included	Description
	one second-level DIH and DAH, one main content server and two Smart Search content servers) • Image Server • CFS Server	
All in one	• Proxy Server Components (including DIH, DAH, community, category, agentstore, view, one second-level DIH and DAH, one main content server and two Smart Search content servers) • Image Server • CFS Server • OMNI Group Server • HTTP Connector • File System Connector	Deploys all components in one physical machine. In this way, you can use the full Smart Analytics functionality without a large volume of data.
Basic for SM Service Portal	• Proxy Server Components (including DIH, DAH, community, category, agentstore, view, one second-level DIH and DAH, one main content server and two Smart Search content servers) • Image Server	Deploys the required components to support IDOL on Service Manager Service Portal. For more information, see "Set up Smart Analytics for Service Manager Service Portal" on page 278.

Installation template	Components included	Description
	• CFS Server • Portal Content • Query Manipulation Server	
Distributed IDOL content server	Content Server	Installs remote or additional content servers to handle more data.
Distributed image server	• Image Server • Image Proxy Server	By default, one image server is included in the basic installation to handle OCR process. If there are too many image processing requests, you can deploy a distributed image server.
Customize	No pre-set components	Install any component based on your customized requirements. **Note:** Do not select **Portal Content** and **Query Manipulation Server** unless you plan to run Service Portal. Do not select **IDOL content server** at the same time when you have selected **Proxy Server Components**. If you plan to install distributed IDOL content servers on the same machine where you want to deploy the Proxy Server Components, install Proxy Server Components and distributed IDOL content servers separately by performing the install process different times.

Note: If you plan to install the content servers and the proxy server on different machines, it is recommended that you install the content servers first. Because without content server installed and started, the proxy server cannot start and the OOB data cannot be imported. For detailed steps of installing Smart Analytics components on different machines, see "Example: Deploying Smart Analytics on multiple servers" on

page 269.

c. Specify the IP address of the remote machine on which you have installed or will install Smart Analytics components, and then press **Enter**.

d. Follow the configuration steps to configure the components you selected. Press **Enter** after each configuration step.

   If you did not select Main Content, Smart Search Content 1 or Smart Search Content2 in the installation template as described in step c, the installer displays configuration pages for you to specify the IPs and ports of the remote servers on which you have installed or will install these contents servers.

   If you do not specify IPs and ports for remote content servers on the configuration pages, or you want to change your settings after installation, you need to manually edit the IPs and Ports in the following configuration files and corresponding sections:

File	Configurations
<*Smart Analytics Installation*> /IDOL/IDOLServer.cfg	[Service] …… ServiceStatusClients=…,<Remote Main Content Server IP> ServiceControlClients=…,<Remote Main Content Server IP> …… [Server] …… QueryClients=…,<Remote Main Content Server IP> AdminClients=…,<Remote Main Content Server IP> IndexClients=…,<Remote Main Content Server IP> …… [IDOLServer1] …… Host=<Remote Main Content Server IP> Port=<Remote Main Content Server Port> ……

File	Configurations
<Smart Analytics Installation> /level2proxy/IDOLServer.cfg	[Service] …… ServiceStatusClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> ServiceControlClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> …… [Server] …… QueryClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> AdminClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> IndexClients=……,<First Remote Smart Search Content Server IP>,<Second Remote Smart Search Content Server IP> …… [DistributionIDOLServers] Number=2 [IDOLServer<0>] Host=<First Remote Smart Search Content Server IP> Port=<First Remote Smart Search Content Server Port> …… [IDOLServer<1>] Host=<Second Remote Smart Search Content Server IP> Port=<Second Remote Smart Search Content Server Port>

Some useful information for configuration:

Configure Smart Search Proxy Server > **Replicas** : Specifies the number of identical copies of each document to index. This is configured in the level2proxy\IDOLServer.cfg file.

The default value is set to **0**, which means that there is only one copy of each document for Smart Search. If you set the number as 1, it means that there will be two mirrored copies of the document in your Smart Search content servers.

In Smart Search proxy level, content is distributed between virtual nodes, which the DIH assigns to its child servers. When you configure replicas, DIH copies the documents in a particular virtual node to two or more child servers. This method ensures there are two mirrored copies of the document in your system without you having to set up specifically mirrored child servers.

> **Note:** The number of copies (that is, the value of Replicas plus one) must be no more than the number of child servers. If you create more copies than existing Smart Search child servers, DIH does not start.

e. Check the pre-installation summary, and then press **Enter**.

f. Wait for the installation to complete.

10. Press **Enter** to exit the installer.

Post-install actions

1. Run the following command to import the out-of-box data before you start any components of Smart Analytics, r:

   ```
   [INSTALL_DIR]/OOBData/ImportOOBData.sh
   ```

2. Start the components of SM Smart Analytics.

   Start all the components with a single command

   To start all the components, run the following command:

   ```
   [INSTALL_DIR]/scripts/StartALL.sh
   ```

   > **Note:**

a. This script starts all the components that you installed one by one.

b. By running this command, you also start components like connectors, if they are installed.

Tip: If you want to stop all these components, run the following command:

```
[INSTALL_DIR]/scripts/StopALL.sh
```

Start the components with separate commands

To start a single component that you installed, run the corresponding command as follows:

- To start a content server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StartContent[x].sh
  ```

  Note: Replace [x] with the number of your content server, for example, `StartContent1`.

  Tip: If you want to stop a content server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StopContent[x].sh
  ```

- To start both the main proxy server and the Smart Search proxy server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StartIDOL.sh
  ```

  Note: Before you start the main proxy server, make sure all the content servers have started.

  Tip: If you want to stop the main proxy server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StopIDOL.sh
  ```

- To start a Connector Framework Server (CFS), run the following command:

  ```
  [INSTALL_DIR]/scripts/StartCFS.sh
  ```

  Tip: If you want to stop a Connector Framework Server (CFS), run the following command:

  ```
  [INSTALL_DIR]/scripts/StopCFS.sh
  ```

- To start an image server, run the following command:

  ```
  [INSTALL_DIR]/scripts/StartImageServer[x].sh
  ```

> **Note:** Replace [x] with the number of your image server, for example, `StartImageServer1`.

> **Tip:** If you want to stop an image server, run the following command:
>
> `[INSTALL_DIR]/scripts/StopImageServer[x].sh`

- To start an image proxy server, run the following command:

  `[INSTALL_DIR]/scripts/StartImageDAH.sh`

  > **Tip:** If you want to stop an image proxy server, run the following command:
  >
  > `[INSTALL_DIR]/scripts/StopImageDAH.sh`

- To start an HTTP connector, run the following command:

  `[INSTALL_DIR]/scripts/StartHTTPConnector.sh`

  > **Tip:** If you want to stop an HTTP connector, run the following command:
  >
  > `[INSTALL_DIR]/scripts/StopHTTPConnector.sh`

- To start a file system connector, run the following command:

  `[INSTALL_DIR]/scripts/StartFileSystemConnector.sh`

  > **Tip:** If you want to stop a file system connector, run the following command:
  >
  > `[INSTALL_DIR]/scripts/StopFileSystemConnector.sh`

- To start an SM Service Portal content server, run the following command:

  `[INSTALL_DIR]/scripts/StartContent-SMSP.sh`

  > **Tip:** If you want to stop a Service Portal content server, run the following command:
  >
  > `[INSTALL_DIR]/scripts/StopContent-SMSP.sh`

- To start a Query Manipulation Server, run the following command:

  `[INSTALL_DIR]/scripts/StartQMS.sh`

  > **Tip:** If you want to stop a Query Manipulation Server, run the following command:
  >
  > `[INSTALL_DIR]/scripts/StopQMS.sh`

3. After installation, you can modify the following configuration files to change the previous settings:

- Smart Analytics main server: <*Smart Analytics Installation*>/IDOL/IDOLServer.cfg
- Image server: <*Smart Analytics Installation*>/ImageServer#/ImageServer#.cfg
- Image proxy server: <*Smart Analytics Installation*>/ImageProxyServer/dah.cfg

  This is only required if you have installed multiple image servers in the distributed mode.
- Content server: <*Smart Analytics Installation*>/Content#/Content#.cfg
- CFS server: <*Smart Analytics Installation*>/CFS/CFS.cfg
- HTTP connector: <*Smart Analytics Installation*>/HTTPConnector/httpconnector.cfg
- File system connector: <*Smart Analytics Installation*>/FileSystemConnector/filesystemconnector.cfg
- Portal content: <*Smart Analytics Installation*>/Content-SMSP/Content-SMSP.cfg
- Query Manipulation Server: <*Smart Analytics Installation*>/QMS/QMS.cfg

> **Note:** If you installed any connectors, you may need edit their configuration files manually. For more information, see "Configure connectors" on page 293.

Restart the corresponding components after you modify the related configuration files.

> **Tip:** If you want to uninstall SM Smart Analytics, see "Uninstall Smart Analytics" on page 307.

Example: Deploying Smart Analytics on multiple servers

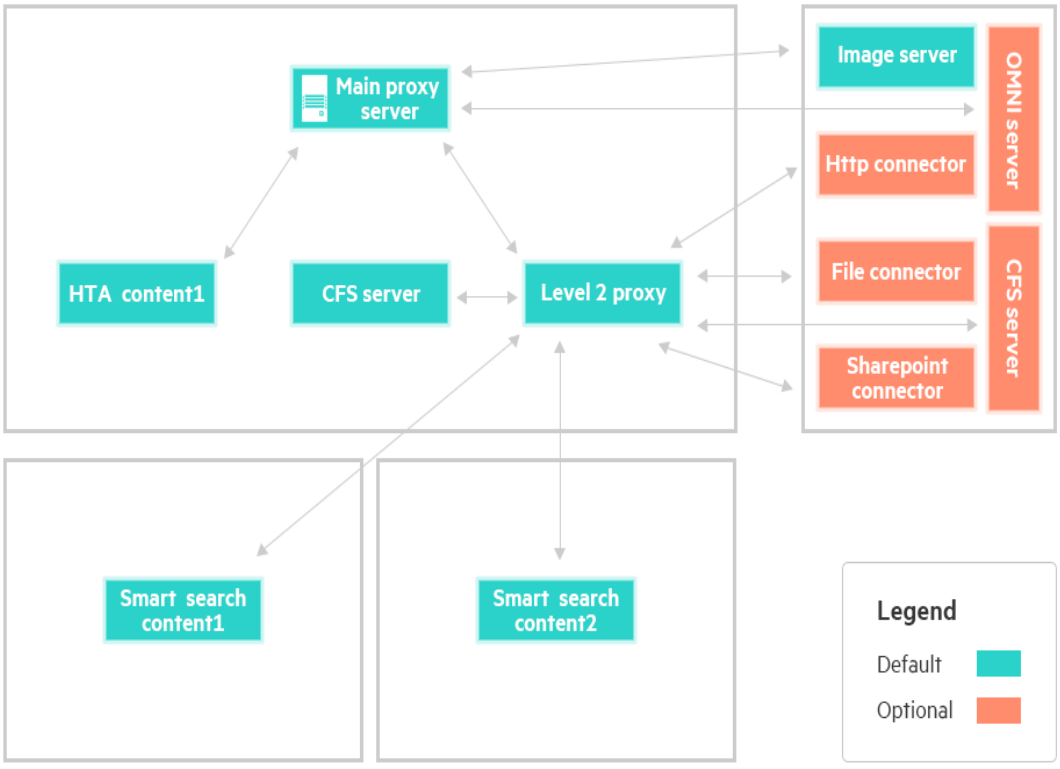
This section provides an installation example for typical large enterprise environment. The example describes how to deploy Smart Analytics on four physical servers with an architecture as follows:

- Server 1 (Smart Search Content 1, default port number 30010)
- Server 2 (Smart Search Content 2, default port number 30020)
- Server 3 (Main Server)
  - Main proxy server (default port number 9000)
  - Level 2 proxy server (default port number 20010)

- HTA content server (default port number 10010)
- CFS server (default port number 7000)

- Server 4 (Image server and other optional components)
  - Image server (default port number 18000)
  - CFS server (default port number 7000)
  - OMNI group server (default port number 5057)
  - File system connector (default port number 1234)
  - HTTP connector (default port number 5678)
  - Sharepoint connector (default port number 36000)

The following diagram provides a graphical illustration of the architecture in this example:



To deploy Smart Analytics on four physical servers, follow these steps:

1. On the first machine, install the first Smart Search Content server.
    a. Run the Smart Analytics installer.
    b. Follow the on-screen instructions until you see the Select Installation Type page. Select **Advanced Install**.
    c. Specify SM Server IP.
    d. On the Choose Distributed Components page, select **Distributed Content Server** from the **Install Template** drop-down list.
    e. Specify Smart Analytics main server IP, which is the IP address of the machine where you plan to install the main server.
    f. Specify the number of content servers to 1.
    g. Specify the content server ports.
    h. Confirm the Pre-Installation Summary and start the installation.
2. On the second machine, repeat the steps above to install the second Smart Search Content server.
3. On the third machine, install the main server.
    a. Run the Smart Analytics installer.
    b. Follow the on-screen instructions until you see the Select Installation Type page. Select **Advanced Install**.
    c. Specify SM Server IP.
    d. On the Choose Distributed Components page, select **Customize** from the **Install Template** drop-down list.
    e. Select **Proxy Server Components** and **CFS Server**, which contain components for IDOL server, level2proxy server and CFS Server.
    f. Select **Main Content**.
    g. Specify remote server IPs, separating with commas.
    h. Follow the on-screen instructions to continue the configuration steps.
    i. Confirm the Pre-Installation Summary and start the installation.
4. On the fourth machine, install the rest components.
    a. Run the Smart Analytics installer.
    b. Follow the on-screen instructions until you see the Select Installation Type page. Select

Advanced Install.

c. Specify SM Server IP.

d. On the Choose Distributed Components page, select **Customize** from the **Install Template** drop-down list.

e. Select the following components:

- Image server
- CFS server
- OMNI group server
- File connector
- HTTP connector
- Sharepoint connector

f. Specify the Smart Analytics main server IP, which is the IP address of the machine where you have installed the main server.

g. Follow the on-screen instructions to continue the configuration steps.

h. Confirm the Pre-Installation Summary and start the installation.

For more information about configuring Smart Analytics, see•"Install Smart Analytics" on page 242.

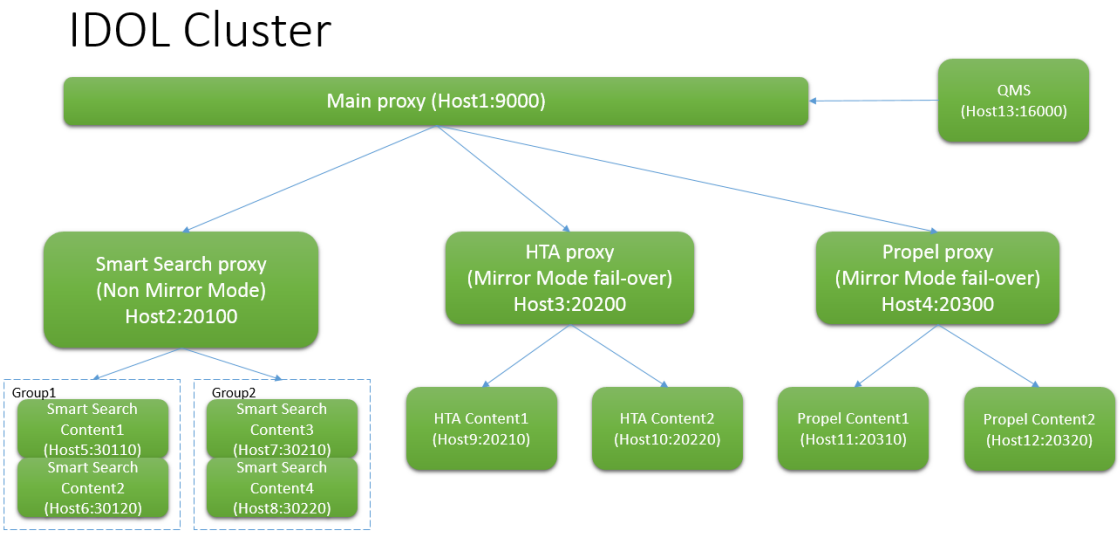
Configure Smart Analytics for high availability

This section provides instructions for you to configure Service Manager Smart Analytics for high availability.

Overview

To reduce potential down time, it is recommended that you configure Smart Analytics for high availability. The following diagram is an example architecture of Smart Analytics configured for high

availability:



In this diagram:

- Propel content2 is the failover content of Propel Content1 and vice versa.
- Smart Search content2 is the fail-over content of Smart Search content1 and vice versa.
- HTA content2 is the fail-over content of HTA content1 and vice versa.

> **Note:**
>
> - Smart Search data is distributed among groups, while content servers in a group are mirrored to each other as fail over backup. For better index and query performance, it is suggested to store no more than 3 million records for each content server. You can adjust the number of groups accordingly to fit actual scenarios. For example, if Smart Search would have 9 million records, at least 3 groups should be used for Smart Search, which means 6 content servers in total used as Smart Search content servers.
> - Propel and QMS are supported only in Smart Analytics 9.50.
> - You can configure high availability for all contents or contents of a specific component only, for example, Smart Search contents.
> - The ports are provided only for reference. You can change the ports by modifying the corresponding configuration files.
> - You can locate the proxy and QMS servers on the same machine or different machines. However, it is recommended that the rest content servers be located on different machines. For example, Host 1, 2, 3, 4 and 13 in the diagram can be the same machine, while Host 5-12 different ones.

Configuration steps

To configure Smart Analytics for high availability as depicted in the diagram, follow these steps:

1. Install and configure the proxies for high availability as needed.

   In the diagram, Smart Analytics uses four proxies to organize its contents: one main proxy and three level 2 proxies under the main proxy.

   Install and configure main proxy

   a. Install the main proxy by running the Smart Analytics installer.

   b. Select **Advanced Install**.

   c. From the Install Template drop-down list, select **Customize**.

   d. Select the **Proxy Server Components** check box with the other check boxes unchecked.

   e. Follow the on-screen instructions to finish the install.

   f. Once the installation is complete, modify the `.\IDOL\IDOLServer.cfg` file so that main proxy locates its three level 2 proxy servers, as shown below:

```
Main proxy setting:
……
[DistributionIDOLServers]
Number=3

[IDOLServer0]
Name=SmartSearch
Host=Host2
Port=20100
DistributeByFieldsValues=GlobalSearch

[IDOLServer1]
Name=Content1
Host=Host3
Port=20200
DistributeByFieldsValues=CONTENT1

[IDOLServer2]
Name=Content-Propel
Host=Host4
Port=20300
DistributeByFieldsValues=PROPEL
……
```

Install and configure the three Level 2 proxies: Smart search proxy, HTA proxy and Propel proxy

a. From the Main proxy installation location, copy the `level2proxy` folder to each of the three locations where you plan to set up the level 2 proxies. The three level 2 proxies can use the same or different hosts.

> **Note:** Copy the "level2proxy" folder to two other locations if you plan to use the original "level2proxy" as one of the three level 2 proxies.

b. Modify the corresponding configuration files of the level 2 proxies, as shown below:

- Smart search proxy:

  Modify the `< Smart Search Proxy directory>\IDOLServer.cfg` file so that the proxy locates its four content servers and arranges them as two groups with non-mirror mode, as shown below

```
Smart Search Proxy setting:
……
[DistributionSettings]
mirrormode=false
//DistributeOnBatch=true //To send documents in batches
//DIH settings:
DistributeByReference=true
UseConsistentHashing=true
//DAH setting:
SimpleCombinatorMode=true
DistributionMethod=0

[ConsistentHashing]
//number of virtual nodes
VirtualNodes=4096
//The number of copies (that is, the value of Replicas plus one) must be
smaller than number of DistributionIDOLServers.
Replicas=0

//This section is equivalent to the [engines] section in the DAH and DIH
standalone configuration
[DistributionIDOLServers]
Number=2

[IDOLServer0]
Host=Host5,Host6
Port=30110,30120
……
[IDOLServer1]
```

```
Host=Host7,Host8
Port=30210,30220
……
```

- HTA proxy:

  Modify the `<HTA proxy directory>\IDOLServer.cfg` file so that the proxy locates its two content server as mirror mode, as shown below:

```
HTA proxy setting:
……
[DistributionSettings]
mirrormode=true
//DistributeOnBatch=true //To send documents in batches
//DIH settings:
//DistributeByReference=true
//UseConsistentHashing=true
//DAH setting:
//SimpleCombinatorMode=true
DistributionMethod=0
//[ConsistentHashing]
//number of virtual nodes
//VirtualNodes=4096
//The number of copies (that is, the value of Replicas plus one) must be
smaller than number of DistributionIDOLServers.
//Replicas=0

//This section is equivalent to the [engines] section in the DAH and DIH
standalone configuration
[DistributionIDOLServers]
Number=2

[IDOLServer0]
Host=Host9
Port=20210
……
[IDOLServer1]
Host=Host10
Port=20220
……
```

- Propel proxy:

  Modify the `<Propel proxy directory>\IDOLServer.cfg` file so that the proxy locates its two content server as mirror mode, as shown below:

```
Propel proxy setting:
……
[DistributionSettings]
mirrormode=true
//DistributeOnBatch=true //To send documents in batches
//DIH settings:
//DistributeByReference=true
//UseConsistentHashing=true
//DAH setting:
//SimpleCombinatorMode=true
DistributionMethod=0
//[ConsistentHashing]
//number of virtual nodes
//VirtualNodes=4096
//The number of copies (that is, the value of Replicas plus one) must be
smaller than number of DistributionIDOLServers.
//Replicas=0

//This section is equivalent to the [engines] section in the DAH and DIH
standalone configuration
[DistributionIDOLServers]
Number=2

[IDOLServer0]
Host=Host11
Port=20310
……
[IDOLServer1]
Host=Host12
Port=20320
……
```

2. Install and configure failover content servers by using the Smart Analytics installer or copying existing ones of Smart Analytics, as described below:

   Install four content servers for Smart Search on four machines by performing either of the following:

   a. On each of four machines, run the Smart Analytics installer and select **Advanced Install**. Then, from the Install Template drop-down list, select **Distributed Content Server**, and then select the **Content Server** check box.

   b. From the Smart Analytics installation directory, copy the `Content2`/`Content3`, `modules` and `langfiles` folders, as well as the `synonym.txt` file to each of the four machines. After these copied, you should remodify all four content servers' configuration files by correcting the ports and all related file location paths of `modules`, `langfiles` and `synonym.txt`.

Install two content servers for HTA on two machines by performing either of the following:

a. On each of four machines, run the Smart Analytics installer and select Advanced Install. Then, from the Install Template drop-down list, select Distributed Content Server, and then select the Content Server check box.

b. From the Smart Analytics installation directory, copy the `Content1`, `modules` and `langfiles` folders, as well as the `synonym.txt` file to each of the two machines. After these copied, you should remodify both content servers' configuration files by correcting the ports and all related file location paths of `modules`, `langfiles` and `synonym.txt`.

Install two content servers for Propel on two machines by performing either of the following:

a. On each of two machines, run the Smart Analytics installer and select Advanced Install. Then, from the Install Template drop-down list, select Distributed Content Server, and then select the Content Server check box.

b. From the Smart Analytics installation directory, copy the `Content-SMSP`, `modules` and `langfiles` folders, as well as the `synonym.txt` file to each of the two machines. After these copied, you should remodify both content servers' configuration files by correcting the ports and all related file location paths of `modules`, `langfiles` and `synonym.txt`.

Set up Smart Analytics for Service Manager Service Portal

> **Note:** Before you install the SM Smart Analytics servers, make sure that your servers meet the system requirements as specified in "System requirements" on page 247.

Starting from Service Manager9.50, you can set up Smart Analytics to be the search engine for the Service Manager Service Portal. The following section provides two scenarios:

- If you plan to use Smart Search for Service Portal, see "Use full Smart Analytics for Service Manager Service Portal" on the next page.
- If you do not want to use Smart Search for Service Portal, see "Use Service Manager Service Portal without Smart Analytics" on page 280. In this case, KM search uses the Solr search engine and you only install components that are required for the portal search.

Use full Smart Analytics for Service Manager Service Portal

1. Run the Smart Analytics installer, and select **Advanced Install** as your installation type.
2. On the Choose Distributed Components page, select Basic for SM Service Portal from the **Install Template** drop-down list.
3. Follow the on-screen instructions to finish the installation. For detailed information about the configuration steps, see "Install Smart Analytics on Windows" on page 249.
4. Required components for both Smart Analytics and Service Portal search are installed.

   In <*Smart Analytics Installation*>/IDOL/IDOLServer.cfg, you should find the following configurations:

```
[DistributionIDOLServers]
Number=3

[IDOLServer0]
Name=SmartSearch
Host=<Smart Search Proxy Host IP>
Port=<SMART SERARCH PROXY PORT>
DistributeByFieldsValues=GlobalSearch

[IDOLServer1]
Name=Content1
Host=<MAIN CONTENT IP>
Port=<MAIN CONTENT PORT>
DistributeByFieldsValues=CONTENT1

[IDOLServer2]
Name=Content-Propel
Host=<PORTAL CONTENT IP>
Port=<PORTAL CONTENT PORT>
DistributeByFieldsValues=PROPEL
```

Use Service Manager Service Portal without Smart Analytics

1. Run the Smart Analytics installer, and select **Advanced Install** as your installation type.
2. On the Choose Distributed Components page, select Basic for SM Service Portal from the **Install Template** drop-down list, and then clear the check boxes for Image Server and CFS Server.

   > **Tip:** You can also manually delete the following folders after installation to save resources:
   >
   > - <*Smart Analytics Installation*>/level2proxy
   > - <*Smart Analytics Installation*>/Content2
   > - <*Smart Analytics Installation*>/Content3

3. Follow the on-screen instructions to finish the installation. For detailed information about the configuration steps, see "Install Smart Analytics on Windows" on page 249.
4. Required components for Service Portal search are installed.

   In <*Smart Analytics Installation*>/IDOL/IDOLServer.cfg, you should find the following configurations:

```
[DistributionIDOLServers]
Number=2

[IDOLServer0]
Name=Content1
Host=<MAIN CONTENT IP>
Port=<MAIN CONTENT PORT>
DistributeByFieldsValues=CONTENT1

[IDOLServer1]
Name=Content-Propel
Host=<PORTAL CONTENT IP>
Port=<PORTAL CONTENT PORT>
DistributeByFieldsValues=PROPEL
```

Enable Smart Analytics in Service Manager

User Role: Administrator

To enable Smart Analytics in Service Manager and set up connections, follow these steps:

> **Note:** If you want to set up an SSL connection, search for "Configure TSL/SSL for two-way authentication" in the Service Manager Help Center.

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration**.
2. Click the **Enable Smart Analytics** button to enable Smart Analytics.

   After you click this button, a message is displayed to state that once you migrate to IDOL, you cannot use SOLR as the search engine any more and you have to log out and re-log in to Service Manager before Smart Analytics is applied.
3. Click **Yes** to migrate to IDOL. Your account logs out automatically and you need to re-log in to Service Manager.
4. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration**.
5. Enter the address and port for Smart Analytics server, and then click **Test Connection**.
6. Enter the address and port for the default CFS server, and then click **Test Connection**. This default CFS server is used for Service Manager attachment index.
7. Enter the address and port for the Image Server, and then click **Test Connection**.
8. Click **Save**.

   Once you click **Save**, all the Service Manager Integration Suite tasks for the Smart Analytics integration are automatically started.

Configure Smart Analytics in Service Manager

To configure Smart Analytics in Service Manager, follow these steps:

1. Set up data cleansing configuration. See "Configure data cleansing" on the next page.
2. Configure Smart Ticket. See "Configure Smart Ticket" on page 286.
3. Configure Hot Topic Analytics. See "Configure Hot Topic Analytics" on page 292.
4. Set up smart search connectors. See "Configure connectors" on page 293.
5. Configure Smart Search. See "Configure Smart Search" on page 303.
6. Add the "idol.assistant" capability word to the operator records. See "Add Smart Analytics capability word for power users" on page 306.

Configure data cleansing

User Role: Administrator

The purpose of data cleansing is to remove unwanted contents from the Smart Analytics source data set that is used to train and index into Smart Analytics as well as in runtime processing.

> **Note:**
>
> - For Smart Ticket and Hot Topic Analytics features, data cleansing is only applied to the "Title Field" or "Content Fields" that are defined in configurations.
> - For Smart Search, data cleansing can be applied to any field individually which you can configure. For detailed information, search for "Managing Smart Search Knowledgebases" in the Service Manager Help Center.
> - All modification for data cleansing will take effect from next round of indexing.

To add a data cleansing configuration, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Data Cleansing**.
2. Select a module. For example, Interaction.

   > **Note:** In the module drop-down list there is a Global option. This means that it's a global data cleansing record for all modules which are using Hot Topic Analytics and Smart Ticket.

3. Select one of the following actions:
   - **Remove**: Remove the matched texts and index the rest to SM Smart Analytics.
   - **Include**: Extract and index the texts between the start pattern and the end pattern exclusively.
   - **Exclude**: Exclude the texts that match the pattern (including start, end, and all the words between them) and index the rest to SM Smart Analytics.
   - **ExtractFromTemplate**: Extract the content from template that is configured as regular expressions. The capturing groups that are matched by the Regular Expressions are extracted and returned.
4. Enter the text or pattern for the action that you selected. For the **Remove** action, you only need to type the text string to be removed. For the **Include** and **Exclude** actions, the start pattern is the

text string that you need to specify while the end pattern can be one of these options: a text string that you specify, end of line, or end of document.

The processing of the **ExtractFromTemplate** action is of first priority. The Data cleansing actions are processes in the following order:

a. **ExtractFromTemplate**

   If there are matched texts found, then return. Otherwise, perform the **Include** action.

b. **Include**

   If there are matched texts found, then perform the **Remove** action. Otherwise, perform the **Exclude** action..

c. **Exclude**

   If there are matched texts found, then perform the **Remove** action.

d. **Remove**

To learn how the text or pattern takes effect, see the following examples.

- Example of the **Remove** action:

Original content	`[telephone communication history with customer]: Microsoft Office keeps asking for installation of additional components / language packs.`
Specified text to be removed	`[telephone communication history with customer]:`
After cleansing	`Microsoft Office keeps asking for installation of additional components / language packs`

- Examples of the **Include** action:

Original content	`Description of the issue:`
	`Sent items are not being sent by Outlook.`
	`Actions suggested by help desk agent:`
	`asked customer to check network connection status,`
	`shows connection is OK`

Start pattern	`description of the issue:`
End pattern	`actions suggested by help desk agent:`
After cleansing	`Sent items are not being sent by Outlook.`

Original content	Description of the issue: Items are not sent by Outlook. Actions suggested by help desk agent: asked customer to check network connection status, shows connection is OK
Start pattern	description of the issue:
End pattern	**End of line**
After cleansing	Items are not sent by Outlook.

Original content	Description of the issue: Sent items are not being sent by Outlook. Actions suggested by help desk agent: asked customer to check network connection status, shows connection is OK
Start pattern	description of the issue:
End pattern	**End of document**
After cleansing	Sent items are not being sent by Outlook. Actions suggested by help desk agent: asked customer to check network connection status, shows connection is OK

- Examples of the **Exclude** action:

Original content	SQL Server is down and cannot be restarted. [appendix: error log] Details: Xxxxxxxxxxxxxxx [end of appendix]
Start pattern	[appendix: error log]
End pattern	[end of appendix]
After cleansing	SQL Server is down and cannot be restarted.

Original content	SQL Server is down and cannot be restarted. [appendix: error log] Details: Xxxxxxxxxxxxxxx [end of appendix]

Start pattern	`[appendix: error log]`
End pattern	**End of line**

After cleansing	`SQL Server is down and cannot be restarted.`
	`Xxxxxxxxxxxxxxx`
	`[end of appendix]`

Original content	`SQL Server is down and cannot be restarted.`
	`[appendix: error log] Details:`
	`Xxxxxxxxxxxxxxx`
	`[end of appendix]`

Start pattern	`[appendix: error log]`
End pattern	**End of document**
After cleansing	`SQL Server is down and cannot be restarted.`

- Example of the **ExtractFromTemplate** action:

Example configuration	Brief description of the problem: ([^]*)FirstName:([^]*)LastName:([^]*)Phone:([^]*)
Data before cleansing	**Brief description of the problem**: The user called because he could not access to eDocs. The user was able to find the eDocs administrator but that person does not work for the company anymore First Name : Herr Maximo Christian Last Name : Graf Phone : 01 234 567
Data after cleansing	The user called because he could not access to eDocs. The user was able to find the eDocs administrator but that person does not work for the company anymore Herr Maximo Christian Graf 01 234 567

Note: Regular expression is supported only for the **ExtractFromTemplate** action.

5. Select the **Match Case** check box if you only want to find the texts that match the case of the text or pattern that you entered.

6. Select the **Active** check box to activate this configuration.
7. Click **Add**. The new data cleansing configuration is now added.

Configure Smart Ticket

User Role: Administrator

Smart Ticket provides the following two out-of-box Smart Ticket (auto-classification) configurations:

- Standard category field
- Service category field

These out-of-box configurations are best practices based on the out-of-box data. You can use or modify these configurations, or you can add new configurations that best reflect your business needs.

Add a new Smart Ticket task

In the out-of-box system, two Smart Ticket configuration tasks ("Standard category field" and "Service category field") are used for Smart Ticket by default. You can choose to use these out-of-box Smart Ticket tasks, or you can create new Smart Ticket tasks.

To add a new Smart Ticket task, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Select **Blank** from the drop-down list, and then click **Add**.

   > **Note:** You can also select one of the out-of-box templates ("Category" or "Affected Service") from the drop-down list, and then click **Add** to create a new Smart Ticket task based on the template.

3. Type the task name for the new Smart Ticket configuration.
4. Go to the **Configurations** tab.
5. Select a module for auto-classification. For example, Interaction.
6. In the **Training Sample Query** field, define a query to refine the sample data. The default value is `category~="service catalog"`, which means the data that is not in the "service catalog"

category can be selected as the training samples.

7. Select the target fields to be automatically filled by SM Smart Analytics. You can select up to three levels. For example, Category, Subcategory, and Area.
8. Select the source fields that the auto-classification is based on. For example, title and description.
9. In the **Training Optimization** tab, modify the settings for training optimization.

> **Note:** We recommend that you keep the default settings. For more information on improving accuracy for Smart Ticket, search for "Improving accuracy for Smart Ticket" in the Service Manager Help Center.

Setting	Description
Training Samples Per Category	The maximum records to be used as the training samples for each category. Default: 200
Test Data Coverage	The percentage of records out of the total source data that are used to test the trained system. Default: 5
Source Data Coverage	The percentage of records out of the total source data that are used to train the system. Default: 90
Training Method	◦ Choose "use best terms" for a faster training process if you have huge data volume. ◦ Choose "use training documents" for a higher accuracy with a slower training process. Default: use training documents
Adjust Term Weight From Test Result	Select this option to automatically adjust the term weight for some terms in some categories based on testing result. Default: Disabled
Remove Low Weight Document	After the training is finished by using the "training documents" method, check the weight of every training document, and then remove the low-weight training documents from the training sample pool. Default: Disabled **Weight Threshold** The threshold to remove the low weight training documents, after finish training by using the "training documents" training method.

Setting	Description
	Min Number of Training Samples The minimum number of the training documents in a category. Use this parameter to ensure that a certain number of training samples will not be removed when the system removes the low weight training documents.

10. Click **Add**. The new auto-classification task is now added to the **Current Configuration List**.
11. Modify the Smart Ticket form (idol.quick.new.interaction) to use the new Smart Ticket task that you just created.

> **Note:** This step is only required for operators to create Smart Interaction from index.do. The new auto-classification task will take effect directly on the user requests from SRC and ESS after a training is performed.

Perform training and testing

To perform a training for a Smart Ticket task, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click the task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
3. Click the **Training** button to start training this auto-classification.

> **Tip:** You can click **Refresh Status** to view the latest training status.

4. When the training is done, click **Testing**. When the testing is finished, you can view an estimated result of the accuracy for this auto-classification in the **Testing Result** field.

> **Note:** Smart Analytics does not support duplicated category names that are different only in text cases (For example, two categories named as "AVAILABILITY" and "availability"). If such categories exist during the training, the system logs an error and aborts the training process.

> **Tip:** The quality of the sample data is critical to the accuracy of the auto-classification. To refine your sample data, you can define a query in the **Training Sample Query** field under the **Configurations** tab. For more best practices to improve accuracy, search for "Improving accuracy for Smart Ticket" in the Service Manager Help Center.

> **Tip:** If you disable or enable the Multi-Company mode for Service Manager, you need to delete the

existing Smart Ticket configuration tasks and re-create them before you perform training.

Apply a rule-based training

You can append the rule-based analysis on top of the meaning based analysis. The typical scenario is that if one particular record has the same relevancy within several categories, you can append a rule to one specific category to improve the categorization accuracy.

"Rule Field Name" is where you can specify the field based on which you define the rule.

"Apply Rule" lists all the categories, where you can choose the target category and set the value for the rule you want to append.

For example, suppose there are two affected services, "printer_San Diego" and "printer_Shanghai". You can define the rule field as "Primary Contact Location City". Then, set value "San Diego" to the "printer_San Diego", and set value "Shanghai" to the "printer_Shanghai". With this rule, if the contact person for the new coming record is from the San Diego office, the record will be automatically filled with "printer_San Diego" as the affected service.

To apply a rule-based training for an auto-classification, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
3. Go to the **Rule Base** tab.
4. In the **Rule Field Name** field, specify the field name based on which you define the rule.
5. Click **Apply Rule**, and then click **Search**. A list containing all the categories appears, where you can choose the target category and set the value for the rule that you want to apply.
6. Click a category.
7. In the **Rule Field Value** field, set the value for the rule that you want to apply.
8. Click the **Apply Rule** button.

Perform tuning in the Smart Ticket definition

Another way to improve the accuracy of Smart Ticket is to perform tuning continually for the Smart Ticket definition.

To perform tuning in the Smart Ticket definition, follow these steps:

1. Service Desk agents select tuning candidates during their daily work:
   a. In an interaction record, update the fields suggested by Smart Ticket if the suggested values are incorrect, such as category or affected service.
   b. After the interaction is closed, from the interaction record, click **More** > **Add to Tuning Records** to add this record as a tuning candidate for Smart Ticket.

   > **Note:** The **Add to Tuning Records** option is only available when an interaction is in the "Closed" status.

2. A system administrator tunes Smart Ticket after a period of time to increase the accuracy:
   a. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
   b. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
   c. Go to the **Tuning** tab.
   d. Click **Manage Tuning Records** to open **Tuning Records** where you can find all the tuning candidates.
   e. Delete the meaningless or inappropriate records. The rest of records will be used in tuning Smart Ticket.
   f. Click the **Tuning** button to start the tuning process.

Configure Smart Ticket for multi-company

SM Smart Analytics supports multi-tenancy. When multi-company mode is enabled in Service Manager, you can configure specific Smart Ticket task to apply to multiple companies when applicable. The Smart Ticket configuration takes effect on these companies individually by segregating their data in Smart Analytics database.

To specify the companies in a Smart Ticket configuration, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. Click a task name of a Smart Ticket configuration. The **Smart Ticket Task** screen appears.
3. Click the **Multiple Company** tab, and then do one of the following:

- Click **Add Company** to add companies to this configuration.

  > **Note:** A training is needed if you add a new company.

- Click **Remove Company** to remove companies from this configuration.

> **Tip:** If you are unable to see the **Multiple Company** tab, search for "Troubleshooting: Smart Analytics setup" in the Service Manager Help Center.

> **Note:** Mandanten in Smart Ticket supports only multiple company.

Configure Smart Ticket for OCR

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
2. From the toolbar, click **More** or the **More Actions** button, and then select **Tailoring**. The Smart Ticket Settings page opens.
3. Update the following fields as needed.

Field Name	Description
Use FFT (Fast Fourier Transform) to remove the grid noise during OCR	The default value is true. When selected, the system uses Fast Fourier Transform (FFT) to remove the grid noise during OCR. However, using FFT consumes around 400 MB memory for each image and makes the OCR process slower. You can disable this feature if you want to speed up the system performance.
Maximum image size allowed to perform OCR without resizing (pixel):	The default value is 2000 pixels. It is recommended that you keep the default value unchanged. Specifies the maximum pixels of an image that is allowed to perform OCR without resizing. Images that larger than the specified value will be resized before Smart Analytics performs OCR.
The images size after resizing (pixel):	The default value is 700 pixels. Specifies the number of pixels to which an image is re-sized when the image size exceeds the maximum image size allowed to perform OCR without resizing.

	To ensure best OCR quality, the recommended value for this field is from 600 to 1200.

Configure Hot Topic Analytics

User Role: Administrator

To configure Hot Topic Analytics, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**.
2. Select and open a Hot Topic Analytics configuration record from the configuration list. For example, Incident.

   > **Note:** In the out-of-box system, four Hot Topic Analytics configuration records are provided (for the Interaction, Problem, Incident, and Survey modules). If you want to add a new Hot Topic Analytics configuration for another module, select a file from the **Add Configuration** drop-down list, and then click **Add**. For more information, search for "Enable Hot Topic Analytics for other modules" in the Service Manager Help Center.

3. From the **Analytic Corpus** tab, modify the following settings as needed:
   - **Index Condition**: Define a query to specify the records that you want to include in Hot Topic Analytics.
   - **Title Field**: Select a field to define the title when viewing an individual record in Hot Topic Analytics. The title field is also an important data source for hot topic hunting.
   - **Contents Fields**: Select the data source for Hot Topic Analytics. Be sure to use only text fields such as description and solution.
4. From the **Filter Fields** tab, modify the following settings as needed:
   - **Timestamp Field**: Select a field to indicate the time stamp for filtering.
   - **Properties Fields**: Select fields that can be used for advanced filtering in Hot Topic Analytics. For example, you can define Category, Priority, or Source as a filter.
5. From the **Advanced** tab, modify the following settings as needed:
   - **Expiry Day**: Hot Topic Analytics removes the data that was indexed earlier than the setting in this field from its analysis.

- **Max Return Results**: Define the maximum number of records returned from Hot Topic Analytics.
- **Group By**: Specify the field that is used to group the records as the last level in the hot topic map.
- **Analytics Action**: Specify the query condition for the analytics action.

> **Note:** In the out-of-box system, the **Analytics Action** setting is only available in the Hot Topic Analytics configuration record for incidents with the following three action queries: Set Parent, Create Problem, and Create Change/Article. If you want to add more custom action queries in the **Analytics Action** section, search for "Add more "Analytics Action" in the Hot Topic Analytics for Incidents" in the Service Manager Help Center.

6. Click **Save** to save your modification.
7. Click the **Start Index** button to start indexing.

> **Tip:** You can click the **Refresh Status** button to refresh the index status.

Configure connectors

User Role: Administrator

To enable search actions among different data sources, you need to configure different connectors and servers, and monitor their working status. You can get the URL information from the respective .cfg file of the connectors after you have configured them on your servers.

Configure SharePoint Connector

To configure SharePoint Connector, follow these steps:

1. Make sure that the OMNI Group Server and SharePoint Connector components were included when Smart Analytics was installed.

> **Note:** You can install OMNI Group Server and SharePoint connector either along with other components by using the All in One install template, or install them separately by using the Customize install template through advanced installation. For more details, see Advanced Installation in "Install Smart Analytics" on page 242

2. Go to <*Smart Analytics Installation*>/SharepointRemoteConnector, locate the `SharepointRemoteConnector.cfg` file, and then configure the `[FetchTasks]` and `[MyTask]` sections as needed.

Example:

```
[FetchTasks]
Number=1
0=MyTask

[Default]

[MyTask]
SharepointOnline=false
SharepointUrlType=SiteCollection
SharepointUrl=http://<SharePoint URL>/
Username=<username>
Password=<password>

IndexSites=true
IndexLists=true
IndexFolders=true
IndexAttachments=true
IndexUserProfiles=false
MappedSecurity=true
EncryptACLEntries=true
//Domain=DOMAIN
IncludeProviderNameInACLs=true
GroupServerDebugOutputFile=SynchronizeGroupsDEBUG.log
ScheduleCycles=-1
UseEmailAsGroupName=true
```

3. Restart your SharePoint Server.
4. If you want to use OMNI Group Server, continue the following steps:

   a. Go to <*Smart Analytics installation*>/OmniGroupServer, locate the `OmniGroupServer.cfg` file, and then configure the `[LDAP]` and `[Sharepoint]` sections as needed

      Example:

      ```
      [LDAP]
      ActiveDirectory=True
      GroupServerLibrary=ogs_ldap.dll
      //GroupServerCycles=1
      LDAPServer=abc.asciapacific.example.net
      LDAPPort=389
      LDAPUserBase=OU=CN,OU=Users,OU=Accounts,DC=asicapacific,DC=example,DC=net
      LDAPGroupBase=CN=PDL@example.com, OU=Managed
      Groups,OU=Accounts,DC=asicapacific,DC=example,DC=net
      //UserFilter=(objectClass=<objectClass>)
      //GroupFilter=(objectClass=<objectClass>)
      LDAPUsername=user@example.com
      ```

```
LDAPPassword=<password>

ExtractDomainFromDN=true
LDAPMode=Group
PageSize=10000
KeyUserName=sAMAccountName
LDAPEnableReverseLookup=true

[SharePoint]
GroupServerJobType=Connector
ConnectorHost=<ConnectorHost>
ConnectorPort=36000
ConnectorTask=MyTask
```

> **Note:** Make sure that the value of `ConnectorTask` is consistent with `<TaskName>` in the `[FetchTasks]` section of the `SharepointRemoteConnector.cfg` file.

b. Go to <*Smart Analytics installation*>/IDOL, locate the `IDOLServer.cfg` file, uncomment `GroupServerHost` and `GroupServerPort`, and then specify OMNI Group Server Host and Port as needed.

Example:

```
[SharePoint]
//Authentication
Library=C:\Program Files (x86)\HPE\Service Manager
9.50\SmartAnalytics/modules/user_ldapsecurity
V4=TRUE
EnableLogging=TRUE
DocumentSecurity=true
CaseSensitiveUserNames=False
CaseSensitiveGroupNames=False
SecurityFieldCSVs=username,group
DocumentSecurityType=SharePoint
GroupServerHost=<GroupServerHost>
GroupServerPort=5057
GroupServerRepository=Combine
//SyncRolesFromGroups=true
EnableLogging=TRUE
EscapedEntries=true
```

c. Restart the Smart Analytics Server and the OMNI Group Server.

5. Log on to Service Manager, and then click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The Smart Search configuration page appears.
6. Click the **Connector Configuration** link to open the connector configuration page.
7. From the **CFS Server** tab, a list of all CFS server URLs is provided. You can click the **Refresh**

Status button to refresh the URL list. Connectors need CFS servers to transfer data, so after you add a new connector, the corresponding CFS server information is added to this list.

> **Note:** If there two or more connectors that are installed on the same machine and share one CFS server, there is no new URLs added to the list.

8. Go to the **SharePoint Connector** tab, perform the following actions:
   - **Add a SharePoint connector**: Type a configured SharePoint connector URL here, for example: http://192.168.255.255:36000/. You can click **Test connection** to test the URL connection status, and then click **Add** to add this URL to the current list.

     > **Note:**
     > - The "/" at the end of the URL is mandatory.
     > - Make sure the status for SharePoint is online.
     > - To get the URL information for the SharePoint connector you have configured, check the following configuration file:
     >
     >   <*Smart Analytics Installation*>/SharepointRemoteConnector/SharepointRemoteConnector.cfg

   - **sAMAccountName Field**: Choose the field type from the drop-down list. This field is the mapping field of SharePoint and SM users.

     If SharePoint on premise is used, configure this field to the domain account field of the SM operator table.

     If SharePoint Online is used only, there is no need to set this field as operator email field is used for user mapping.

   - **Delete**: Select a SharePoint connector URL and then click this button to delete it from the list.
   - **Refresh Status**: Click to refresh the status of the URL list.
9. From the **OMNI Group Server** tab, a Repository list of all OMNI group servers is provided. OMNI Group Server provides the LDAP configuration information which may be required for SharePoint login. You can also check the target task of a repository and its working status. You can click the **Refresh Status** button to refresh the URL list.
10. (For Security SharePoint), go to <*Smart Analytics installation*>/OmniGroupServer, locate the `OmniGroupServer.cfg` file, and specify `FiledName0` to the option you selected for the **sAMAccountName** Field.

    ```
    ExtractDomainFromDN=true
    LDAPMode=Group
    ```

```
PageSize=10000
KeyUserName=sAMAccountName
LDAPEnableReserveLookup=true

KeyGroupName=mail
KeyMember=member
LDAPDebugLogging=TRUE
FieldKey0=sAMAccountName
FieldName0=Email
FieldKey1=mail
FieldName1=mail
FieldKey2=cn
FieldName2=cn
GroupServerMaxDatastoreQueue=100000
//remove domain prefix for groups
GroupServerOp0=StartAfter
GroupServerOpParam0=0;\
GroupServerOpApplyTo0=GROUP
//Just to avoid unnecessary queries for members that don't exist.
//This might not have any effect if the group members are properly managed.
DisableUserFromDNSearch=TRUE
DisableGroupFromDNSearch=TRUE
```

11. Restart the Omni Group server.
12. Do the following to add a splib library for the sharepoint connector:
    a. go to Smart Search Configuration page.
    b. Specify Knowledgebase Name,
    c. Select splib for **Type**
    d. Click **Add**.
13. The Knowledgebase Maintenance page appears.
14. Specify **Connector** and **Task**, and then select the **Do not use OmniGroupServer for access count** check box.
15. Click **Save**.
16. Click **Full Reindex** and **Refresh Status**.
17. You can perform the search when the status changes to Indexing and Doc Count for SharePoint is greater than 1.

> **Note:** Log off and then log back on to your Service Manager if you can not find library in your Smart Search library list.

Configure HTTP Connector

To configure the HTTP Connector, follow these steps:

1. Make sure that the httpconnector component was included when Smart Analytics was installed.

   > **Note:** You can install httpconnector either along with other components by using the All in One install template or install the connector separately by using the Customize install template through advanced installation. For more details, see section of Advanced Installation in "Install Smart Analytics" on page 242

2. Go to <*Smart Analytics Installation*>/HTTPConnector, locate the `httpconnector.cfg` file, and then configure the `[FetchTasks]` and `[MYSITE]` sections as needed.

   Example for one task:

   ```
   [FetchTasks]
   Number=1
   0=MYSITE

   [MYSITE]
   URL=http://MYSITE.com
   DIRECTORY=HTTPconnector
   CantHaveCSVs=*.css,*.js
   CantHaveCheck=1
   //StayOnSite=True
   //Depth=99
   ProxyHost=<ProxyHost>
   ProxyPort=8080
   //FOLLOWROBOTPROTOCAL=FALSE
   //----Login with form----
   //LOGINMETHOD=FORMPOST
   //LOGINURL=https://login.com/
   //LOGINUSERFIELD=os_username
   //LOGINUSERVALUE=USERNAME@EXAMPLE.COM
   //LGOINPASSFIELD=os_password
   //LOGINPASSVALUE=PASSWORD_ENCRYPTED
   //LoginSubmitField=ButtonID
   //----HTTP digest authentication----
   //DigestUsername=USERNAME
   //DigestPassword=PASSWORD_ENCRYPTED
   //----NTLM authentication----
   //NTLMUsername=USERNAME
   //NTLMPassword=PASSWORD
   ```

   To configure multiple tasks, for example, two tasks, configure the .cfg file as follows:

   ```
   [FetchTasks]
   Number=2
   ```

```
0=MYSITE1
1=MYSITE2

[MYSITE1]
...

[MYSITE2]
...
```

The following table describes the parameters of the `[MYSITE]` section in the httpconnector.cfg file. If you want to configure multiple tasks for one connector, you just need to copy the content in the `[MYSITE]` section and rename the section.

Parameter	Description
`URL=http://MYSITE.COM`	Use this parameter to specify the root URL of the website for web crawling.
`DIRECTORY=MYSITE`	Specify the file location to save the crawling pages.
`CantHaveCSVs=*.css,*.js`	Specify the file types which are excluded from search resources. In this example, the .css and .js files are excluded.
`CantHaveCheck=1`	Specify that the value specified in the `CantHaveCSVs` parameter must be excluded from the URL.
`//StayOnSite=False`	The web crawling does not stay on the current site and will follow the links that leave the current page.
`//Depth=99`	Specify the maximum depth to which the connector can follow links during web crawling. In this example, this parameter is commented, which means it uses the default value (3).
`//ProxyHost=PROXY.COM`	Specify the proxy URL.
`//ProxyPort=80`	Specify the proxy port.
`//FOLLOWROBOTPROTOCOL=FALSE`	Specify whether the HTTP connector follows the protocol of the website. Most websites have a robot protocol to claim which page can be fetched by the spider. If you enable this parameter, the HTTP connector will not follow the protocol.
`//----Login with form----`	Uncomment the content under this section if

Parameter	Description
	you use a login form to log in to your websites.
//LOGINMETHOD=FORMPOST	Specify that the website requires you to enter information such as the user name and password, and the form uses the POST method to send this information to the site's server.
//LOGINURL=https://login.com/	Specify the login URL.
//LOGINUSERFIELD=os_username	Specify the ID of the field in which you enter your username. You can get the ID by viewing the source of the web page.
//LOGINUSERVALUE=USERNAME@COMPANY.COM	Specify the user name.
//LOGINPASSFIELD=os_password	Specify the ID of the field in which you enter your password.
//LOGINPASSVALUE=PASSWORD_ENCRYPTED	Specify your password.
//LoginSubmitField=ButtonID	Specify the ID of the button you click to log in to your website
//----HTTP digest authentication----	Uncomment the content under this section if you use an HTTP digest authentication to log in to your website.
//DigestUsername=USERNAME	Specify the user name for HTTP digest authentication.
//DigestPassword=PASSWORD_ENCRYPTED	Specify the password for HTTP digest authentication.
//----NTLM authentication----	Uncomment the content under this section if you use NTLM authentication to log in to your web page.
//NTLMUsername=USERNAME	Specify the user name for NTLM authentication.
//NTLMPassword=PASSWORD	Specify the password for NTLM authentication.

3. Restart the Httpconnector Server.
4. Log on to Service Manager, and then click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The Smart Search configuration page appears.
5. Click the **Connector Configuration** link to open the connector configuration page.
6. From the **HTTP Connector** tab, a list of all connector URLs and their status is provided. You can

perform the following actions:

- **Add an HTTP connector**: Type a new HTTP connector URL here, for example, http://192.168.255.255:5678/. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list.

  > **Note:**
  > - The "/" at the end of the URL is mandatory.
  > - Make sure the status for SharePoint is online.
  > - To get the URL information for the HTTP connector you have configured, check the following configuration file:
  >
  >   <Smart Analytics Installation>/HTTPConnector/httpconnector.cfg

- **Delete**: Select an HTTP connector URL, and then click this button to delete it from the list.
- **Refresh Status**: Click to refresh the status of the URL list.

7. Do the following to add a weblib library for the http connector:
   a. Go to Smart Search Configuration page.
   b. Specify Knowledgebase Name
   c. Select weblib for Type,
   d. Click **Add**.
8. The Knowledgebase Maintenance page appears.
9. Specify **Connector** and **Task**.
10. Click **Save**.
11. Click **Full Reindex** and **Refresh Status**
12. You can perform the search when the status changes to Indexing and Doc Count for SharePoint is greater than 1.

    > **Note:** Log off and then log back on to your Service Manager if you can not find weblib library in your Smart Search library list.

Configure File System Connector

To configure File System Connector, follow these steps:

1. Make sure that the component File System Connector was included when Smart Analytics was installed.

> **Note:** You can install File System Connector either along with other components by using the All in One install template, or install the connector separately by using the Customize install template through advanced installation. For more details, see Advanced Installation in "Install Smart Analytics" on page 242.

2. Go to <*Smart Analytics Installation*>/FileSystemConnector, locate the `filesystemconnector.cfg` file, and then configure the `[FetchTasks]` and `[MyTask]` sections as needed.

   Example:

```
[FetchTasks]
Number=1
0=MYTASK

[MYTASK]
//specifies the interval (in seconds) between scheduled synchronize actions.
ScheduleRepeatSecs=300
//specifies whether the connector searches subfolders.
DirectoryRecursive=TRUE
//The DirectoryPathCSVs parameter specifies a comma-separated list of folders
to search for files.
DirectoryPathCSVs=\\JORA7\ShareDirectory
//A regular expression that specifies the folders to search for files. The
connector only searches folders
//that are within the location specified by DirectoryPathCSVs
//where the full path of the folder matches the regular expression
//where the full path of all parent folders (up to the folder specified by
DirectoryPathCSVs) match the regular expression.
PathCrawlRegex=.*
//A regular expression that specifies the folders to ignore. The connector
ignores any folders where the path matches the regular expression.
//If a folder is ignored, all of its subfolders are also ignored.
//PathCrawlRegex=
//The DirectoryFileMatch parameter limits the files that are retrieved by the
connector. The value of this parameter is a wildcard expression
//The filename of a file must match the wildcard expression, otherwise the file
is ignored. default to all files
DirectoryFileMatch=*.pdf,*.doc,*.ppt,*.log
```

3. Log on to Service Manager, and then click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The Smart Search configuration page appears.
4. Click the **Connector Configuration** link to open the connector configuration page.
5. From the **File System Connector** tab, a list of all connector URLs and their status is provided. You can perform the following actions:

- **Add a File system connector**: Type a new file system connector URL here, for example: http://192.168.255.255:1234/. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list.

  > **Note:**
  >
  > - The "/" at the end of the URL is mandatory.
  > - Make sure the task status is online.
  > - To get the URL information for the file system connector you have configured, check the following configuration file:
  >
  >   <Smart Analytics Installation>/FileSystemConnector/filesystemconnector.cfg

- **Delete**: Select a file system connector URL, and then click this button to delete it from the list.
- **Refresh Status**: Click to refresh the status of the URL list.

> **Note:** When the fileserver connectors (including CFS server) and the fileserver share folders are on the same machine, Service Manager supports the UNC path (DirectoryPathCSVs=\\path\to\shared\folder) by using the IE browser.

6. Do the following to add a fsyslib library for the file system connector:
   a. Go to Smart Search Configuration page.
   b. Specify **Knowledgebase Name**.
   c. Select fsylib for **Type**.
   d. Click **Add**.
7. The Knowledgebase Maintenance page appears.
8. Specify **Connector** and **Task**.
9. Click **Save**.
10. Click **Full Reindex** and **Refresh Status**

Configure Smart Search

User Role: Administrator

To configure Smart Search, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**.

   The **Smart Search Configuration** page opens.

2. From the **Add Knowledgebase** section, specify the following settings as needed:

   - **Knowledgebase name**: Specifies the name of the library you want to add.
   - **Knowledgebase type**: Specifies the type of the library you want to add.
   - **Add**: Adds the library you specified as a new knowledgebase.

     Once you click the **Add** button, the new IDOL knowledgebase record is added and a new knowledgebase maintenance page is displayed. Configure the required knowledgebase information on the maintenance page. For detailed information about different types and configuration steps of knowledgebases, search for "Manage Smart Search Knowledgebases" in the Service Manager Help Center.

3. From the **Environment Configuration** section, modify the following settings as needed:

   - **Expiry days**: Smart Search removes the data that was indexed longer than the setting in this field from search.
   - **Assign the default knowledge view group to all operators**: If this option is selected, the default knowledge view group is assigned to all operators.
   - **Connector configuration**: Click to configure and monitor the status of the connectors and servers. For detailed information, see "Configure connectors" on page 293.

4. From the **Current Knowledgebase List** section, you can check the following information.

Field	Description
Knowledgebase Name	Specifies the name of the Smart Search knowledgebase. **Note:** When the administrator adds a new library, users can only see this library available on the list after next login.
Type	Specifies the type of the Smart Search knowledgebase.
Display Name	Specifies the display name for the Smart Search knowledgebase. You can change this value from a knowledgebase details page.
Interval	Displays the current interval used to update the selected knowledgebase index. Each interval unit is 5 minutes (default). You can change this value from a knowledgebase details page.
Index Status	Displays the current index status of the library. A library has the following

Field	Description
	four index status: ◦ Offline: the library is newly added or the Smart Search server is shut down. ◦ Not started: the **Full Reindex** button is clicked for the library and the indexing is in the queue. ◦ Indexing: the indexing for the library is ongoing. ◦ Finished: the indexing for the library is finished.
Doc count	Displays the number of records in the library. The number of the records is affected by the replica settings. When a content server is disabled, the number may be incorrect before you redistribute the server data.
Last Index time	Displays the time when the libary is last indexed.
Full Reindex:	When you click the **Full Reindex** button, the IDOL search engine performs a full re-index of the selected library. However, because indexing runs as a background process, the search engine does not begin indexing until the specified refresh interval is reached. Performing a full re-index on a large knowledgebase may have a significant impact on system resources. Therefore, it is recommended that you perform a full re-index of a small amount of records in a knowledgebase, for example, records created within 90 days. For the rest of the records, you can perform incremental indexing by using the `AddToKMBUTable` ScriptLibrary. For more information, search for "Perform indexing of large-scale knowledgebases" in the Service Manager Help Center.
Refresh Status	Refreshes the index status of the knowledgebases.

To modify settings for any current knowledgebase, click the respective link from the list. For detailed information about knowledgebase settings, search for "Manage Smart Search Knowledgebases" in the Service Manager Help Center.

5. When you first install the IDOL search engine after having used the Solr search engine, you need to do the following:

   Check libraries in the **Current Knowledgebase List**. From the kmsearchsecurity script of each library, delete the code which you updated to enable Mandanten Security for libraries when using Solr, and then replace the deleted code with the following:

   ```
   function getSecurityInfo(user, record)

   {

   return "";
   ```

```
}
```

> **Note:** Starting from Service Manager 9.41, Mandanten security control is introduced as a built-in feature in Smart Search. Users no longer need to implement it manually by updating the KM search security script. If you keep the KM Search security script which was updated for Mandanten security, the built-in Mandanten control in Smart Search does not work.

6. Click **Save** to save your modification.
7. Click **Full Re-index**.
8. Log off and then log onto Service Manager for the changes to work.
9. Perform a Smart Search to verify your configuration.

   If you encounter session time out or long response time when performing the first Smart Search after indexing, set a higher value for the `TermCachePersistentKB` parameter in the `[TermCache]` section for all content server configuration files(content<N>.cfg) and then restart your content servers.

   > **Note:** The default value for this parameter is 512000. You can configure the parameter value according to system memory availability and desired querying speed. For example, if you selected All-in-one install template when deploying Smart Analytics, you can keep the default value unchanged. If you deployed your content servers on multiple machines, it is recommended you modify the value to 2097152.

Add Smart Analytics capability word for power users

User Role: Administrator

To enable power users such as Service Desk Agent or Problem Coordinator to use the Smart Analytics features, you need to add the "idol.assistant" capability word to their operator records. The operators with this capability word can see Smart Analytics menus and use these features.

> **Note:** ESS self-service users are able to submit Smart Request records after you enable SM Smart Analytics. No additional capability word is needed.

To add the "idol.assistant" capability word to an operator record, follow these steps:

1. From the System Navigator, click **System Administration** > **Ongoing Maintenance** > **Operators**.

2. Enter or select your search criteria, and then click **Search**.
3. Select an operator from the record list to view the operator record.
4. Click the **Startup** tab.
5. Add `idol.assistant` in the **Execute Capabilities** section.

Uninstall Smart Analytics

User Role: Administrator

If you want to uninstall Smart Analytics, follow the instructions in this section.

> **Note:**
>
> - Before you uninstall Smart Analytics, we recommend that you back up your index and category data if you want to restore it in the future.
> - Restart the system after you uninstall Smart Analytics. Otherwise, the services and files cannot be totally removed. Besides, the data and configurations remain after uninstall, and you must delete then manually for safety concerns.

Windows

To uninstall Service Manager Smart Analytics from Windows, follow these steps:

1. Go to **Control Panel** > **Programs** > **Uninstall a program**.
2. Select **HPE SM 9.50 Smart Analytics**, and then click **Uninstall/Change**. The Unistall HPE SM 9.50 Smart Analytics wizard is displayed.
3. Click **Next**.
4. If you want to completely remove Smart Analytics, select **Complete Uninstall**. If you want uninstall specific Smart Analytics features, select **Uninstall Specific Features**.

   > **Note:** If your Smart Analytics is upgraded from a former version, and there is an image server installed, you have to delete the files and service manually when you are uninstalling.

5. Click **Next**, and then follow the on-screen instructions to uninstall Smart Analytics.

Linux

To uninstall Service Manager Smart Analytics from Linux, follow these steps:

1. Go to the _uninstall folder under the Smart Analytics installation directory.
2. Type `./uninstaller -?` from the command line interface to view the uninstallation options and instructions.

   > **Note:** As the Maintenance Mode is not enabled in the SM Smart Analytics uninstaller, the parameters under the Maintenance Mode are not applicable.

3. Use the available commands, and then follow the on-screen instructions to uninstall Smart Analytics.

   For example, you can use `uninstaller -i console` to launch a command line based interactive uninstall process. If you log on to the system through X-Window, you can launch the graphical uninstaller by using the `uninstaller -i swing` command.

   You can specify the features that you want to uninstall, or you can uninstall Service Manager Smart Analytics completely.

Install and configure the Solr Search Engine

The Solr-based search engine enables the Knowledge Management module to index knowledge documents in different formats. For more information, see the "Overview of the Solr Search Engine" on page 311 help topic.

> - As of Service Manager 9.41, you can choose to use either the IDOL Search Engine or the Solr Search Engine for Knowledge Management.
> - If you have purchased Service Manager Smart Analytics, you do not need to install the Solr Search Engine. Additionally, once you have enabled Smart Analytics, you cannot use Solr as the search engine any more.

Follow these instructions to install the Solr Search Engine.

Introduction to the Solr Search Engine Guide

> **Note:** Starting with version 9.41, Service Manager supports both the Solr Search Engine and the IDOL Search Engine for Knowledge Management (KM) search. The IDOL Search Engine is available only when you have Smart Analytics installed and enabled. Once Smart Analytics is enabled, you cannot use the Solr Search Engine anymore. For information about how to install and configure Smart Analytics and use Smart Search, see the *Smart Analytics Administrator and User Guide*.

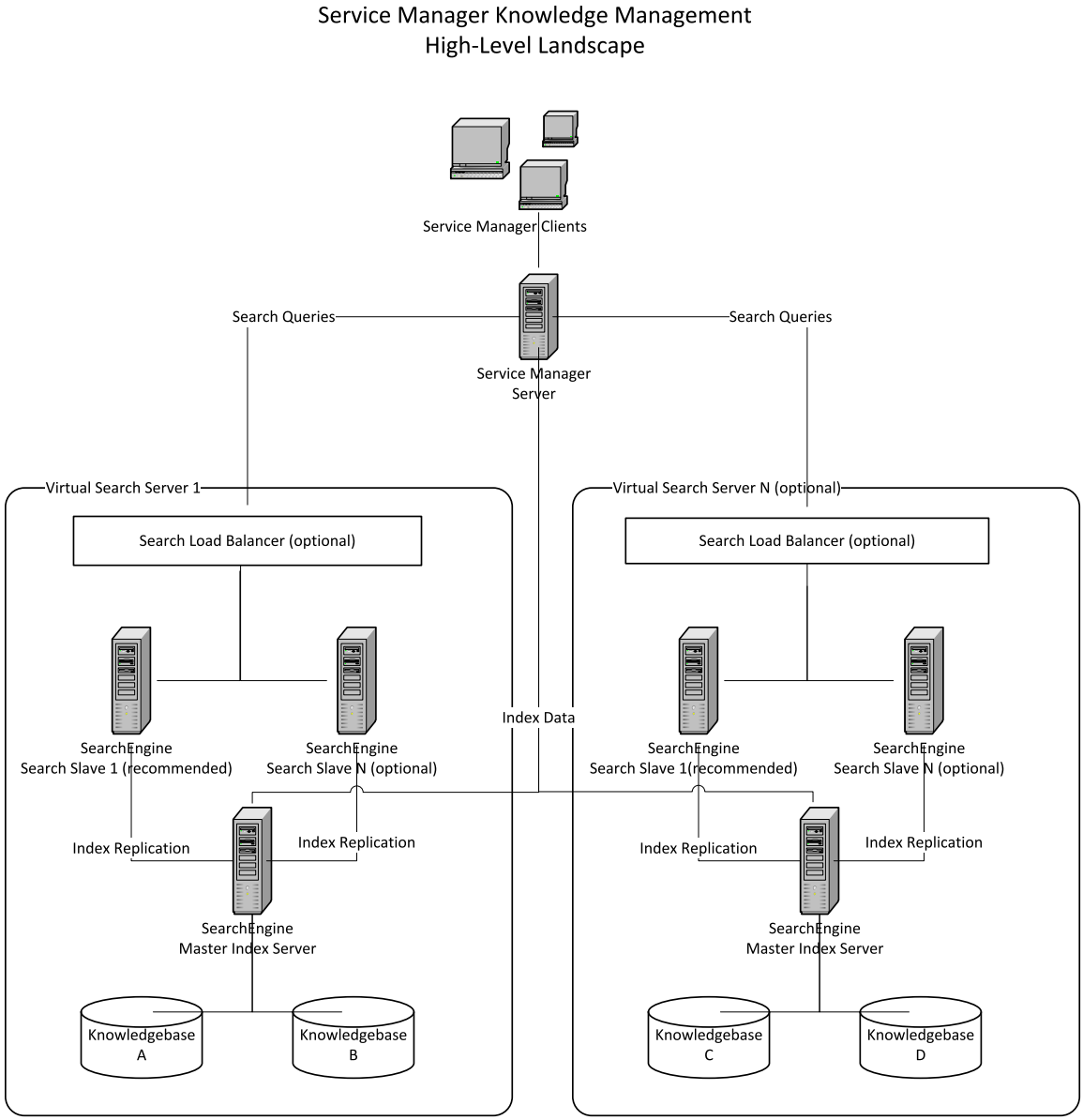
This guide describes how to install the Solr-based Knowledge Management search engine, set up search servers, configure the search engine, and re-index knowledgebases. It also describes how to enforce Mandanten security in the Knowledge Management module where the Solr search engine is used.

Overview of the Solr Search Engine

The Solr-based search engine enables the Knowledge Management module to index over 1,200 unique file formats, including the latest versions of Microsoft Office and OpenOffice formats, PDF, HTML/XML, compression, image, audio, etc.

Due to its flexible architecture, the Solr search engine provides scalability and improves indexing performance by supporting the use of multiple index servers. It supports high availability architectures,which include decoupling of search servers from index servers, replication of the search server to multiple servers, and the addition of a load balancer across multiple search servers; in addition, it can provide fail-safe capabilities, such as the creation of a second index server or search server for failover and the ability to switch to a backup server immediately without having to restart or log out and log back in to your Service Manager server.

The following diagram illustrates an example Service Manager Knowledge Management high-level landscape.



A Knowledge Management search server is composed of three parts: an indexer, a searcher, and a crawler. These server parts are responsible for the following:

- **Indexer**: Indexes documents into searchable data
- **Searcher**: Provides results to users' search requests
- **Crawler**: Indexes the file system and web content

Knowledgebases are assigned to a Knowledge Management search server. If you have a single search server definition, all knowledgebases will be indexed and searched according to that configuration.

When one or more slave servers are defined, all knowledgebases assigned to this virtual search engine will be replicated to each slave. Replication happens when a knowledgebase is re-indexed or the index is updated. Depending on the size of the knowledgebases, they may not be immediately searchable while the replication process is running. If this is a new slave server, you will have to wait for the replication process to finish before you are able to search. Subsequent updates or re-indexes will happen in the background. The slave server will continue to serve search requests on the old knowledgebase until the updated knowledgebase comes on line. It will then automatically begin serving search requests against the new knowledgebase.

Supported Platforms

The search engine runs on multiple platforms, with the same server compatibility as Service Manager.

Language Support

Due to its up-to-date technology, the search engine offers improved Asian language support. Thesaurus maintenance is a lot easier compared to the K2 search engine, because it can now be done through text-based editing. For more information, see "Supported Languages for the Solr Search Engine" on page 362 and "Create Search Engine Thesaurus Files" on page 367.

Upgrade

Upgrading from a custom legacy search engine to the cutting edge Solr search engine is invisible to the end-user, and the administrator only needs to assign the new Solr search servers to the existing knowledgebases and re-index. The Search Engine Management has been greatly simplified – there is no more need for mapped drives and complex environment records. For more information, see "Upgrading from the K2 Search Engine" on page 314.

Flexible Installation of File/Web Crawlers

The File/Web Crawlers are no longer chained to the search engine, and can be located separately, with many new website formats supported.

Upgrading from the K2 Search Engine

The Service Manager 9.50 client and server support only the Service Manager 9.3x Applications, which can only work with the Solr Search Engine.

Once you have upgraded your server and clients to Service Manager 9.50, you must uninstall the K2 Search Engine and install the Solr Search Engine.

Once you run the applications upgrade for Service Manager 9.50, you will lose support for the K2 Search Engine, which affects script libraries, menus, the search library (including advanced search), and how you manage knowledgebases.

To upgrade to the Solr Search Engine, you will need to do the following:

1. Install the Solr Search Engine.
   a. "Meet the Solr Search Engine Requirements" on page 315
   b. "Install the Solr Search Engine" on page 315
2. Configure Service Manager to connect to the new Solr Search Engine and KM Web Crawler by entering the host names, ports, etc., as the old connection information will not work. See "Managing Knowledgebase Search Servers" on page 323.
3. Re-index all of your knowledgebases, as the old indexes will not work. See "Perform a Full Reindex on a Knowledgebase" on page 376.

   > **Tip**: If your knowledgebases contain large amounts of data, re-index them before going into production (live) mode.

4. If you have any tailored forms, follow the normal Service Manager applications tailoring procedures to update the new versions. For more information, see the *HPE Service Manager Tailoring Best Practices Guide*.
5. If you have modified your dbdict, merge your dbdict changes.

> **Note:** If you do not have the administrative experience necessary to manage migrating to the Solr Search Engine, you should get assistance from your local application developers and database administrators.

Installing the Solr Search Engine

The section describes the steps to install a single KM Solr Search Engine instance.

> While a single instance may be suitable for pre-production testing, you may want to install multiple instances for a more robust production system. For information about recommended search server configurations, see "Managing Knowledgebase Search Servers" on page 323.

Meet the Solr Search Engine Requirements

Ensure that the target system complies with the installation requirements, as listed in the *Service Manager 9.50 Support Matrix* on the HPE Support Matrices web site (https://softwaresupport.hpe.com/group/softwaresupport/support-matrices).

HPE recommends using the following configurations for the Solr Search Engine:

- RAM: Minimum of 8GB with 4GB dedicated to the JVM that hosts the Solr Search Engine.
  For better performance, 16GB of RAM with 8GB dedicated to the JVM that hosts the Solr Search Engine.

  > **Note:** It is important to consider the size of the indexes when allocating RAM. Performance is greatly improved if there is enough RAM available to the OS, so that all the index files can be easily cached by the OS as disk seeks to load stored fields and other data from the KM index files, which can slow performance. With 4GB of RAM for the OS, an index of approximately 3GB in size could be cached easily. However, if that number is doubled to 8GB of RAM for the OS, a 6GB or 7GB index could be cached.

- The servers should ideally have at least four processors (no less than two).
- 800 MHz or higher processor
- 400 MB of disc space designated for /tmp (UNIX) and \TEMP (Windows)

Install the Solr Search Engine

Running the Knowledge Management (KM) Search Engine installer will automatically install the Solr Search Engine, KM Web Crawler, and an embedded Apache Tomcat Server. The Solr Search Engine

and KM Web Crawler can be installed separately.

The Solr Search Engine is highly configurable. While a single instance may be suitable for pre-production testing, you may want to install more instances on several machines for a more robust production system. For recommendations on production system configurations, see "Managing Knowledgebase Search Servers" on page 323.

To install the Service Manager Solr Search Engine using the installation wizard, follow these steps:

1. Download the Service Manager 9.50 Solr Search Engine installation package (SM9.50-1.zip) from HPE Software Support Online website.
2. Navigate to the **Installation\KnowledgeManagement** directory.
3. Start the installer wizard.
   - **For Windows:** double-click the **kmsetup-9.50.exe** file.
   - **For Unix:** run the **kmsetup-9.50.bin** file.
4. From the Choose Locale dialog box, choose a language for the installation program. The default is English.
5. Click **OK**.
6. Click **Next**. The license agreement is displayed.
7. Once you have read and agree to the terms of the license agreement, select **I accept the terms of the License Agreement** and then click **Next**.
8. Choose one of the following installation sets and then click **Next**:
   - **Typical:** Installs the Solr Search Engine, KM Web Crawler, and Tomcat Server.
   - **Solr Search Engine:** Installs the Solr Search Engine only with Tomcat Server.
   - **KM Crawler:** Installs the KM Crawler only with Tomcat Server. If you do not plan to crawl file systems or web content, you do not need to install the crawler. The crawler can also be installed by itself on another machine to reduce resource consumption between the crawling process and the indexer.
9. Choose an Installation folder and then click **Next**. The default installation directory opens. For example: `C:\Program Files (x86)\HPE\Service Manager 9.50\SearchEngine` or `/opt/HPE/ServiceManager9.50/SearchEngine`.

   > **Note:** If necessary, click **Choose** to choose a different location.

10. On the Tomcat Port Selection screen, enter the following port numbers and then click **Next**:
    - Tomcat Port number (the default is 8080)
    - Tomcat Shutdown Port number (the default is 8005)

    > **Note:** If the default ports are in use on the server host, you need to use other ports (for example, 8180 and 8105). Record these settings, as you will need them to configure Service Manager to communicate with the Solr Search Engine. See "Add a Virtual Search Server" on page 325.

11. A pre-installation summary displays the following information:
    - Product name selected for installation
    - Installation folder
    - Disk space information for installation target with required bytes and available bytes
12. Click **Install**. The installation begins.
13. The Solr Search Engine is installed. Click **Done** to exit the installer.

Uninstall the Solr Search Engine

The Windows and UNIX uninstall folder and program are the same. You can uninstall the Solr Search Engine as follows:

1. In the <Service Manager Installation Directory>\Search_Engine directory, select **Search_Engine_Uninstall**.
2. Click **Change_or_uninstall.exe**. A message displays, stating that the HPE Solr Search Engine 1.00 and its features will be removed, except files and folders created after the installation.
3. Click **Next** and then select one of the following options:
    - **Complete Uninstall:** To remove all features and components of the HPE Solr Search Engine 1.00 that were installed by the installer, except files and folders created after the installation
    - **Uninstall Specific Features:** To remove specific features of the HPE solr Search Engine 1.00 that were installed by the installer.
4. Click **Next**. The uninstaller begins to remove the features. When the uninstall is complete, a list of the files that have been removed is displayed.

The uninstall process intentionally preserves the files that have changed since the initial installation. You must manually remove these files if you want to completely uninstall the Solr Search Engine from your system.

Before You Start the Solr Search Engine

Once you have installed a Solr Search Engine instance, you need to start it. Before doing so, you need to do the following:

1. Create new system variables on the Search Engine server host:
   - **Variable:=** JAVA_HOME
     Value: = <home folder of JDK>. For example: `C:\Program Files\Java\jdk1.8.0_31`

     > **Note:** The Service Manager 9.50 Solr Search Engine requires JDK 1.8 (either Oracle or OpenJDK). The latest JDK 1.8 is recommended.

   - **Variable:** JAVA_TOOL_OPTIONS
     Value: `-Dfile.encoding=UTF8`
2. Add one of the following lines to the sm.ini file, located in the <Service Manager install>\Server\RUN directory.

   `plugin0:kmplugin.dll` (if the SM server is running on Windows)

   `plugin0:libkmplugin.so` (if the SM server is running on Unix)
3. If your sm.ini file already contains the following line, remove it.

   ```
   KMSearchEngineClass:com.hp.ov.sm.server.plugins.knowledgemanagement.solr.KMSolr
       Search
   ```

   > **Note:** This parameter is no longer needed for Service Manager Solr Search Engine version 9.41 or later. If it is present in the sm.ini file, a warning message will occur in the Service Manager server log (sm.log).
4. Once you have modified the `sm.ini` file, restart the Service Manager server.

Start and Stop the Solr Search Engine

You can start and stop the Solr Search Engine by using the command line scripts or through a Windows Service.

Security best practices

Since the Search Engine uses Tomcat as the web server, be sure to follow the following best practices (see also the Apache documentation for information on Tomcat security best practices).

- On Windows operating systems, you need to create a user account that has been granted the **Log on as a service** right and has **Full Control** permissions to the search engine installation directory (default: C:\Program Files (x86)\HPE\ServiceManagerx.xx\SearchEngine). Further, make sure the **HPE KM Search Engine - Master** or **HPE KM Search Engine - Slave** service is set to run as this user.
- On Unix systems, follow these steps:
  a. Install the Search Engine as root.
  b. Create a user to run the Search Engine. Suppose the user is SearchEngineUser.
  c. Run the following command to change the owner of the Search Engine installation directory:

     ```
     sudo chown -R SearchEngineUser Search_Engine_install_directory
     ```

  d. Run the following command to start the Search Engine:

     ```
     sudo -u SearchEngineUser Search_Engine_install_directory/startup.sh
     ```

For more information about the startup.sh script and running the Search Engine as a Windows service, see "Start and stop the Search Engine using scripts" below and "Start and stop the Search Engine as a Windows service" on the next page.

Start and stop the Search Engine using scripts

Run the following executable scripts in the Solr Search Engine installation folder to start and stop the Search Engine.

Search engine startup scripts

Name	Purpose
startup.cmd	Starts the master Solr Search Engine server on a Windows system.

Search engine startup scripts, continued

Name	Purpose
	Starts the KMCrawler that has been installed separately.
startup.cmd slave	Starts the slave Solr Search Engine server on a Windows system.
startup.sh	Starts the master Solr Search Engine server on a UNIX system.
startup.sh slave	Starts the slave Solr Search Engine server on a UNIX system.

Search engine shutdown scripts

Name	Purpose
shutdown.cmd	• Shuts down the master Solr Search Engine server on a Window system. • Shuts down the KMCrawler if it was installed separately.
shutdown.cmd slave	Shuts down the slave Solr Search Engine server on a Windows system.
shutdown.sh	• Shuts down the master Solr Search Engine server on a UNIX system. • Shuts down the KMCrawler if it was installed separately.
shutdown.sh slave	Shuts down the slave Solr Search Engine server on a UNIX system.

Start and stop the Search Engine as a Windows service

You can register and install the Search Engine as a Windows service, and then start and stop the Solr Search Engine as a Windows service.

Register and install the Search engine as a Windows service

Run the following scripts to register the Solr Search Engine as a Windows service. Once the Solr Search Engine is registered as a Windows service, then you can use startup and shutdown scripts through the Windows service. The name of the Windows service in the Windows console is: **HPE KM Search Engine**.

The following table lists the registration scripts for Windows systems.

Name	Purpose
installasservice.cmd install master	Installs the master Solr Search Engine server as a Windows Service.

Name	Purpose
Installasservice.cmd install slave <identifier>	Installs the slave server as a Windows Service.
installasservice.cmd install	Installs the KMCrawler as a Windows Service when the KMCrawler has been installed separately.
installasservice.cmd remove master	Removes the master Windows Service.
installasservice.cmd remove slave <identifier>	Removes the slave Windows Service.
installasservice.cmd remove	Removes the KMCrawler Windows Service.

Start and stop the Solr Search Engine as a Windows Service

1. From the Windows Start menu, select **Control Panel** > **Administrative Tools** > **Services**.
2. Select the service that you want to start, for example: **HPE KM Search Engine - Master**, **HPE KM Search Engine - Slave <identifier>**, or **HPE KM Search Engine - Crawler**.
3. To start the service, right-click the service and select **Start**.
4. To stop the service, right-click the service and select **Stop**.

Once you have installed and started your search engine instances, you are ready to configure them and verify their connectivity in Knowledge Management. For more information, see "Managing Knowledgebase Search Servers" on page 323.

Enable SSL for the Solr Search Engine

After the Solr Search Engine installation is complete, you can optionally enable SSL for communications between the Service Manager Server and the Solr Search Engine.

To do this, follow these steps:

1. Generate certificates for both the Service Manager Server and the Solr Search Engine.

   For details, see the "Generate FIPS validated certificates for the SM Server and other components" topic in the Service Manager Help Center.

   > **Note:** For FIPS mode, the certificate type is pkcs12; for standard SSL mode, use the jks

certificate type instead.

2. Enable SSL in the Service Manager Server.

   To do this, configure the following parameters in the Server's RUN\sm.ini file:

   ```
   ssl:1
   sslConnector:1
   ssl_reqClientAuth:2
   keystoreFile:sun-server-smserver.mycompany.net.jks
   keystorePass:serverkeystore
   ssl_trustedClientsJKS:trustedclients.jks
   ssl_trustedClientsPwd:trustedclients
   truststoreFile:smcacerts.jks
   truststorePass:changeit
   ```

   Note: You need to replace the certificate files and their passwords with your own values.

3. Enable SSL in the Solr Search Engine.

   For details, see the "Steps to configure FIPS mode in the Solr Search Engine" section in the "Configure FIPS mode in the Solr Search Engine" topic in the Service Manager Help Center.

Managing Knowledgebase Search Servers

Deploying a single search engine instance is not recommended for production environments. For information about recommended configurations for a production environment, see "Recommended Search Server Configurations " below.

Recommended Search Server Configurations

The following provides recommended configurations of the Solr Search Engine for a production environment.

Recommended configuration for improved performance

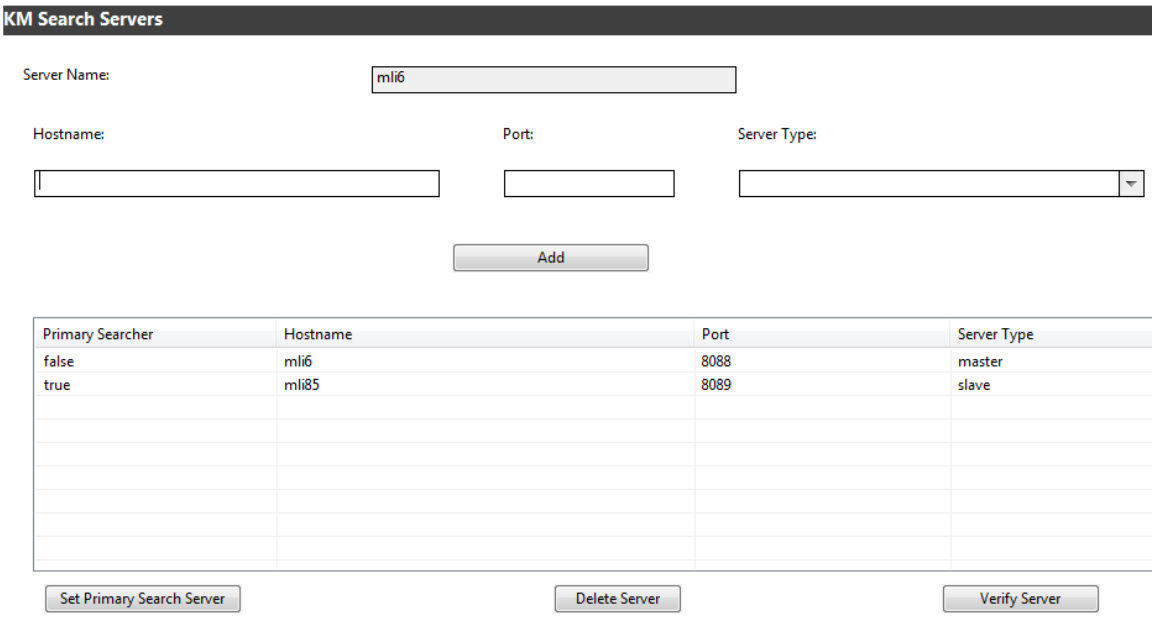
A search server with a master and a slave is the recommended minimum configuration for a production system. You must install a separate instance of the search engine on a separate port or a separate machine; you cannot define a slave server with the same parameters as the master server.

For improved system performance and to allow indexes to be replaced, you can separate the indexer and searcher onto two separate machines, as follows:

- On machine A, perform a full install of the Solr search engine.
- On machine B, install the searcher and indexer components (without the crawler).
- Add two servers for the search server: Machine A as the master server and machine B as a slave server.
- Set machine B as the primary searcher.

In this configuration, all indexing and crawling will be performed by machine A, and all searching will be performed by machine B. Indexes will automatically be replicated to machine B when changes are made to the original indexes on machine A, the master server.

See the following figure for an example of this configuration.



Recommended configuration for improved performance and failover

For better performance and to provide failover capabilities, add a second slave server and configure a load balancer to handle search requests for both machines A and B. In this scenario, you will have three machines. In this setup, all indexing and crawling will be performed on Machine A.

- Machine A will have a full install of the Solr search engine.
- Machines B and C will only need the searcher and indexer components of the install (without the crawler).
- Load balancer is installed and configured on machine B, machine C, or on another system.

  > **Note**: The Solr search engine does not ship with a load balancer.

- For the search server, you will add four servers:
  - Machine A as the master server.
  - Machines B and C as slave servers.
  - Load balancer is added as a reference and is set as the primary searcher. Search requests will be directed to the load balancer, which will then redirect search requests to either machine B or C, depending on the load. Machine B or C will perform the actual search task.

The configurations above can be replicated to cover any loads you may have. If you have large knowledgebases, you can create additional search servers of any configuration, and then assign the knowledgebases individually to each search server. See "Overview of the Solr Search Engine" on page 311 for a diagram of a Service Manager Knowledge Management high-level landscape.

For information about adding a search server cluster, see "Add a Virtual Search Server" below.

Add a Virtual Search Server

User Role: System Administrator, KMAdmin

The Knowledge Management search server form displays settings used for configuring the Knowledge Management search servers (or search engines) to provide connectivity to Service Manager for knowledgebase searching. The search engines can be installed on separate machines to enhance performance.

A virtual search server must contain one master server and may also contain several slave servers or a load balancer server. In most cases, a single virtual server should be sufficient for most organizations. However, your particular organization may choose to encapsulate your knowledgebases into multiple virtual servers for performance reasons or to prevent all knowledgebases from going down at the same time. See "Overview of the Solr Search Engine" on page 311 for the diagram of an example virtual server configuration.

To add a virtual search server, add a master first and then add slave or load balancer servers to it as needed. The following describes the three types of search servers:

- **Master**: Indexing will always happen on this server. You can only have one master server per virtual search engine. This is the minimum server definition needed for a working virtual search engine configuration.
- **Slave**: Slave servers are optional. When defined and the Primary Searcher field is set to true, all search requests for knowledgebases assigned to this virtual search engine will be directed to this server.
- **Load Balancer**: Load balancers are optional. When defined and the Primary Searcher field is set to true, all search requests will be directed to this server. You also need to install a load balancer (an Apache web server) for load balancing of the virtual search server.

  > **Note** For load balancing of the Solr search engine, only Apache has been tested and is currently supported by HPE.

Primary Searcher

If a virtual server contains one master and only one slave, the slave must be the primary searcher. If a virtual server contains one master and more than one slave, a load balancer is needed, and the load balancer must be the primary searcher.

Search requests are always initially directed to this server. If the primary searcher is a load balancer, it will redirect the requests to the other servers in the virtual server group.

To add a new virtual search server:

1. From the navigator menu, select **Knowledge Management > Configuration > Configure Search Servers**.
2. In the **Server Name** field, enter the server name that specifies the name for the virtual search server - Knowledge Management search server. Choose a unique name to describe the search server, as in "Production" or "Development."

   > **Caution** You cannot change server names once the record is added.

3. Click **Add**. The fields for the virtual search server will be displayed.

   > **Note** All fields are required for adding or editing search server records.

4. Add a master to the new search server.
   a. Complete the following fields:
      - **Hostname** Enter the server name (or IP address) of the machine where the master server is installed.

        > **Caution** Do not specify **localhost** as the Hostname of a search server, no matter whether it is a master, slave or load balancer.

      - **Port**: The search engine requires an open port for communication. For most Tomcat web servers, the default port is **8080**. The web server listens to this port number for the search engine.

        > **Note** Ensure that the port you select is not blocked or otherwise restricted by a firewall.

      - **Server Type**: Select **Master**.

   b. Click **Add**. The master search server is added to the virtual search server.

   c. Select the master server from the table and then click the **Verify Server** button to send a test ping to that server. For more information, see "Verify Knowledgebase Search Server Connectivity" on page 330.

      Optionally, you can continue to add slave or load balancer servers to the search server.

5. Optionally, add a slave search server.
   a. In the **Server Name** and **Port** fields, enter the server name (or IP address) and port of the slave server host.

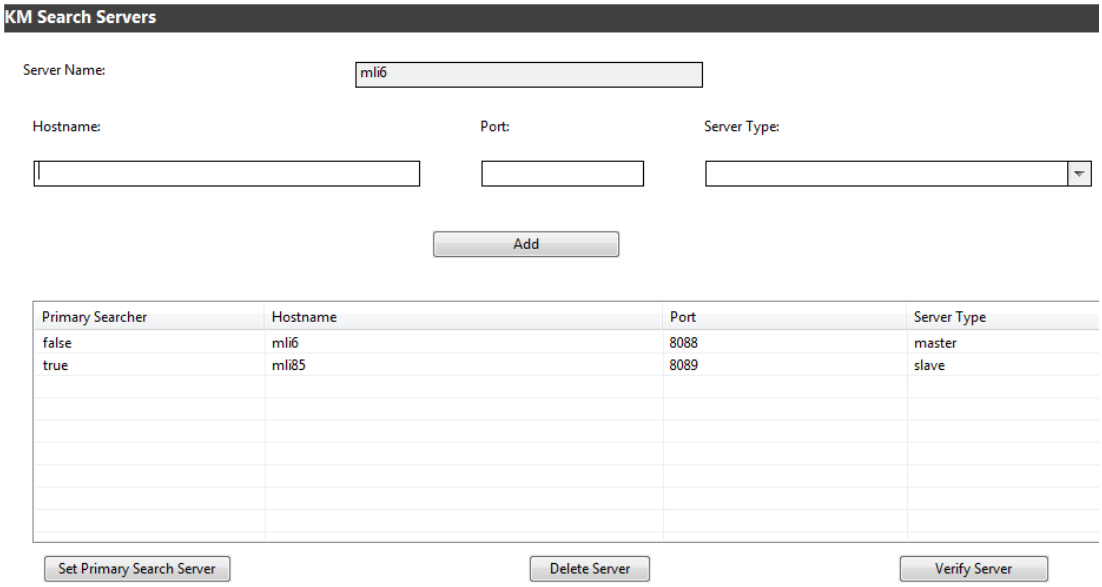
      > **Caution** You should not designate any search server as localhost.

b. Select **Slave** for **Server Type**.

c. Click **Add**. The slave server is added to the table.

d. Verify the slave server connectivity. See "Verify Knowledgebase Search Server Connectivity" on page 330.

The following figure shows an example master and slave configuration.

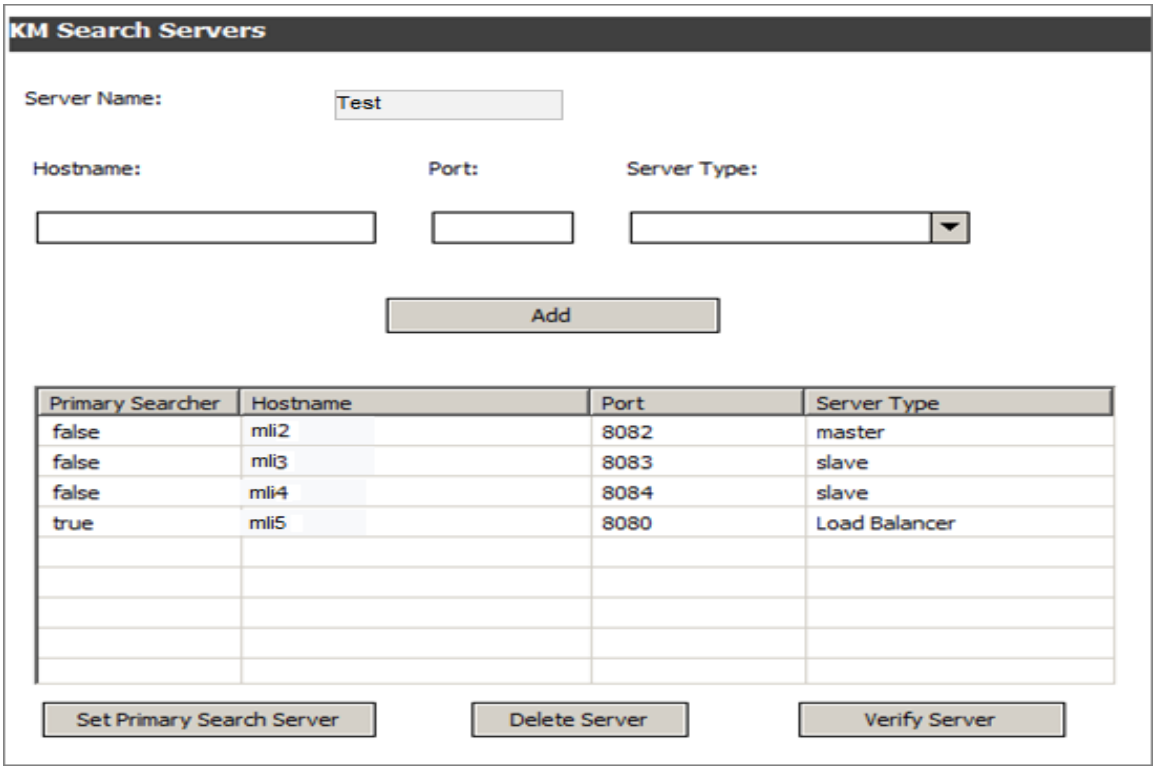


6. Optionally, add a load balancer search server and configure load balancing:

a. Make sure you have already added one master and at least two slave search servers, as described above.

> **Important** You must install a load balancer (for example, an Apache web server) of your own choice, as no load balancer is provided with Knowledge Management. You must choose a unique port for your load balancer; do not use a port defined for a master server or slave server. A minimum of two slave servers is recommended for load balancing. Do not load balance a single slave server with the master server. If the master server is re-indexing, the load balancer may send a search request to the master server and the search will fail.

The following example describes how you can configure load balancing for a virtual search server, using an Apache web server as a load balancer. This example assumes the following virtual search server configuration is used.



b. Set one of the salves as the Primary Searcher. For details, see "Specify a Primary Searcher" on page 330.

c. Perform a full re-indexing of an existing knowledgebase. For details, see "Perform a Full Reindex on a Knowledgebase" on page 376.

d. Click **Search Knowledgebase**, select the indexed knowledgebase, and verify the search functionality is working fine.

e. Install an Apache 2.x server on a machine that you want to use as the load balancer server.

f. Modify the httpd.conf file in the conf directory to enable the proxy server.

   i. Uncomment the following loadModule lines.

   ```
   LoadModule proxy_http_module modules/mod_proxy_http.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_module modules/mod_proxy.so
   ```

   ii. Add the following proxy server configuration to the end of the file.

   ```
   #example
   ProxyRequests Off
   ProxyPass /KMCores balancer://mycluster/
   ```

```
ProxyPassReverse /KMCores balancer://mycluster/
<Proxy balancer://mycluster>
BalancerMember http://mli3:8083/KMCores
BalancerMember http://mli4:8084/KMCores
</Proxy>
```

Where: **mycluster** is a descriptive name for the search server cluster, while **mli3:8083** and **mli4:8084** are the host names and ports of the slaves.

g. Start the Apache server.

h. Verify that the proxy server works fine for load balancing (http://mli5:8080/KMCores).

i. Add the load balancer server to the virtual search server.

   i. In the **Server Name** and **Port** fields, enter the server name (or IP address) and port of the Apache server.

   ii. Select **Load Balancer** for **Server Type**, and click **Add**. The load balancer server is added.

j. Set the load balancer server as the Primary Searcher. For details, see "Specify a Primary Searcher" on the next page.

The load balancing configuration is complete.

To delete an existing server from a virtual search server (that is, a search server cluster):

1. Select the server from the table.
2. Click the **Delete Server** button.

> **Caution** You should not delete a Primary Search server. You need to select another server to handle search requests. Once the Primary Searcher server setting is changed to another server, you can delete the server.

To delete an existing virtual search server:

Delete a virtual search server only if there are no knowledgebases assigned to it. If no knowledgebases point to the server, you can delete the server.

1. On the **Knowledge Management** > **Configuration** > **Knowlegebases** screen, change the Search Server Name to an alternate server.
2. Click **Knowledge Management** > **Configuration** > Configure Search Servers.
3. Click **Search**.

4. Select the virtual search server you want to delete.
5. Click **Delete**.

Verify Knowledgebase Search Server Connectivity

User Role: System Administrator, KMAdmin

When a search server is added or edited, you need to test whether Service Manager is communicating with the server.

To verify the knowledgebase search server is communicating with Service Manager:

1. From the navigator menu, select **Knowledge Management > Configuration > Configure Search Servers** and then click **Search**.
2. Select the server name you want to verify.
3. Click **Verify Server**. If the search server is correctly set up, an information window displays with the following message: **Search Engine Connected**.

   Once the server settings are verified, you may index and search the knowledgebases.

Specify a Primary Searcher

User Role: System Administrator, KMAdmin

When you have configured a search server with a master and one or more slaves/load balancers, you need to specify one of these servers as a Primary Searcher. All search requests for knowledgebases assigned to this virtual search engine will be redirected to this server. If the primary searcher server goes down,you can set the Primary Searcher field to 'true' on another server to restore search functionality. For more information on search server configuration considerations, see "Recommended Search Server Configurations " on page 323.

To specify a primary searcher:

1. Click **Knowledge Management** > **Configuration** > **Configure Search Servers**.
2. Click **Search**. A list of search servers (if configured) is displayed.
3. Double-click a search server from the list to open the record.

> **Note**: If the search server contains only a master,its Primary Searcher field is set to true by default; if the search server contains a master and one or more slaves/load balancers, the master is by default specified as a primary searcher, but you can change the default setting.

4. Select a server from the record, click the **Set Primary Search Server** button. The server's **Primary Searcher** field changes from **false** to **true**.
5. Click **Save** to save the search server record.

Specify a Search Server for Each Knowledgebase

User Role: System Administrator, KMAdmin

All default knowledgebases will map to the search server that is added first. An administrator can add a second search server to point to an additional search engine installation, if needed. Individual knowledgebases can then be separated onto different search servers.

To specify a search server for a knowledgebase:

1. Navigate to **Knowledge Management > Configuration > Knowledgebases**, and click **Search**.
2. Select a knowledgebase from the list.
3. In the Search Server field, select a search server.
4. Click **Save**.

   You do not have to log out or restart your Service Manager server for the changes to take effect.

Once you have assigned a search server for each knowledgebase, you are ready to perform a full re-indexing of the knowledgebases. For more information, see "Indexing the Knowledgebases" on page 372.

Configuring the Solr Search Engine

Before you can use the Knowledge Management (KM) Solr Search Engine, you will need to set up the KM environment, configure the Search Engine, create indexes, and configure the Nutch Web Crawler.

Important: To configure the KM Solr Search Engine and Nutch Web Crawler, you should be an experienced System Administrator who is familiar with your installation.

The following checklist outlines the tasks that you should complete to configure the KM Solr Search Engine and Nutch Web Crawler:

1. Edit the Knowledge Management environment record if needed. See "Edit the Knowledge Management Environment Record" on the next page.
2. Set up and verify server connectivity for multiple servers. Since the KM Solr search engine and Nutch Web Crawler can be installed on multiple servers, you need to set up connectivity for all servers.
   - Configure a search server cluster. For information on the master + slave + load balancer architecture, see "Managing Knowledgebase Search Servers" on page 323.
   - List all servers in a cluster. See "Add a Virtual Search Server" on page 325.
   - Assign the virtual search server to existing knowledgebases. See "Managing Knowledgebases" on page 335.
3. Add knowledgebases if needed. You can add three types of knowledgebases: sclib, weblib, and fsyslib. For more information, see "Add an sclib Knowledgebase" on page 335, "Add a weblib Knowledgebase" on page 347, and "Add an fsyslib Knowledgebase" on page 354.
4. Enable your language(s). Out-of-the-box, only English is enabled.

   You will need to add your language(s) to the search engine's collection configuration file, known as the schema. This schema file is located in the Service Manager server directory. For details, see "Enable Languages in the Solr Search Engine" on page 365.

   You will also need to activate your language(s) in the **language** table. For details, see "Activate a Knowledge Management language" on page 363. For information on which languages are supported by the search engine that can be enabled for Knowledge Management, see the KM Identifier values in the **language** table.
5. If needed, create your own thesaurus dictionaries for use when searching content. The KM Solr Search Engine supports thesaurus files (or dictionaries) for individual languages, but none are provided out-of-the-box. To create your own thesaurus dictionaries, see "Create Search Engine Thesaurus Files" on page 367.

6. Modify the stop words for your language(s) if needed. See "Modify Stop Words" on page 369.
7. When you first install the KM Solr search engine after having used the K2 search engine, you will need to re-index all of your knowledgebases, as the old indexes will not work. Once the new index has been created, you can re-index all of your knowledgebases. Read about the indexing process in "Indexing the Knowledgebases" on page 372, and also see "Perform a Full Reindex on a Knowledgebase" on page 376.
8. Make sure that the KMUpdate process is started. See "Indexing the Knowledgebases" on page 372.

Edit the Knowledge Management Environment Record

User role: System Administrator, KMAdmin

Before you can use Knowledge Management and the search engine, you must configure settings. The Knowledge Management Environment record allows you to set up connectivity and define options, such as enabling adaptive learning and setting the number of documents to be returned from a search. This record contains default settings. However, you can configure these settings to meet your business needs.

To configure the Knowledge Management application environment settings, do the following:

1. Click one of the following:
   - **Knowledge Management > Administration > Environment**
   - **System Administration > Ongoing Maintenance > Environment Records > Knowledge Management Environment**
2. Select new options or clear default options. Your changes redefine the Knowledge Management environment for all users.
3. **Assign the Default Knowledge View Group to all operators** who will have permission to search knowledge. A check mark ensures that all operators are able to view any documents in those document categories to which the default knowledge view group has access.
4. Select the check box to enable **Use Adaptive Learning to enhance search results** to weight search results based on usage. You can artificially weight documents using Adaptive Learning by adding a phrase and adding a number of occurrences with the phrase to specify that the term or

phrase occurs in the document a specified number of times. If the phrase is not literally present, this can have the effect of putting the phrase, or word, in the document. It also simulates the number of times the phrase is added to the document index, based on the quantity you choose to apply.

Notes:

- Clear the check box to disable Adaptive Learning.
- When you disable Adaptive Learning, you need to go to the "Manage Knowledgebases" screen and reindex all knowledgebases of type sclib.
- Adaptive Learning data is not deleted when Adaptive Learning is disabled.

5. Specify the **Maximum number of documents** to be returned from a search.
6. Specify the **Default expiration period** of time a document should be stored in the document queue before it expires.

   Note: The time period specified here will be over-ridden if an expiration date was specified when the document was created using the Contribute New Document function.
7. Specify the style text for search results.
8. If you have deployed Service Request Catalog for Service Manager, enable Knowledge Management search for Service Request Catalog users.
   a. Select the **SRC?** check box.
   b. In the Search Server field, select a virtual search server from the list.
   c. Click **Full Reindex**.

   > **Note**: Only the Service Manager knowledge library is available for Service Request Catalog users to search.
9. When you have finished making your changes, click **Save** and **OK**.
10. Log out of Service Manager and then log back in again for your changes to take effect.

    Warning: When these fields are not set correctly and a user attempts to access a knowledgebase, the Manage Knowledgebase form displays an error, stating that the search engine is incorrect or not found, and asking you to check the environment settings.

Managing Knowledgebases

There are three types of knowledgebases that you can add to Knowledge Management in Service Manager. You can add an sclib knowledgebase, an fsyslib knowledgebase, and a weblib knowledgebase. An sclib knowledgebase is created from a table in Service Manager. For example the out-of-the-box Incident_Library uses the probsummary table. A weblib knowledgebase is created by using web crawling to browse and index an external web site. The system creates an fsyslib knowledgebase when it crawls a file system.

The Knowledgebases feature enables administrators to add and delete knowledgebases. In order to add a knowledgebase and make it functional you need to:

- Identify the type of knowledgebase
- Map fields for indexing and searching
- If needed, update the four ScriptLibrary scripts that were created when you added the knowledgebase:
  <LibraryNameHere>_kmaccess
  <LibraryNameHere>_kmcategoryidxscript
  <LibraryNameHere>_kmprocesslibcriteria
  <LibraryNameHere>_kmsearchsecurity
- For sclib type knowledgebases only, create a new tab for the knowledgebase for advanced searching

Add an sclib Knowledgebase

User role: System Administrator, KMAdmin

The **sclib** type is used to index data contained in Service Manager tables, such as knowledge articles or other records. Out-of-the-box, there are five sclib knowledgebases:

- Incident_Library: used to index data of all Incident records.
- Interaction_Library: used to index data of all Interaction records.
- Knowledge_Library: used to index data of all knowledge articles.
- KnownError_Library: used to index data of all Known Error records.
- Problem_Library: used to index data of all Problem records.

You may need to add more sclib knowledgebases in your production environment. To do so, you need to perform the following tasks.

Task 1: Add an sclib knowledgebase record.

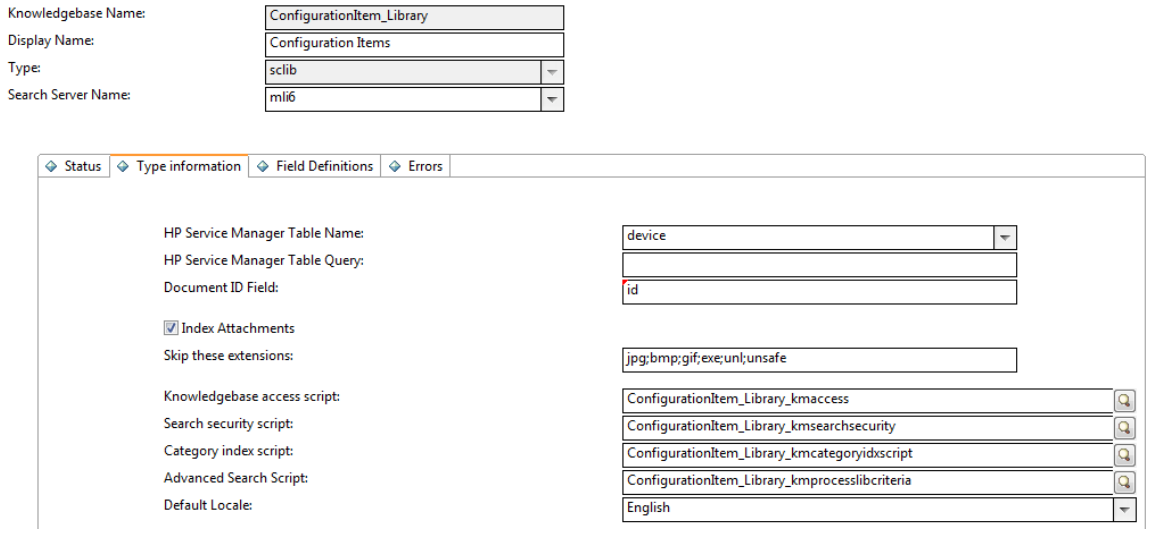
To add a sclib knowledgebase record:

1. Click **Knowledge Management > Configuration > Knowledgebases**.
2. Type a name for the new knowledgebase.
3. Type a display name for the new knowledgebase.
4. Select **sclib** in the Type list.
5. Click **Add**.
6. Type the Refresh Interval rate on the Status tab so that the selected knowledgebase index is updated at the specified interval. Each interval unit is five minutes (default). You may increase the interval to slow down the time between updates, or you may set the number at zero (0) to disable updates to the index.
7. On the **Type information** tab, provide the necessary information. The system creates a default Knowledgebase access script, a Search security script, and Category index scripts.

Field	Description
HPE Service Manager Table Name:	This is the Service Manager table that will be indexed. A valid Service Manager table is required. For example: **kmdocument**.
HPE Service Manager Table Query:	Used to enter a Service Manager style query to limit what records in the table are indexed. For example, a query to return only documents that are neither draft nor retired in the kmdocument table**:** `status ~= "draft" and status ~="retired"`. A blank query indicates that all records will be indexed.
Document ID Field:	Every table in Service Manager has a unique ID field and this field identifies the field name of the ID field. The indexer uses this field to uniquely identify each document in the index. This is a required field for indexing a knowledgebase.
Index Attachments	If the table being indexed has attachments, select this check box to have the attachments indexed. **Caution:** The search engine can index a wide variety of data types. However, indexing attachments is processor intensive. Each attachment must be extracted from the attachment table, written out to the local file system, and then streamed to the search engine server.

Field	Description
Skip These Extensions:	A semicolon-separated list of file extensions that should not be indexed nor extracted. Certain file types either cannot be indexed, or provide no relevance. By providing these extensions, you can increase index performance. **Note:** Sample `gif;jpg` without any spaces.
Knowledgebase access script:	This script specifies the script the system uses to determine if a particular user has rights to access the knowledgebase. See the default script for detailed information.
Search security script:	This script further limits what users have access to, when they have access to the knowledgebase. This script returns a query string that is added to the user's normal query to limit the scope of the particular user's access to documents in the knowledgebase. See the default script for detailed information.
Category index script:	This script processes the document category so that the indexer can translate the document's category into a string that the search engine can use later to find the document based on the user's category access.
Advanced Search Script:	This script is used to build and return a string of library-specific query values that were entered by the user under the tabs in the Advanced Search screen. Tailor this script when a knowledgebase has a tab in the Advanced Search screen and you wish to modify the fields available for Advanced Search.
Default Locale:	Specifies the default language used by the search engine when searching and indexing. By default, the language code is English.

The following figure shows the **Type information** tab of an example sclib knowledgebase named ConfigurationItem_Library.

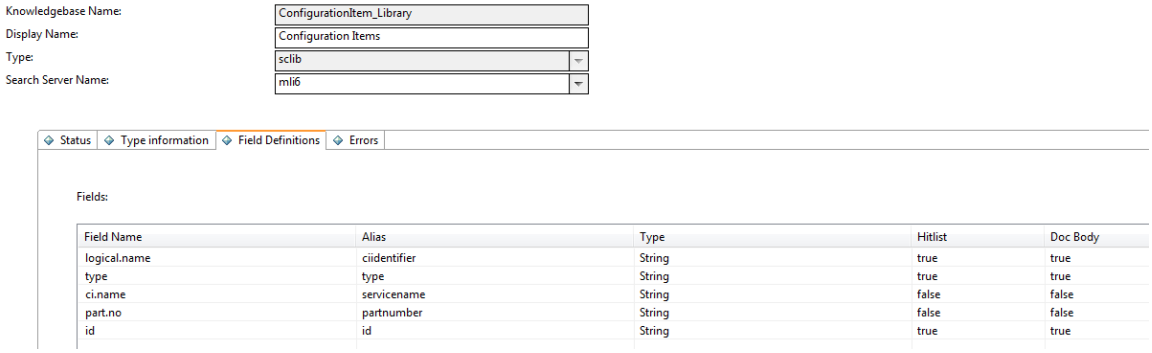


8. Provide the necessary field definition data for the new knowledgebase.

Field	Description
Field Name	Specifies the field name in the Service Manager table included in the index.
Alias	Specifies the name that the field is to be indexed as. You can make use of the Alias field to have a single common field name for searching and for the hitlist. For example, you may wish to alias different fields from different tables as "Title" so they can be searched using Advanced Search. Fields can have more than one alias. Separate these fields with a semicolon. An alias can be the same name as the field name. If the alias name includes ".", the system converts the period to an underscore when indexed.
Type	Indicates whether the field is a plain text string, a rich text string or a date type. The indexer ignores HTML markup in rich text strings and indexes plain text strings completely.
Hitlist	Defines what fields are available on the search hitlist. Fields marked as "true" in the hitlist column are available to be included on a search results hitlist display.
Doc Body	This column is a Boolean (True/False) field. By setting the field in this column to "true," the system indexes the field's content as part of the document body and also as an individual field. The search engine searches only the document body in the simple search. Fields with the Doc Body marked as "false" can only be searched by doing a field search with the Advanced Search.
Delete Field	Used to delete a field from the table. a. Select the field you want to delete. • In the Windows client, click a field to select it.

Field	Description
	• In the web client, hold down the Shift key as you click a field to select it. b. Click the **Delete Field** button to delete the field.

The following figure shows the **Field Definitions** tab of the ConfigurationItem_Library knowledgebase. These fields are defined in the **device** table, and you need to specify an Alias for each of them.



9. Configure the **Status** tab.

The **Status** tab for an sclib knowledgebase provides information about the selected knowledgebase's index and details about the search servers to which the knowledgebase is connected. This information includes:

Field	Description
Master, Slave, or **Load Balancer**	This field provides information about the search servers that are connected to the selected knowledgebase. Details on each server connection include type of server (Master, Slave, or Load Balancer), state of the server, date the server was created, and the number of documents that were indexed in the knowledgebase. For more information, see **State**, **Created**, and **Docs**. To make changes to a search server, go to **Knowledge Management > Configuration > Configure Search Servers** and select the search server.
State	Indicates whether the knowledgebase is on-line, off-line, or replicating (if it is a slave server). If State is blank, the knowledgebase is either off-line or the search engine is not connected.
Created	Displays the date and time the knowledgebase was created. This value will change when the **Full Reindex** button is pressed.
Docs	Displays the number of documents currently indexed in the knowledgebase . This number may or may not exactly match the number of records in the table being

Field	Description
	indexed. Factors that can contribute to this include: Using a selection query other than "true" on the Type Information tab or when a document is indexed into multiple document categories. It is indexed once for each document category to which it is assigned.
Refresh Interval	Displays the current interval used to update the selected knowledgebase index. Each interval unit is 5 minutes (default). You may increase the interval, which slows down time between updates, by increasing this number. Setting this number to 0 (zero) disables updates to the index. To re-start indexing, reset the interval to a value greater than zero. **Note:** Changes made to the table being indexed will be cached even if the update interval is set to 0. These changes will be processed once the interval is set higher than 0. A full re-index removes all changes for this knowledgebase from the change cache.

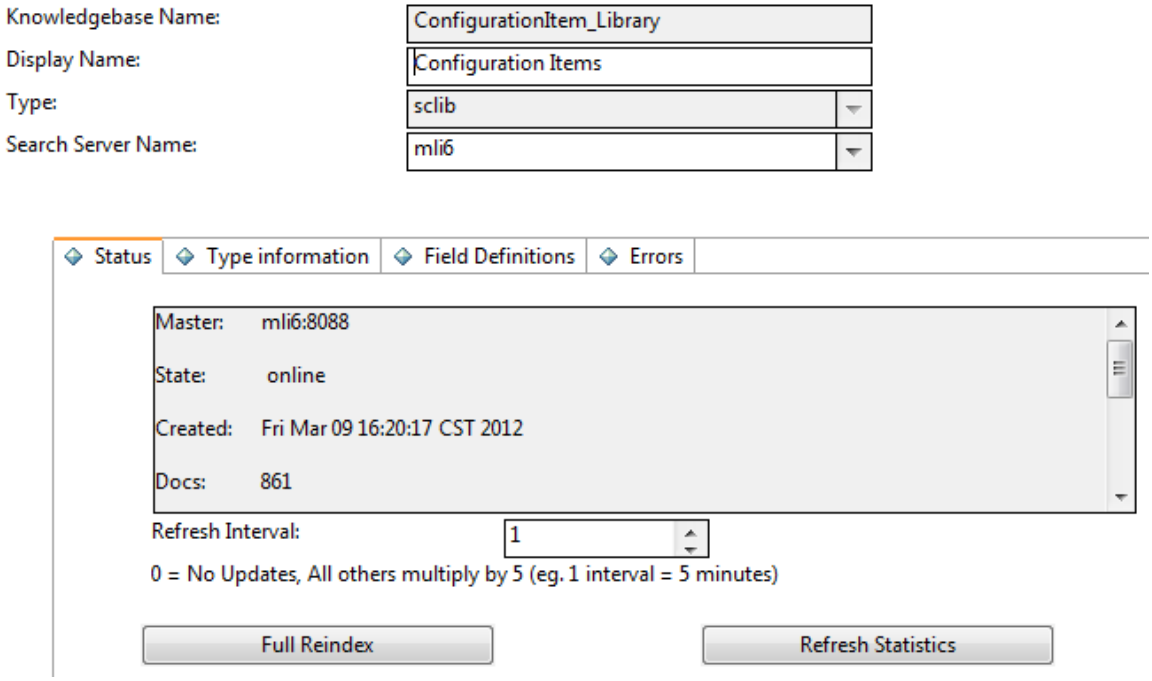
The tab also includes buttons for indexing.

Button	Description
Full Reindex:	When selected, the search engine performs a full re-index of a knowledgebase. If the index does not exist, it will be created. If it does exist, it will be deleted and re-created. A full re-index will remove all changes for this knowledgebase from the change cache since they will no longer be relevant. When you click the Full Reindex button, the KMUpdate process begins initialization processing to start indexing a knowledgebase, but because indexing runs as a background process, the search engine does not begin indexing until the specified refresh interval is reached. Doing a full re-index on a large knowledgebase may have a significant impact on system resources. Certain actions require a full re-index. These actions are: ◦ Initial setup (no indexes exist). ◦ Changing any value on the Type Information tab or the Field Definitions tab. ◦ When a large number of changes or new documents have been added. For example, when you import new documents. ◦ When search engine performance becomes sluggish. As updates are applied to the index, they are added as incremental index files. If you have a knowledgebase that has had many changes applied, these incremental index files can slow the search engine down, since it must perform your query on each one. A full re-index builds a new clean index that performs better. This is similar to defragmenting a hard drive.

Button	Description
	Note: If you have a single master server defined, users will not be able to search the knowledgebase being re-indexed until the process completes successfully. If you have one or more slave servers, users will continue to search the old knowledgebase while the index is being re-created on the master server. Once indexing is complete, the old knowledgebase will be replaced by the new knowledgebase on the slave servers automatically and seamlessly, without disrupting user searchers.
Refresh Statistics	When selected, the search engine refreshes the statistics of the indexing process to show how many documents are indexed and searchable at that time in the process.

10. Click **Save**.
11. Click **Full Reindex** on the **Status** tab to re-index the documents in the knowledgebase.
12. Click **Refresh Statistics** on the **Status** tab to refresh statistics tracking knowledge documents at various stages.

    The following figure shows that a Full Re-indexing has been completed for the example ConfigurationItem_Library knowledgebase.



    Now, you can perform simple searches in the new knowledgebase. However, if you want to enable the Advanced Search functionality for the knowledgebase, you need to complete the following additional tasks.

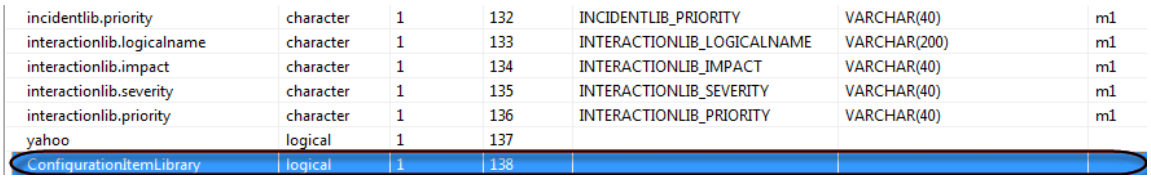
Task 2: Add new fields in the kmquery table.

You must add new fields to the kmquery dbdict record, which specifies the fields available for searching during an advanced search of the new knowledgebase.

When you add a field, use the naming convention <element_name>lib.<field_name> to make it available for advanced searching. Taking the ConfigurationItem_Library knowledgebase for example, you can use **ci** or **configurationitem** for <element_name>, followed by the field's Alias name defined on the **Field Definitions** tab. For example,for the **logical.name** field, you can add an entry of **cilib.ciidentifier**.

> **Note**: These field names are used in the format input and are mapped into the query in the <LibraryNameHere>kmprocesslibcriteria script library.

When you add a new sclib type library, the system adds a new Boolean field. For example, if you named your new knowledgebase ConfigurationItem_Library, the system adds a Boolean field named ConfigurationItemLibrary.



incidentlib.priority	character	1	132	INCIDENTLIB_PRIORITY	VARCHAR(40)	m1
interactionlib.logicalname	character	1	133	INTERACTIONLIB_LOGICALNAME	VARCHAR(200)	m1
interactionlib.impact	character	1	134	INTERACTIONLIB_IMPACT	VARCHAR(40)	m1
interactionlib.severity	character	1	135	INTERACTIONLIB_SEVERITY	VARCHAR(40)	m1
interactionlib.priority	character	1	136	INTERACTIONLIB_PRIORITY	VARCHAR(40)	m1
yahoo	logical	1	137			
ConfigurationItemLibrary	logical	1	138			

As an example, the following steps illustrate how to add new fields in the kmquery dbdict record for the ConfigurationItem_Library knowledgebase.

1. Log in to the Service Manager Windows client as a system administrator.
2. Type **dbdict** in the command line, and press Enter.
3. In the **File Name** field, type **kmquery**, and click **Search**. The kmquery dbdict record opens.
4. On the **Fields** tab, place the cursor on the **descriptor** row, and click **New Field/Key** to add the following example fields to the kmquery dbdict record.

ConfigurationItemLibrary	logical	1	138	CONFIGURATIONITEMLIBRARY	CHAR(1)	m1
cilib.ciidentifier	character	1	139	CILIB_IDENTIFIER	VARCHAR(200)	m1
cilib.type	character	1	140	CLILIB_TYPE	VARCHAR(60)	m1
clilib.status	character	1	141	CILIB_STATUS	VARCHAR(60)	m1
cilib.partnumber	character	1	142	CILIB_PARTNUMBER	VARCHAR(60)	m1
cilib.id	character	1	143	CILIB_ID	VARCHAR(60)	m1

5. Click **OK**.
6. Select **SM Alters**. A message displays: **Record updated in the dbdict file**.

Task 3: Add the new fields to the Advanced Search Script of the knowledgebase.

Once you have added the Advanced Search fields in the kmquery dbdict, add the fields in the advanced search script that was created when the knowledgebase record was added. You can find this script on the **Type information** tab of the sclib knowledgebase record. For example, for the ConfigurationItem_Library knowledgebase, the Advanced Search Script is named **ConfigurationItem_Library_kmprocesslibcriteria**.

As an example, the following steps illustrate how to add the new fields in task 2 to the **ConfigurationItem_Library_kmprocesslibcriteria** script.

1. Log in to Service Manager as a system administrator.
2. Type **sl** in the command line, and press Enter.
3. In the **Name** field, type **ConfigurationItem_Library_kmprocesslibcriteria**, and then click **Search**.
4. Add the following lines to the script.

```
function ProcessLibCriteria(KMQuery)

{

var getenginename = system.library.KMSearchInterface.getEngineName();

var strQuery = "";

if (getenginename == "K2")

{

if(KMQuery.cilib_ciidentifier != null)

strQuery += " <AND> (ciidentifier <CONTAINS> " + KMQuery.cilib_ciidentifier + "
<AND> _style <CONTAINS> ConfigurationItem_Library)";

if(KMQuery.cilib_type != null)

strQuery += " <AND> (type <CONTAINS> " + KMQuery.cilib_type + " <AND> _style
<CONTAINS> ConfigurationItem_Library)";

y)";

if(KMQuery.cilib_status != null)

strQuery += " <AND> (status <CONTAINS> " + KMQuery.cilib_status + " <AND> _
style <CONTAINS> ConfigurationItem_Library)";

if(KMQuery.cilib_partnumber != null)

strQuery += " <AND> (partnumber <CONTAINS> " + KMQuery.cilib_partnumber + "
<AND> _style <CONTAINS> ConfigurationItem_Library)";

if(KMQuery.cilib_id != null)

strQuery += " <AND> (id <CONTAINS> " + KMQuery.cilib_id + " <AND> _style
<CONTAINS> ConfigurationItem_Library)";
```

```
}

else

{

if(KMQuery.cilib_ciidentifier  != null)

strQuery += " (ciidentifier : " + KMQuery.cilib_ciidentifier + " AND
knowledgebase_name: ConfigurationItem_Library)";

if(KMQuery.cilib_type != null)

strQuery += " (type: \"" + KMQuery.cilib_type + "\" AND knowledgebase_name:
ConfigurationItem_Library)";

if(KMQuery.cilib_status != null)

strQuery += " (status: " + KMQuery.cilib_status + " AND knowledgebase_name:
ConfigurationItem_Library)";

if(KMQuery.cilib_partnumber != null)

strQuery += " (partnumber: " + KMQuery.cilib_partnumber + " AND knowledgebase_
name: ConfigurationItem_Library)";

if(KMQuery.cilib_id != null)

strQuery += " (id: " + KMQuery.cilib_id + " AND knowledgebase_name:
ConfigurationItem_Library)";

}

return strQuery;

}
```

5. Save and compile the script. A message should display: **Successful compilation of JavaScript function or expression**.

Task 4: Create a viewing format for the knowledge candidates for the knowledgebase.

Use Forms Designer to create a viewing form for the knowledge candidates for the new knowledgebase. When users click a search result (knowledge candidate) of the new knowledgebase, it opens in this form.

Task 5: Add a tab to the Knowledgebase Advanced Search form.

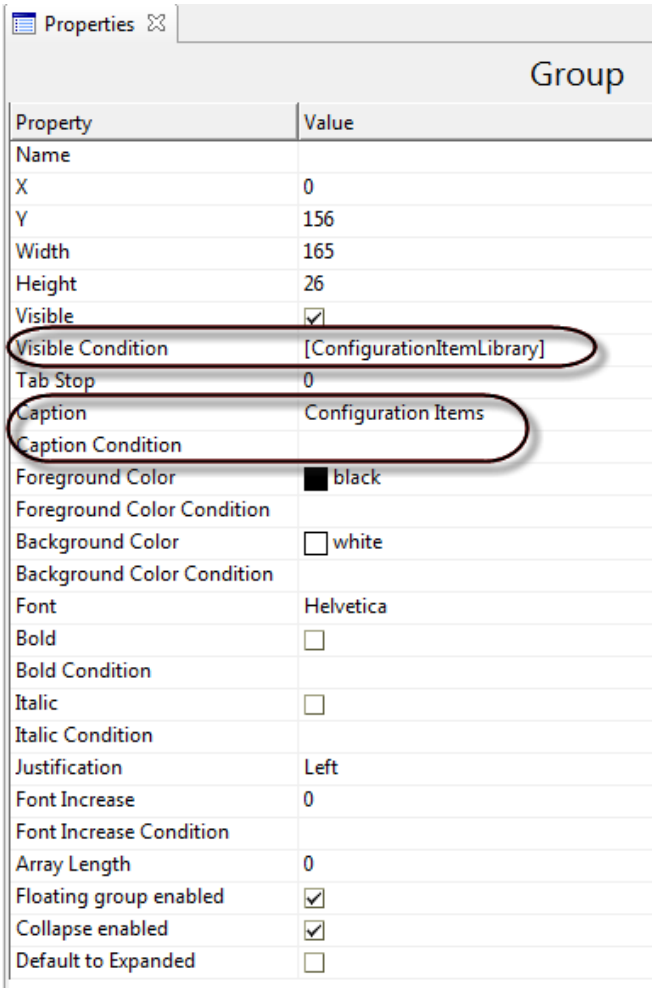
Use the Forms Designer to add a new widget to include the fields that have been added in the kmquery dbdict. Set the visible condition for the widget to use the same Boolean field name the system added when you added the new knowledgebase.

As an example, the following steps illustrate how to add a widget for the ConfigurationItem_Library knowledgebase.

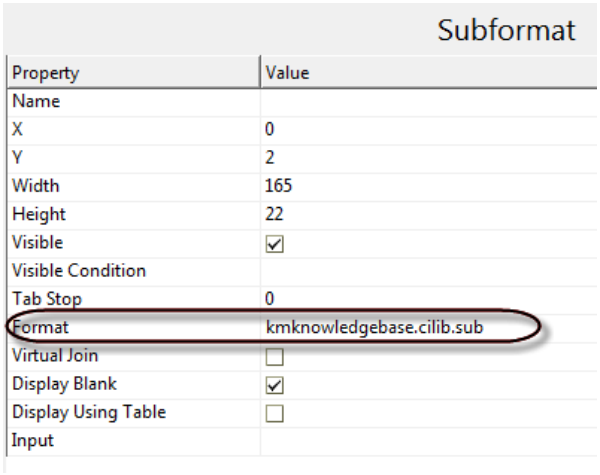
1. Log in to Service Manager as a system administrator.
2. Type **fd** in the command line, and press ENTER.
3. Create a subform for the ConfigurationItem_Library knowledgebase.
   a. In the Form field, type **kmknowledgebase.cilib.sub**, and then click **New**.
   b. Click **No** to create the subform without using the form wizard.
   c. Create the subform with all fields you have added to the kmquery dbdict record.

4. Add a widget for the ConfigurationItem_Library knowledgebase.
   a. In Forms Designer, open the **kmknowledgebase.advsearch.g** form in Design mode. Out-of-the-box, this form contains the following Group controls: **Knowledge Library**, **Known Errors**, **Problems**, **Incidents**, and **Interactions**.
   b. Create a new Group widget by copying an existing Group control, for example, the **Interactions** group.
   c. Change the following properties of the new group:
      - Visible Condition: **[ConfigurationItemLibrary]** (This is the Boolean field name the system added to the kmquery dbdict record when you added the new knowledgebase)
      - Caption: **Configuration Items**

- Caption Condition: Leave this setting empty.



d. Select the subform enclosed in the group, and change the Format property to **kmknowledgebase.cilib.sub**.



e. Click **OK**.

5. Verify that KM Advanced Search is enabled for the new knowledgebase.
   a. Navigate to **Knowledge Management** > **Search Knowledgebase**.
   b. In the **Search In** section, select and then deselect the Configuration Items library, to verify that the Configuration Items widget displays and disappears accordingly.

   c. Enter values in certain Configuration Item fields, and then click **Search**, to verify that Advanced Search works correctly for configuration item records.

Add a weblib Knowledgebase

User role: System Administrator

Web crawling enables administrators to make outside knowledge sources accessible to users and reduce administration costs. With this feature, you can:

- Index and search external Web content, such as RightAnswers and Microsoft's TechNet.
- Index and search Intranet content, such as internal corporate web content.

If you have large number of documents that you do not want to import into Service Manager but still wish to index and search, you can publish these documents to a web server for crawling with the web crawler. You can also crawl these documents with the file system crawler.

Indexing requirements for web crawling

The indexing requirements for a weblib-type knowledgbase are different than those of an sclib type. For weblib types, Service Manager stores only information used to create the knowledgebase (collection) format and the information used by the search engine to index the pages being crawled.

Log files for web crawling

Log files are generated during indexing for the web pages being crawled. These log files are located in the following directory:

```
C:\Program Files (x86)\HPE\Service Manager x.xx\Search_
Engine\kmcrawler\logs
```

The log files end in .log.

The two most important log files in this folder are `skipkeys.log` and `joberror.log`. The `skipkeys.log` provides detailed information as to why a particular page was skipped during indexing. For example, if a page is an excluded mime type or if the path depth has been exceeded, it is logged in this file. The `joberror.log` contains the errors encountered by the indexer. For example, if you provided a start URL that could not be reached, it is logged here.

To add a new weblib knowledgebase, you need to complete the following tasks.

Task 1: Add a weblib type knowledgebase record.

To add a weblib type knowledgebase record:

1. Click **Knowledge Management > Configuration > Knowledgebases**.
2. Type a unique name for the new knowledgebase in the Knowledgebase name field (required). For example, **My_Web**.
3. Type a display name for the knowledgebase (required). For example, **My Web**.
4. Select **weblib** in the Type field list.
5. Click **Add**.

The knowledgebase record is added. Continue to configure the tabs of the record and test the knowledgebase, as described in the following tasks.

Task 2: Configure the Type information tab.

The Type Information tab maintains information about the knowledgebase's source and security. Configure the following **Type information** settings.

Field	Description
URLs	**URL:** Type the URLs in the space provided. You can enter more than one URL, but use only one URL per line. **Note**: The "http://" prefix is required for all URL's. For example: `http://www.bbc.com`
URL path depth	Limits indexing to the specified number of path segments in the URL or file system path. The default is 100 path segments. The path length is determined as follows: • The host name and drive letter are not included. For example, neither `www.spider.com:80/` or `C:\` are included in determining the path length. • All elements following the host name are included. • The actual file name, if present, is included. For example, `/world.html` is included when determining the path length. • Any directory paths between the host and the actual file name are included. For example: For the following URL, the path length would be 4: `http://www.spider:80/comics/fun/funny/world.html` where: comics = 1 segment fun = 1 segment funny = 1 segment world.html = 1 segment
Max links to follow	Specifies the maximum number of levels from the starting URL that an indexing includes. If you see extremely large numbers of documents in a knowledgebase where you do not expect them, consider experimenting with this option, in conjunction with the Content options, to reduce the reach of the index. Specify a number between 0 and 255. The default is 255, which is equivalent to there are no limits on the number of jumps.
Constrain indexing to host domains	By default, links are not followed outside the hosts provided in the URLs. Un-checking this box lets the indexer index outside the hosts specified.
Mime Types	• **Unlimited:** The search engine supports over 1,200 different MIME types.

Field	Description
	Selecting "Unlimited" will include this full list of MIME types during crawling. • **Include:**List the MIME file types to be included in the index. Specify the file type by using the MIME specification. Enter only one MIME type per line. You may use the "*" wildcard only for MIME types. For example, "text/*". This example will include all the MIME types that start with "text/". • **Exclude:** List the file types NOT to be included in the index. Specify the file type by using the MIME specification. Enter only one MIME type per line. You may use the "*" wildcard only for MIME types. For example, "text/*". This example excludes all the MIME types that start with "text/". The default values in the drop-down list for MIME types can be configured as follows: 1. Go To **Tailoring > Database Manager**. 2. Search for the **kmmimetypes** table to retrieve the full list of MIME types. **Note**: You can edit the list of MIME types. See "Edit the List of MIME Types" on page 353. 3. Check the **Mimelist** box, so that the all available MIME types will appear in the drop-down list. 4. Save your changes.
Proxy Configuration	• **Proxy Host:** Provides the proxy host name when the web site being crawled uses a proxy server. • **Port:** The port number used by the proxy server. • **Username:** The user name required by the proxy server for access. This may not be required for all proxy servers. • **Password:** The password associated with the user name provided. This may not be required by all proxy servers.
Security Scripts	• **Knowledgebase access script:** This script specifies the script the system uses to determine if a particular user has rights to access the knowledgebase. See the default script for more detailed information. • **Search security script:** This script further limits what the user has access to when accessing the knowledgebase. This script returns a query string that is added to the user's normal query to limit the scope of the particular user's access to documents in the knowledgebase. See the default script for more detailed information. • **Category index script:** This script processes the document category so that the indexer can translate the document's category into a string that the search engine can use later to find the document based on the user's category access. • **Advanced search script:** This script processes a string of library-specific query values using the KMQuery object. The values in KMQuery were entered by the user under the tabs in the Advanced Search screen. You can tailor this script if this knowledgebase has a tab in the Advanced Search screen.

Field	Description
	• **Default locale:** Specifies the default language used by the search engine when searching and indexing. By default, the language code matches the language you logged in as.

Task 2: Configure the Status tab.

The Status tab for a weblib knowledgebase displays information about the selected knowledgebase's index. This information includes the following:

Field	Description
Master, Slave, or **Load Balancer**	This field provides information about the search servers that are connected to the selected knowledgebase. Details on each server connection include type of server (Master, Slave, or Load Balancer), state of the server, date the server was created, and the number of documents that were indexed in the knowledgebase. For more information, see the **State**, **Created**, and **Docs** settings. To make changes to a search server, go to **Knowledge Management > Manage Search Servers** and select the search server.
State	Indicates whether the knowledgebase is on-line, off-line, or replicating (if it is a slave server). If State is blank, the knowledgebase is either off-line or the search engine is not connected. If the knowledgebase has not been created, this field is blank.
Created	Displays the knowledgebase creation date and time. If the knowledgebase has not been created, this field is blank.
Docs	Displays the number of documents contained in the index. If the knowledgebase has not been created, this field is blank. If the knowledgebase has been created but not indexed, this field will show 0 documents.
Status	Since the index is created separately from the knowledgebase creation, the Status field displays the current status of the index. Values can be "Not Created," "Created," "Running," and "Finished."
Schedule this index?	You can choose to schedule the index to start on a particular day and time. Select the **Schedule this index?** check box to enable scheduling.
Start Date	Select the first day you wish this index to run. Adjust the time values to the time of day the index should run.
Frequency	You can schedule the index to run once, hourly, daily, weekly, or monthly. For example, if you scheduled the index to run on Monday, May 5, at 6 p.m. and selected an hourly frequency, the index would run the first time on Monday, May 5, at 6 p.m. and would then run again at 7 p.m., 8 p.m., and so on until you updated the schedule. **Note**: When indexing, the search engine only indexes documents that have changed since the last run.

Field	Description
Crawler Host	Specify the host name of a search server for web crawling. It can be a master or slave search server; however for optimized performance you can use a dedicated server for crawling only.
Crawler Port	Specify the Tomcat port of the crawler host.

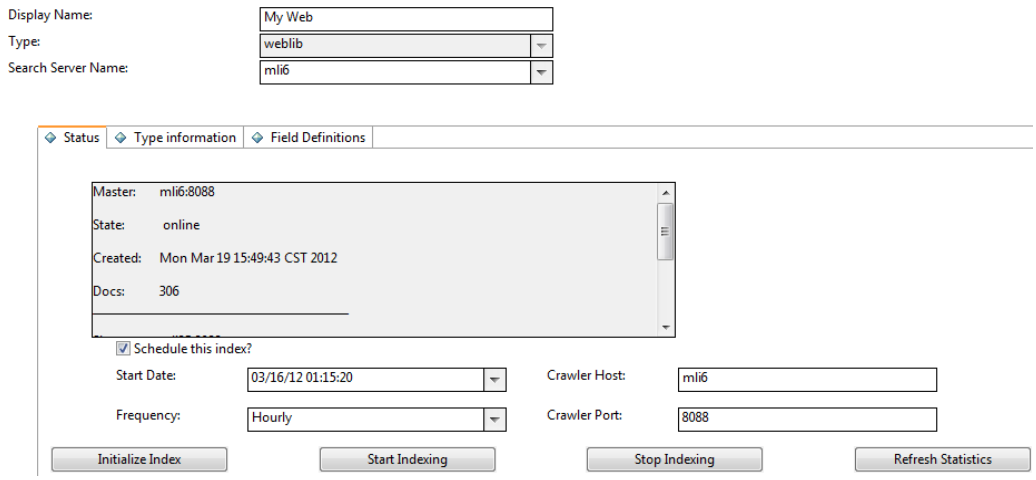
The tab also includes buttons for indexing.

Button	Description
Initialize Index	Once you have all your settings specified for a new knowledgebase, click this button. The system sends the settings to the search engine. The search engine creates the empty knowledgebase for index. After a knowledgebase and index have been created, click this button to erase the index and create an empty knowledgebase. You should create a new knowledgebase if you change the parameters on either the **Type information** tab or **Field Definitions** tab.
Start Indexing	Click this button to start an index manually. Instead of scheduling index updates, you can use this button if the file system you are crawling does not change or if you want to test index settings once.
Stop Indexing	Click this button to stop an indexing process that is running. Click the **Start Indexing** button to resume indexing from the point where the index was stopped. To start indexing from the beginning, click **Initialize Index**.
Refresh Statistics	When selected, the search engine refreshes the statistics of the indexing process to show how many documents are indexed and searchable at that time in the process.

Task 3: Index the weblib knowledgebase.

1. On the **Status** tab, click **Initialize Index**.
2. Click **Start Indexing**.
3. Click **Refresh Statistics** to monitor the indexing status. Once the documents have been indexed on the crawler and replicated to the searcher, you can continue to perform a test search on the weblib knowledgebase.

The following figure shows an example.

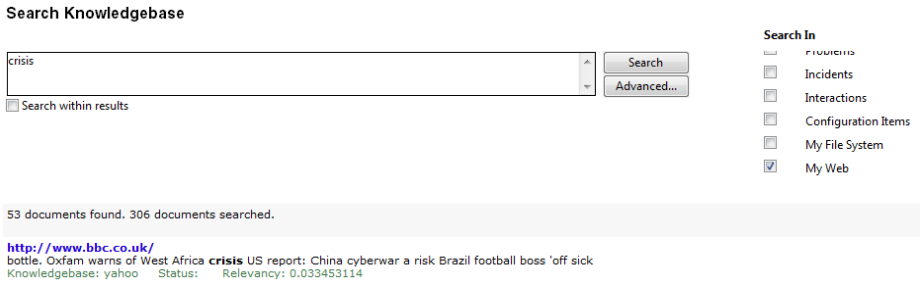


Task 4: Search in the weblib knowledgebase.

Perform a search in the new weblib knowledgebase to verify that it is set up properly.

1. Click **Knowledge Management** > **Search Knowledgebase**.
2. In the Search In section, select only the new weblib knowledgebase.
3. Enter a search word in the search box, and click **Search**.

   The following figure illustrates a list of search results of an example weblib knowledgebase.



Edit the List of MIME Types

User role: System Administrator, KMAdmin

When indexing file systems and web sites, there are MIME type file extensions recognized by the Solr search engine. The web server passes along MIME-type information based on its own internal tables.

To edit the list of MIME types to be included or excluded in the drop-down lists:

1. Click **Tailoring** > **Database Manager**.
2. In the Table field, type **kmmimetypes** and then click **Search**.
3. Based on your business needs, edit the "include" and "exclude" MIME type selections.

   Note: MIME types with the Mimelist checkbox selected (or checked) will display in the drop-down selections.
   a. Select the MIME type **Mimelist** check boxes that are blank, so that those MIME types will be included in the drop-down selections.
   b. Uncheck the MIME type **Mimelist** check boxes that are currently selected, so that those MIME types will be excluded from the drop-down selections.
   c. Click the **Unlimited** radio button to store all MIME types in the kmmimetypes table, so that all MIME types are used.
4. Save your changes.

Add an fsyslib Knowledgebase

User role: System Administrator, KMAdmin

File systems can be crawled to create fsyslib-type knowledgebases. File system crawling enables administrators to make the knowledge in a file system outside of Service Manager accessible to users and to reduce administration costs.

> **Note**: The KM Crawler can crawl only local file systems on the crawler host.

To add an fsyslib-type knowledgebase:

1. Click **Knowledge Management > Configuration > Knowledgebases**.
2. Type a unique name for the new knowledgebase in the Knowledgebase name field (required). For example, **My_FYS**.
3. Type a display name for the knowledgebase (required). For example, **My File System**.
4. Select **fsyslib** in the Type field list.
5. Click **Add**. The knowledgebase record is added.
6. Configure the **Type information** tab.

Field	Description
Directories	◦ **Start Path:** Type the Universal Naming Convention (UNC) directory path. You can enter more than one path, but use only one path per line. If the starting directory is hosted on a UNIX server, also specify: ◦ **Replace this UNIX path:** The UNIX directory to substitute with the Windows mapping to the UNIX server path. ◦ **With this Windows mapping:** The Windows mapping to the UNIX path. This translation of the mapped path is necessary so that the Windows client loads the knowledge article from the correct location when displaying it in the hitlist after a search. For example: Start Path: `/samba/test/webcrawltest` Replace this UNIX path: `/samba/test` With this Windows mapping: `\\blade100\test\\<UNIX mapping on Windows>`
Path depth:	Limits indexing to the specified number of path segments in the file system path. The default is 100 path segments. The path length is determined as follows: ◦ The host name (for example, `\\hostname`) is not included in determining the path length. ◦ All elements following the host name are included and determine the path length in the path name, including the actual file name (for example, `\world.htm`) if it is present. ◦ Any directory paths between the host and the actual file name are included. **Example**: For the following UNC path, the path length would be 4: `\\host\comics\fun\funny\world.html` where: comics = 1 segment fun = 1 segment funny = 1 segment world.html = 1 segment
Mime Types	◦ **Unlimited:** The search engine supports over 1,200 different MIME types. Selecting "Unlimited" will include this full list of MIME types during crawling. ◦ **Include:** List the MiIME file types to be included in the index. Specify the file type by using the MIME specification. Enter only one MIME type per line. You may use the "*" wildcard only for MIME types. For example, "text/*". This example will include all the MIME types that start with "text/".

Field	Description
	◦ **Exclude:** List the file types NOT to be included in the index. Specify the file type by using the MIME specification. Enter only one MIME type per line. You may use the "*" wildcard only for MIME types. For example, "text/*". This example excludes all the MIME types that start with "text/". The default values in the drop-down list for MIME types can be configured as follows: a. Go To **Tailoring > Database Manager**. b. Search for the **kmmimetypes** table to retrieve the full list of MIME types. c. Check the **Mimelist** box, so that the all available MIME types will appear in the drop-down list. d. Save your changes.
Security Scripts	◦ **Knowledgebase access script:** This script specifies the script the system uses to determine if a particular user has rights to access the knowledgebase. See the default script for more detailed information. ◦ **Search security script:** This script further limits what the user has access when given access to the knowledgebase. This script returns a query string that is added to the user's normal query to limit the scope of the particular user's access to documents in the knowledgebase. See the default script for more detailed information. ◦ **Category index script:** This script processes the document category so that the indexer can translate the document's category into a string that the search engine can use later to find the document based on the user's category access. ◦ **Advanced search script:** This script processes a string of library-specific query values using the KMQuery object. The values in KMQuery were entered by the user under the tabs in the Advanced Search screen. You can tailor this script if this knowledgebase has a tab in the Advanced Search screen. ◦ **Default locale:** Specifies the default language used by the search engine when searching and indexing. By default, the language code matches the language you logged in as.

7. Configure the **Field Definitions** tab.

Column	Description
Field Type	Select Constant. You may alias the 'constant' field as you would any other field. Every document indexed will have a field with the name you specified and the value listed in this field. Constant fields can be used for search security, categorization, or similar types of data that you do not have edit access to. Example constant: $PASSAGE_BASED_SUMMARY

Column	Description
Field Name	Define a unique name for your 'constant' field in the Field Name.
Alias	This is the name of the field as it is to be indexed. You can make use of the Alias field to have a single common field name for searching and for the hitlist.
Data Type	Specify the Data Type for date fields to allow date range searching.
Hitlist	Defines what fields are available on the search hitlist. Fields marked as 'true' in the Hitlist field are available to be included on a search results hitlist display.
Value	Specify the value for the 'constant' field. **Note**: The Value field is not used for a field type meta tag.

8. View the **Status** tab.

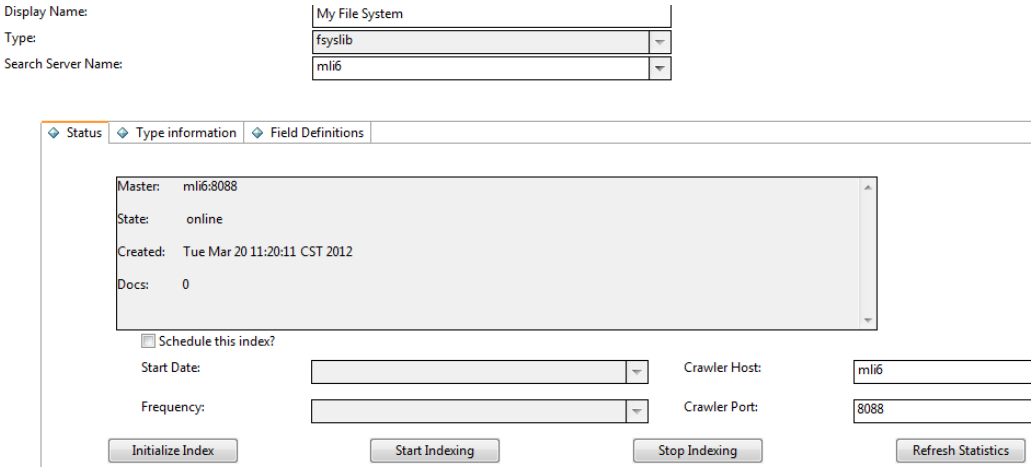
Field	Description
Master, Slave, or **Load Balancer**	This field provides information about the search servers that are connected to the selected knowledgebase. Details on each server connection include type of server (Master, Slave, or Load Balancer), state of the server, date the server was created, and the number of documents that were indexed in the knowledgebase. For more information, see **State**, **Created**, and **Docs**. To make changes to a search server, go to **Knowledge Management > Configuration > Configure Search Servers** and select the search server.
State	Displays whether the collection is online or offline. If the knowledgebase has not been created, this field is blank.
Created	Displays the knowledgebase creation date and time. If the knowledgebase has not been created, this field is blank.
Docs	Displays the number of documents contained in the index. If the knowledgebase has not been created, this field is blank. If the knowledgebase has been created but not indexed, this field will show 0 documents.
Status	Since the index is created separately from the knowledgebase creation, the Status field displays the current status of the index. Values can be "Not Created", "Created", "Running", and "Finished".
Schedule this index?	You can choose to schedule the index to start on a particular day and time. Select the **Schedule this index?** check box to enable scheduling.
Start Date	Select the first day you wish this index to run. Adjust the time values to the time of

Field	Description
	day the index should run.
Frequency	You can schedule the index to run once, hourly, daily, weekly, or monthly. For example, If you scheduled the index to run on Monday, May 5, at 6 p.m. and selected hourly for the frequency, the index would run the first time on Monday, May 5, at 6 p.m. and would then run again at 7 p.m., 8 p.m., and so on until you updated the schedule. When indexing, the search engine only indexes documents that have changed since the last run.
Crawler Host	Specify the host name of a search server for web crawling.
Crawler Port	Specify the Tomcat port of the crawler host.

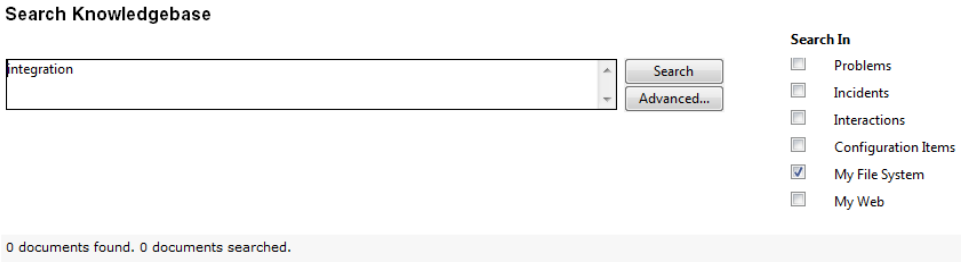
This tab also contains the following indexing buttons:

Button	Description
Initialize Index	Once you have all your settings specified for a new knowledgebase, click this button. The system sends the settings to the search engine. The search engine creates the empty knowledgebase for index. After a knowledgebase and index have been created, click this button to erase the index and create an empty knowledgebase. You should create a new knowledgebase if you change the parameters on either the **Type information** tab or **Field Definitions** tab.
Start Indexing	Click this button to start an index manually. Instead of scheduling index updates, you can use this button if the file system you are crawling does not change or if you want to test index settings once.
Stop Indexing	Click this button to stop an indexing process that is running. Click the **Start Indexing** button to resume indexing from the point where the index was stopped. To start indexing from the beginning, see **Initialize Index**.
Refresh Statistics	When selected, the search engine refreshes the statistics of the indexing process to show how many documents are indexed and searchable at that time in the process.

9. Click **Initialize Index** to index the new fsyslib knowledgebase.



10. Click **Save**.
11. Perform a test search on the new fsyslib knowledgebase to verify that it is set up correctly.



Delete a Knowledgebase

You can delete an existing knowledgebase, using a Delete button available on the Knowledgebase Maintenance form. When you delete a knowledgebase, the system automatically performs certain clean-ups needed for the removed knowledgebase, however for a sclib type knowledgebase, you still need to manually undo the changes to the system you made when adding the knowledgebase.

When you delete a knowledgebase, the system automatically:

- Removes four triggers on the table whose records were indexed: `after.add.KM.<tablename>`, `before.update.KM.<tablename>`, `after,update.KM.<tablename>`, and `before.delete.KM.<tablename>`.
- Removes the Boolean field from the kmquery table that corresponds to the knowledgebase.

- Removes references to the new knowledgebase from three functions in the KMSearch ScriptLibrary: `getAvailableKnowledgeBases`, `getSelectedCollections`, and `getSelectedCollectionsString`.
- Removes the kmquery.default display options that reference the removed knowledgebase.

To delete a knowledgebase:

1. Click **Knowledge Management** > **Configuration** > **Knowledgebases**.
2. Click **Search**.
3. Select the knowledgebase you want to delete.
4. In the knowledgebase detail form, click **Delete** and then click Yes.
5. If it is a weblib or fsyslib type knowledgebase, you do not need to do anything else.
6. If it is an sclib type knowledgebase,continue to clean up any references to the knowledgebase by undoing the changes to the system that you made when you added the knowledgebase.
   a. Remove the tab for the knowledgebase on the kmknowledgebase.advsearch.g form, if you created one.
   b. Remove any knowledgebase-specific fields from the kmquery dbdict that you previously added.
   c. Remove any knowledgebase-specific references that you added to the KMSearch ScriptLibrary.
   d. Delete the read-only viewing format that you created for the knowledge candidates for the knowledgebase.
   e. Remove the format name that you added to the kmquery.linkrequest process record.
   f. Remove the links to this knowledgebase from the kmquery link record for an advanced search record.

Configure Advanced Search for Knowledge Management

User role: System Administrator

Prior to version 9.32, the KM Solr Search Engine does not support Full Match mode for advanced search against KM fields. For example, if you enter "Phone Troubleshooting" in the Title field, your search will return records whose title contains "phone" and also records whose doc body contains "troubleshooting".

Starting with version 9.32, the Solr Search Engine allows you to configure Advanced Search for KM, to enable or disable Full Match mode. You do so by configuring the Advanced Search Script (`<library name>_kmprocesslibcriteria`) for each sclib type knowledgebase.

To configure Advanced Search for a sclib knowledgebase:

1. Make sure you have already added each query field to dbdict `kmquery`.
2. Navigate to **Knowledge Management** > **Configuration** > **Knowledgebases** and open the knowledgebase.
3. On the **Type information** tab, click the Find button next to the Advanced Search Script field. The `<library name>_kmprocesslibcriteria` record opens.
4. For each "`field=value`" type query field, add an entry to the field mapping section, using this format:

   ```
   ["<query_field_name>", "<search_engine_alias>", <true or false>]
   ```

   Where:

   - `<query_field_name>` is the name of the field you added to dbdict "kmquery";
   - `<search_engine_alias>` is the alias specified for the query field in the **Field Definitions** tab of the knowledgebase;
   - `<true or false>`: This part indicates if Advanced Search uses full match mode for this field (when set to true, full match is used).

   The following are examples:

   ```
   this.fieldmapping = [
   ["incidentlib_number","number",false],
   ["incidentlib_status","problemstatus",true],
   ...
   ```

5. If you use custom search criteria that are not simply a "`field=value`" query, add it to the `processSpecial` function defined in the `<library name>_kmprocesslibcriteria` record.
6. Save the advanced search script.

Enabling Languages for KM Search

The Solr search engine supports a set of languages, however only some of them are officially supported in Service Manager. For more information, see "Supported Languages for the Solr Search Engine" below.

To enable a language for KM search, you must activate the language for KM from the language table, and enable it in the Solr search engine schema file.

- "Activate a Knowledge Management language" on the next page
- "Enable Languages in the Solr Search Engine" on page 365

Once you have enabled your languages, you can continue to do the following:

- "Create Search Engine Thesaurus Files" on page 367
- "Modify Stop Words" on page 369
- "Add a New KM Message to the scmessage Table" on page 370
- "Create a Hitlist with Multilingual Labels" on page 371

Supported Languages for the Solr Search Engine

Technically, the Solr search engine supports all languages listed in the **schemastub.xml** file, however only some of them are officially supported in Service Manager.

> **Important**: For Knowledge Management, HPE only provides official support for languages that are officially supported in Service Manager.

The following table lists all languages technically supported in the Solr search engine, and indicates which of them are officially supported in Service Manager.

Languages Supported in Solr Search Engine	Officially Supported in Service Manager?
ARABIC	Yes
CHINESE SIMPLIFIED/TRADITIONAL	Yes
CZECH	Yes
DANISH	No

Languages Supported in Solr Search Engine	Officially Supported in Service Manager?
DUTCH (STANDARD)	Yes
ENGLISH	Yes
FINNISH	No
FRENCH	Yes
GERMAN	Yes
GREEK	No
HEBREW	Yes
HUNGARIAN	Yes
INDONESIAN	No
ITALIAN	Yes
JAPANESE	Yes
KOREAN	Yes
NORWEGIAN NYNORSK	No
POLISH	Yes
PORTUGUESE	Yes
ROMANIAN	No
RUSSIAN	Yes
SLOVAK	No
SPANISH	Yes
SWEDISH	No
THAI	No
TURKISH	No
VIETNAMESE	No

Activate a Knowledge Management language

User role: System Administrator

Languages in the Solr search engine are identified by language codes known as "KM Identifier" values. When a KM Identifier value is assigned to a language, the language can be activated and enabled to be used by the search engine.

Note: Languages not containing a valid KM Identifier value are not supported by the search engine and should not be enabled for Knowledge Management. If they are enabled, the search engine will default to the English language processing rules for both searching and indexing.

To activate a language that has a KM Identifier value for the search engine:

Note: By default, the English language is activated.

1. Click **Tailoring** > **Database Manager**.
2. In the Table field, type **language** and then click **Search**.
3. Double-click the `language` form and click **Search**. A list of language identification records is displayed.
4. Select the applicable language identification record. The record is displayed.

   Note: There are three Chinese language records (Chinese Simplified, Chinese Traditional, and Chinese). Service Manager differentiates between Chinese traditional and Chinese simplified, but the search engine uses only one language file for both languages. To enable Chinese for the search engine, select Chinese.
5. Look at the KM Identifier field. If there is a valid KM Identifier value, then this language can be activated and enabled in the search engine. Following are some examples of the valid KM Identifier values that are stored in the language table.

Language	KM Identifier value
Arabic	ar
English	en
German	de
Spanish	es

6. Select the **Active for Knowledge Management** field to make the language available to be used in the Solr search engine.
7. Click **Save** and **OK**.
8. Users must log out and then log back in for the language activation to take affect.

Enable Languages in the Solr Search Engine

User role: System Administrator

The Solr search engine provides out-of-box languages that can be enabled to allow users to search for knowledge documents using key words in those languages. You can enable or disable languages in the Solr search engine that contain a valid "KM Identifier" value.

> **Note:** HPE recommends that you enable only those languages that are applicable to your knowledgebase. By default, English is the only language enabled.

To enable or disable languages in the Solr search engine:

1. Update the applicable `fieldType`, `field`, and `copyField` language entries in the **schemastub.xml** file.
   a. Locate the **schemastub.xml** file in the Service Manager home directory.
      i. In the Windows client, the default directory is: *C:\Program Files\HPE\Service Manager x.xx*
      ii. In the Linux environment, the install path is: */apps/smxxx/*
      iii. Once you locate the Service Manager home directory, the path to the **schemastub.xml** file is: */Server/RUN/km/styles/schemastub.xml*

   b. In the **schemastub.xml** file, find the reference for the language `fieldType` you want to enable (for example, **text_zh** for the Chinese language) and uncomment the entry.

      Note: The following XML comment tags start and end (surround) the language entry: <!--<fieldType> and </fieldType>-->

      Following is an example of the Chinese language entry:

      <!-- CHINESE SIMPLIFIED/TRADITIONAL -->

      <!-- <fieldType name="text_zh" class="solr.TextField" positionIncrementGap="100">

      <analyzer type="index">

      <tokenizer class="com.teragram.solr.AsianTaggingTokenizerFactory" filename="../../kmsearchengine/languages/data/zh.uhtagger" />

      </analyzer>

<analyzer type="query">

<tokenizer class="com.teragram.solr.AsianTaggingTokenizerFactory" filename="../../kmsearchengine/languages/data/zh.uhtagger" />

<filter class="solr.SynonymFilterFactory" synonyms="../../../languages/thesaurus/synonyms_zh.txt"/>

</analyzer>

</fieldType>

-->

c. Locate the solr field section to uncomment the applicable fields. You will see a list of language-specific docbody and adlearn fields (except docbody, docbody_en, adlearn, and adlearn_en will be commented).

d. Uncomment the applicable language `field` entry.

Note: Do not comment out the default `docbody` and `adlearn` fields. By default, the `docbody_en` and `adlearn_en` fields are enabled. You may safely comment them out if your system does not require English language processing.
For Example:
<!-- <field name="**docbody_zh**" type="text_zh" indexed="true" stored="true" multiValued="true"/> -->

<!-- <field name="**attachment_zh**" type="text_zh" indexed="true" stored="true" multiValued="true"/> -->

<!-- <field name="**adlearn_zh**" type="text_zh" indexed="true" stored="true" multiValued="true"/> -->

e. Uncomment the applicable language `copyField` entry.

Important: The three field entries (`fieldType`, `field`, and `copyField`) must match (you must uncomment all three fields to enable the language).

For example:
<!-- <copyField source="**docbody_zh**" dest="docbody"/> -->

<!-- copyField source="**attachment_zh**" dest="attachment"/ -->

f. Save your changes.

2. Update the Database Manager files.
   a. Click **Tailoring** > **Database Manager**.
   b. In the Table field, type **language** and then click **Search**.
   c. Double-click the `language` form and click **Search**. A list of language identification records is displayed.
   d. Select the applicable language identification record. For this example, there are two records: **Chinese Simplified** (zh-Hans) and **Chinese Traditional** (zh-Hant). The record is displayed.
   e. Select the **Active for Knowledge Management** field to make the language available for Knowledge Management.

      Note: The Service Manager Language table may contain language entries that are not supported by the search engine. Only languages with a valid **KM Identifier** value should be enabled.
   f. Click **Save** and **OK**. Your language should now be available in the locale dropdown on the Advanced Search screen, Contribute Knowledge screens, and for the default locale dropdown on the Manage Knowledgebases Type Information tab.
3. To disable a language that is no longer being used, do the following:
   a. Locate and comment the following entries in the **schemastub.xml** file: `fieldType`, `field`, and `copyField`

      Important: The three field entries (`fieldType`, `field`, and `copyField`) must match (you must comment all three field entries to disable the language).
   b. Save your changes.
   c. Go to the Database Manager identification record and uncheck the **Active for Knowledge Management** field to make the language unavailable for Knowledge Management.
   d. Save your changes.

Create Search Engine Thesaurus Files

The search engine uses the thesaurus when doing a simple search. A synonym search is a type of search that locates occurrences of either the search term or any of its synonyms. For example, a synonym search for computer might return documents that contain laptop or desktop .

Thesaurus expansion happens automatically for terms entered into the simple search screen and is not currently supported for advanced searches. The search engine performs thesaurus expansion on words

in the natural language query box. Thesaurus expansion is done using the dictionary that matches your login language. To use a different language dictionary, change the query language parameter on the advanced search form.

> **Note**: A synonym search term containing a phrase is not supported.

The search engine supports thesaurus files (or dictionaries) for individual languages, but none are provided out-of-box. You may create your own thesaurus dictionaries for use when searching content, or thesaurus expansion can occur automatically for terms that are entered into a simple search screen that is not currently supported by advanced search.

To add a thesaurus file for a certain language:

1. Go to the `{SERVICE_MANAGER_HOME}/Search_Engine/kmsearchengine/languages/thesaurus` folder, and create an empty text file named `synonyms_synonyms_<language id code>.txt`.

   > The thesaurus file name format includes the two-character language id. For example, the English thesaurus text file name is `synonyms_en.txt` and the French thesaurus text file name is `synonyms_fr.txt`.

2. Add content to the thesaurus file. The thesaurus file format is as follows:

```
# blank lines and lines starting with pound are comments.

#Explicit mappings match any token sequence on the left hand side of

 #"=>" and replace with all alternatives on the right hand side.

#Examples:

laptop, desktop => computer

#Equivalent synonyms may be separated with commas

#NOTE: When using commas in files, ensure that single-byte commas
#are used instead of double-byte commas.

#Examples:
foozball , foosball
universe , cosmos

#"computer, laptop, desktop" is equivalent to the explicit mapping:
computer, laptop, desktop => computer

#multiple synonym mapping entries are merged.
foosball => foosball
foozball => foozball

#is equivalent to
foosball => foosball, foozball
```

> **Caution**: When using commas to separate terms in files, you must use the single-byte commas instead of double-byte commas.

3. Save the file in UTF-8 encoding.

> **Cuation**: Because UTF-8 is part of the Unicode standard which enables you to encode text in practically any script and language, be sure you save your files in UTF-8 encoding.

Modify Stop Words

User role: System Administrator

A stop-word list is a list of terms that can be ignored when the search engine is searching or indexing. Typically, stop-word lists include short and common words or prepositions, such as "a," "the," or "with" in English. However, they may also include longer words, such as long number strings, or words that are too common to be useful as search targets, such as the term "internet."

Stop words are removed from words entered in the "Search for" box unless they are enclosed in double quotes (phrase search). They are not removed during indexing to allow for phrase searching.

Stop words are stored in Service Manager in lists by specific language. Not all languages support stop words (for example, Japanese and Chinese). Adjust the list of stop words by either adding or removing words from this list.

The stop-word list for your log-in language is used by default, and is loaded once when you first log in. Changing the query language parameter on the advanced search screen changes the stop-word list used. The new stop-word list is loaded each time you search in a language other than your log-in language. This may cause a delay in your search being submitted as the stop-word list is loaded. If you need to perform extensive searches in a language other than your log-in language, HPE recommends that you log out and then log back in the other language to reduce this delay.

To modify stop words:

1. Click **Knowledge Management > Configuration > Stopwords**.
2. Click **Search**.
3. Select the record for the language code you wish to change.
4. Add a new word or modify an existing word.
5. Click **Save**.

Add a New KM Message to the scmessage Table

User role: System Administrator

Use this procedure to add a new message (token), which makes a label multilingual. After you create this new message, use the Message ID to update the label field for the hitlist you want to be multilingual.

1. Type **db** in the command line or navigate to Database Manager (click **Tailoring > Database Manager**).
2. Type scmessage in the Table box.
3. Click **Search**.
4. Type km in the Class box of the HPE Service Manager Message form.
5. Click **Search**.
6. Review the list of existing km-related system messages.
7. Add a new record where the class is km, the language code is the language of the string being added, the Message ID is unique within the class, and the text string is the text you want to display in the label of the hitlist.
8. Make a note of the Message ID number. You will need it to update the label field and when you add the text strings for the other languages you want to use for this hitlist label.
9. Click **Save** to create the new record.

Use this procedure to add message text in an additional language for an existing message ID.

1. Type **db** in the command line or navigate to Database Manager (click **Tailoring > Database Manager**).
2. Type scmessage in the Table text box.
3. Click **Search**.
4. Type km in the Class box of the HPE Service Manager Message form.
5. Click **Search**.
6. Review the list of existing km-related system messages to find the message number of the message for which you want to add the new language text.

7. Add a new record where the class is km, the language code is the language of the string being added, the Message ID matches the Message ID of the label token for this language, and the text string is the text in the language you want to display in the label of the hitlist.
8. Click **Save** to create the new record.

Create a Hitlist with Multilingual Labels

User role: System Administrator

In addition to creating new document views, administrators can configure the labels for the document view to display in languages other than English.

Note: This procedure is for a hitlist that is not multilingual-enabled. Before you begin, make sure you create a message number ID for each multilingual label and that the message number is defined to display labels in multiple languages.

To create a hitlist with multilingual labels:

Note: The default hitlist is multilingual-enabled in the out-of-box system.

1. Click **Knowledge Management > Configuration > Configure Hitlists**.
2. Click **Search**.
3. Select the hitlist to update.
4. Type the label delimiter (*SCMSG*123*SCMSG*) in the Label field for the label you are making multilingual. The 123 should be the message number ID from the `scmessage` table for the unique message number ID for this label.
5. Continue adding additional label delimiters for each of the multilingual labels in the hitlist.
6. Click **Save**.

Indexing the Knowledgebases

Indexing is performed in the background. A background process, KMUpdate, is responsible for starting the indexer. Indexing a knowledgebase includes submitting records to the `kmknowledgebaseupdates` table.

> **Caution:** There can be only **one** KMUpdate process running at any time. Starting more than one KMUpdate process causes unpredictable behavior on the search engine server.

When scheduled, KMUpdate runs every 5 minutes by default. This Repeat Interval is defined in the KMUpdate schedule record. When KMUpdate runs, the indexer starts. The indexer first queries for all knowledgebases of sclib type. Each knowledgebase has a field called `interval`. There is also an internal field called `current interval`. The indexer first checks that the interval value is not set to zero. An interval of zero causes the indexer to skip any further processing on this knowledgebase and the indexer then moves to the next knowledgebase in the list. If the interval is greater than zero, the indexer compares the value of interval to the value of the internal interval. If they do not match, the internal interval is incremented by 1 and saved. The indexer then skips any further processing of this knowledgebase and moves to the next knowledgebase in the list.

When the values of interval and internal interval match, the indexer queries the `kmknowledgebaseupdates` table for records matching the knowledgebase and begins processing them. Because of processing time, the intervals cannot be based on elapsed time. An interval of two would be 10 minutes only if all records from any knowledgebase with an interval of one were processed in under five minutes. Once complete, the indexer will move to the next knowledgebase in the list. KMUpdate is suspended during indexing so that it cannot start any new indexing until the indexer completes all knowledgebases in its list to prevent overlapping indexing.

Indexing a knowledgebase includes submitting records to the `kmknowledgebaseupdates` table. There are two ways to submit records to the `kmknowledgebaseupdates` table.

- When an administrator selects **Full Reindex** on the Knowledgebase Maintenance form (the Status tab), the system performs the following processing:
  a. Delete the old knowledgebase index.
  b. Create a new empty knowledgebase index based on the current knowledgebase settings.
  c. Remove all records for the knowledgebase from the `kmknowledgebaseupdates` table.
  d. Execute the query provided on the Type Information tab, adding all matching records to the `kmknowledgebaseupdates` table.

- When any record is modified in any table that has a knowledgebase associated with it, there are triggers in the tables associated with a knowledgebase that cause records to be submitted to the `kmknowledgebaseupdates` table.

Managing the KMUpdate process

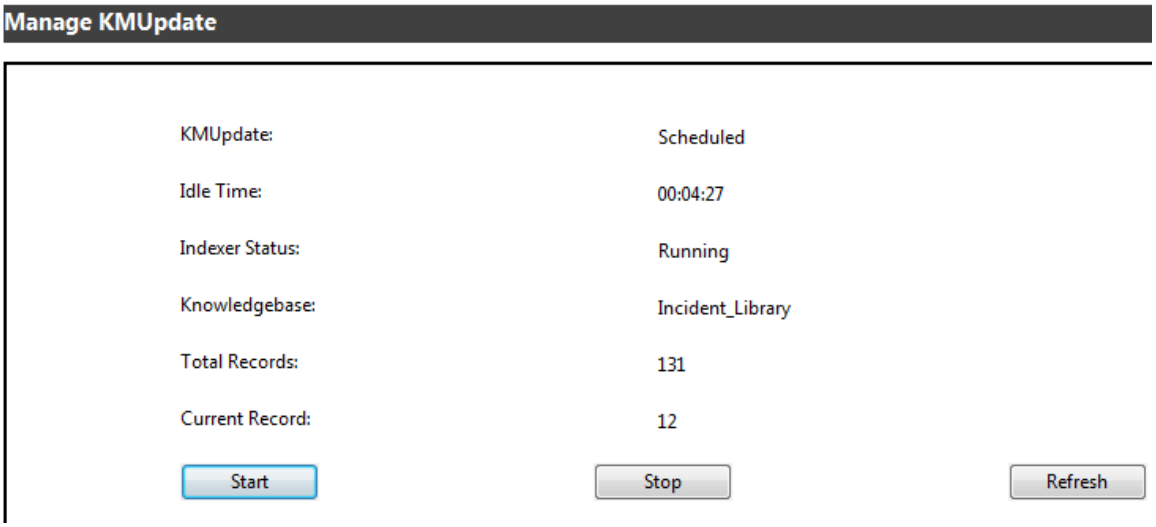
The KMUpdate process controls indexing, which runs in the background. You use the Update Indexes form to stop and restart indexing, and to view the status statistics relating to indexing. If indexing has not started when you stop the KMUpdate process, the interval counter resets and the interval does not begin counting down until you start indexing.

> **Tip:** You can also type `status` in the Command window to display any processes currently running in the system, and this will include the KMUpdate process. You can use the `kill` command to stop indexing or stop any scheduled indexing. Typically, this is only accessible to and done by a System Administrator.

To access the Update Indexes form, navigate to **Knowledge Management** > **Configuration** > **Update Indexes**.

Field	Description
KMUpdate:	Displays whether or not the KMUpdate process is scheduled: **Scheduled**, **Not Scheduled**.
Idle Time:	When the KMUpdate process is scheduled, this field displays the amount of time the process has been idle. When this count reaches the Repeat Interval of the KMUpdate schedule record (default: 5 minutes), the KMUpdate process starts the indexer. If the indexer finds pending updates to the scheduled knowledgebase, the indexer processes them. Otherwise, the indexer updates the internal interval counter.
Indexer Status:	Displays the status of indexing: **Idle**, or **Running**.
Knowledgebase:	Displays the name of the knowledgebase currently being indexed.
Total Records:	Displays the total number of records in the knowledgebase being indexed.
Current Record:	Displays the current number of records that have been processed. Click **Refresh** to view the most current statistics for indexing that is in progress. (For the web client, click **More** > **Refresh Statistics**.)

The following figure shows a scenario where the indexer is indexing the Incident_Library knowledgebase.



(Optional) Enable Incremental Indexing

When you have a huge number of documents to index (for example, hundreds of thousands of documents or even more), the indexing process may take quite long. By default, autoCommit is disabled in the Solr search engine, which means indexed documents are not committed to the search engine and hence not searchable to users until the entire indexing process is complete. Optionally, you can enable incremental indexing so that partial indexed documents are searchable before the initial indexing phase is complete.

In a master-slave environment, perform the following tasks to enable incremental indexing.

Task 1. Enable autoCommit on the master server

To do this, follow these steps:

1. Open the <search engine root directory>\kmsearchengine\KMCores\kmcore\conf\solrconfig.xml file of the master server in a text editor.
2. Specify a value for the maxDocs parameter.
   a. Locate the following line:

      ```
      <updateHandler class="solr.DirectUpdateHandler2" />
      ```

   b. Change this line to the following:

      ```
      <updateHandler class="solr.DirectUpdateHandler2">
          <autoCommit>
      ```

```
    <maxDocs>%{maxDocs}%</maxDocs>
    </autoCommit>
  </updateHandler>
```

Where: **%{maxDocs}%** is a number (for example, 10000) that represents the maximum number of uncommitted documents that are allowed before an auto commit is triggered. When the number of uncommitted documents reaches this threshold, Solr performs a commit and saves the data to its index. Once committed, the documents are searchable to users.

3. Modify the replication setting of the master server.

   a. Locate the following tag:

   ```
   <requestHandler name="/replication" class="solr.ReplicationHandler" >
   ```

   b. Change the content of this tag to the following:

   ```
   <requestHandler name="/replication" class="solr.ReplicationHandler" >
     <lst name="master">
       <str name="replicateAfter">commit</str>
       <str name="replicateAfter">startup</str>
       <str name="confFiles">schema.xml</str>
    </lst>
   </requestHandler>
   ```

   With this configuration, after the master server is started or has performed a commit, it creates tags that identify the files that have been changed. The slaves will then poll the master server and replicate the updated files from the master based on the tags created.

Task 2. Configure replication on the slave server

> **Note:** Repeat the following steps for each slave server.

1. Open the <search engine root directory>\kmsearchengine\KMCores\kmcore\conf\solrconfig.xml file of the slave server in a text editor.
2. Change the content of the replication requestHandler entry to the following:

```
<requestHandler name="/replication" class="solr.ReplicationHandler" >
  <lst name="slave">
     <str name="enable">${enable.slave:true}</str>
    <str name="masterUrl">http://<hostname>:<port>/KMCores/${solr.core.name}
 /replication</str>
    <!-- str name="pollInterval">00:00:20</str -->
  </lst>
 </requestHandler>
```

Where: The **hostname** and **port** parameter values are the host name and port of the master server. You can uncomment the **pollInterval** parameter if you want the polling job to run at a specified interval.

> **Caution:** Either of the tasks requires a full re-index of the knowledgebases for the changes to take effect. Next, you need to perform a full reindex of all knowledgebases. For details, see "Perform a Full Reindex on a Knowledgebase" below.

Perform a Full Reindex on a Knowledgebase

User Role: System Administrator, KMAdmin

After you have upgraded from the K2 Search Engine to the Solr Search Engine or after you have installed the Solr Search Engine, you need to perform a full reindexing for all of your knowledgebases.

Knowledgebase maintenance error reporting

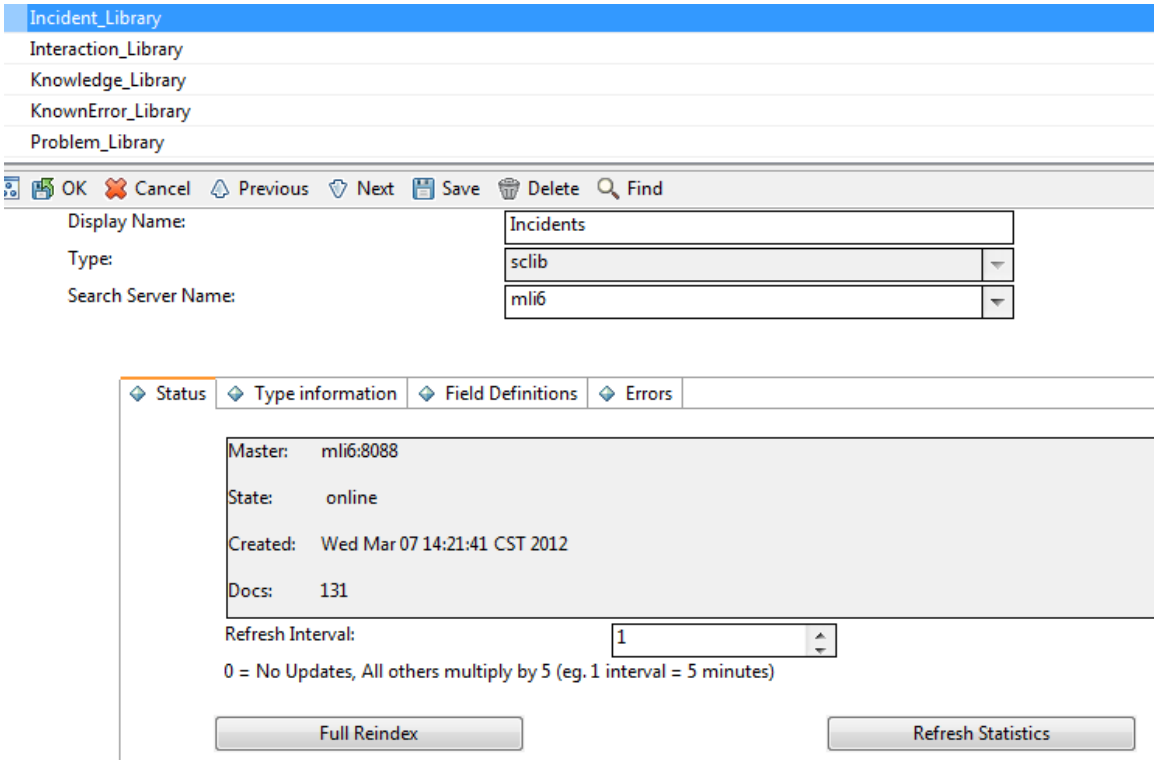
The Knowledgebase Maintenance form contains an **Errors** tab that lists any errors found during indexing. The listed errors apply only to the selected knowledgebase. Once the error is corrected and the document re-indexed, the system removes the error from the list.

The **Errors** tab displays the document ID for the document containing the error and an error message that identifies the error found during indexing. When a document contains an error, you should edit the document and submit it again so that the document can be indexed during next indexing interval. This will make the document available in the knowledgebase.

To perform a full re-index of a knowledgebase, follow these steps:

1. Navigate to **Knowledge Management > Configuration > Knowledgebases**, and click **Search**.
2. Select a knowledgebase from the list.
3. Check that the **Search Server Name** field contains the name of a search server that is connected.
4. On the **Status** tab, click **Full Reindex**.

   The Search Engine starts to index all records in the knowledgebase. Once the indexing is complete, the knowledgebase state changes from **offline** to **online**, and the creation time of the indexes is displayed in the **Created** field.
5. Click **Refresh Statistics**. The total number of records that have been indexed is displayed.



6. Click the **Errors** tab to see if any errors occurred during the indexing and fix them as needed.
7. Do a search against this knowledgebase to verify that the search works properly.
   a. Click **Knowledge Management** > **Search Knowledgebase**.
   b. Select the knowledgebase in the **Search In** section.

      > If the knowledgebase has not been successfully indexed, it is in offline state and not displayed in the **Search In** section.

   c. Enter a search word.
   d. Click **Search**.

      A list of search results is displayed, together with a message that resembles the following: "XXX records found. YYY records searched."

Enforcing Mandanten Security in Knowledge Management

User role: System Administrator

Service Manager offers a security feature called Mandanten for any searches performed within Service Manager. Because the Knowledge Management module uses a third-party search engine (the Solr search engine), it does not apply the settings for Mandanten protection that may have been defined for Service Manager searches against these tables by the customer. You can utilize Mandanten protection for searches executed by the Knowledge Management module to ensure that all searches against these tables comply with the security requirements defined by Mandanten.

Introduction to Mandanten Security

Typically, Mandanten is set up based on the company of the user who is accessing the system, though it can be set up based on any value in any table that needs to be protected. Mandanten protection is set up on a per-table basis. The operator can be a member of one, many, or no security groups. The security groups (`scsecuritygroups` table) set values that define which records the user is allowed to see based on the content of the mandant field; the mandant field is set up for each table in the `scmandant` record. More flexible queries for each table and security group can be added to the `scaccess` table. However, when a user enters a search anywhere within Service Manager, the Mandanten restrictions are appended to that query upon execution, and restricted records will not be part of the returned record set.

Queries executed outside of Service Manager, such as with the Solr search engine, are not Mandanten protected. Information shown in the Knowledge Management hit list is not yet retrieved from the Service Manager internal files. When you select a record from the hit list for viewing, it will then access the Service Manager internal file (such as `probsummary`) that is under Mandanten protection. Access to the record will then be denied based on the Mandanten restrictions, even if the record was displayed in the hit list. To prevent this from happening, update the KM search security scripts to read Mandanten settings and apply these settings to the hitlist as well. For details, see "Update a KM Search Security Script for Mandanten Security" on the next page.

How to Enable Mandanten Security in Knowledge Management

To enable Mandanten security in Knowledge Management, you need to:

1. Set up Mandanten protection according to the online help documentation:
   - The operator needs to belong to one or many security groups.
   - Security groups must have one or many “include” and/or “exclude” values.
   - The `scmandant` file must have a record for the table to protect and define a field in that table as the mandant field.
2. Ensure that all fields used in the `scmandant` and `scaccess` files are defined in the Knowledgebase record’s **Field Definitions** tab. See "Add an sclib Knowledgebase" on page 335.
3. Modify the search security script for the library that uses Mandanten protection, as described in "Update a KM Search Security Script for Mandanten Security" below.

> **Note:** Make sure to run the full re-index as an operator without Mandanten limitations, since the Mandanten query that enforces security on the originating table will limit the records read during the re-index operation.

Update a KM Search Security Script for Mandanten Security

User role: System Administrator

To enable Mandanten security for a library, you need to update its Search Security Script. The following steps use the Incident Library as an example.

1. Open the `Incident_Library_kmsearchsecurity` JavaScript in the ScriptLibrary. The out-of-box security script is as follows:

   ```
   function getSecurityInfo(user, record)
   {
   ```

```
return "";

}
```

2. Change the script above to the following.

```
* Convert the security control from K2 to Solr.

* The security settings come from the security group / field, and Mandanten
security restriction query string.

* There is no need to change the record type for different libraries,

* because the record passed in defines the library and contains the record type
information.

*/

if (!('unique' in Array.prototype)) { /* add function to remove the duplicated
element in array, sort the array first */
       Array.prototype.unique = function(that /* opt */) {
               this.sort();
               for ( var i = 1; i < this.length; i++ ) {
                   if ( this[i] === this[ i - 1 ] ) {
                       this.splice( i--, 1 );
                   }
               }
       };
}
if (!('forEach' in Array.prototype)) { /* add function to iterate element in
array */
  Array.prototype.forEach = function(action, that /* opt */) {
    for ( var i = 0, n = this.length; i < n; i++)
      if (i in this)
        action.call(that, this[i], i, this);
  };
}
/**
 * generate the security information according to the user passed in.
 * @param user, user name
 * @param record, obsoleted parameter.
 * @returns {String}
 */
function getSecurityInfo(user, record) {       /* record stands for the current
library record */
       var querystr = "";
       /* as the table name is already stored in library record, no need to change it
for different library*/
       var tablename = record.sclibtablename;
       var operatorFile = new SCFile("operator");
       var rc = operatorFile.doSelect("name=\"" + user + "\"");
```

```
        if (rc == RC_SUCCESS) {
                var securitygroups = operatorFile.security_group;
                var mandant = new SCFile("scmandant");
                var rc_mandant = mandant.doSelect("filename=\"" + tablename + "\"");
                if (rc_mandant == RC_SUCCESS) {
                        var mandantField = mandant.fieldname;
                        querystr = checkSecurityGroup(securitygroups, mandantField, tablename);
                }
        }
        if (querystr == "()") {
                querystr = "";
        }
        return querystr;
}

/**
 * generate the query string according to the security group passed in
 * @param groups, security group ID
 * @param field, field to add security control
 * @returns {String}, query string contains the mandant security setting.
 */
function checkSecurityGroup(groups, field, tablename) {
        if(field == null) field ="";
        field = field.replace('.','');
        var secgroup = new SCFile("scsecuritygroup");
        var sm_query = "";
        var includeList = new Array(); /* value list within the security control */
        var excludeList = new Array(); /* value list outside the security control */
        var restrictions = new Array();
        var sql = "security.id isin " + system.functions.str(groups);
        var rc = secgroup.doSelect(sql);
        while(rc == RC_SUCCESS){
                includeList = includeList.concat(secgroup.include.toArray());
                excludeList = excludeList.concat(secgroup.exclude.toArray());
                var restriction = get_scaccess_query(secgroup.security_id, tablename);
                if(restriction) restrictions.push(restriction);
                rc = secgroup.getNext();
        }
        if(field && includeList.length>0 ){
                includeList.unique();
                sm_query = field + ":(" + includeList.toString() +")"; /* add include value
list to query */
        }


        if(excludeList.length>0 && field){ /** add exclude value list to query */
                excludeList.unique();
                if(sm_query) {
```

```
                        sm_query += " AND ";
                }
                sm_query += "NOT " + field + ":(" + excludeList.toString() +")";
        }
        sm_query = sm_query.replace(/,/g,', '); /* add a whitespace after separator in
array ',' => ', ' */

        restrictions.forEach(function(item){ /* add mandanten restrict query to km
search string*/
                if(sm_query){
                        sm_query += ' AND ' + item;
                } else {
                        sm_query += item;
                }

        });
        return sm_query;
}

/**
 * get restrict query for security group
 * TODO: get the solr field name from library
 * for now, the solr field name simply removes the '.'(dot) in SCFile field
name.
 */
function get_scaccess_query(groupId, tablename){
        var restriction = '';
        var scaccess=new SCFile("scaccess");
        var rc=scaccess.doSelect("filename=\"" + tablename +"\"" + "and
security.id=\""+groupId+"\"");
        if(rc == RC_SUCCESS){
                var query = scaccess.restricting_query;
                restriction = parse(query);
        }
        return restriction;
}

/**
 * convert the restrict query to solr query string
 * @param sql query string in restrict query.
 * @returns {String}
 */
function parse(sql){
        sql = replaceAND(sql);
        sql = replaceOR(sql);
        sql = replaceISIN(sql);
        sql = replaceNotEqual(sql);
        sql = replaceEqual(sql);
```

```
        sql = replaceEmbrace(sql);
        sql = convertToSolrFields(sql);
        sql = replaceQuote(sql);
        return sql;
}

/**
 * convert 'and' to 'AND'
 * @param str
 * @returns
 */
function replaceAND(str){
        return str.replace(/\band\b/g,'AND');
}

/**
 * convert 'or' to 'OR'
 * @param str
 * @returns
 */
function replaceOR(str){
        return str.replace(/\bor\b/g,'OR');
}

/**
 * convert 'isin' to ':'
 * @param str
 * @returns
 */
function replaceISIN(str){
        return str.replace(/\s*isin\s*/,':');
}

/**
 * convert 'a~=b' to 'NOT a:b'
 * @param str
 * @returns
 */
function replaceNotEqual(str) {
        return str.replace(/\w+\s*~=\s*\w+/g,function(word){
        word = word.replace(/\s+/g,'');
        return 'NOT '+ word.replace(/~=/,':');
});
}

/**
 * convert 'a=b' to 'a:b'
 * @param str
```

```
 * @returns
 */
function replaceEqual(str) {
	return str.replace(/=/g,':');
}

/**
 * convert to solr fields
 * 'a.b.c.d' => 'abcd'
 */
function convertToSolrFields(str) {
	return str.replace(/[.](\w+)/g,"$1");
}

/**
 * convert '{a,b}' to '(a, b)', add a whitespace after comma to adjust solr
query format
 * @param str
 * @returns
 */
function replaceEmbrace(str) {
	str = str.replace(/{/g,'(');
	str = str.replace(/}/g,')');
	str = str.replace(/,/g,', ');
	return str;
}
/**
 * replace double/single quote in given string
 * @param str
 * @returns
 */
function replaceQuote(str) {
	str = str.replace(/"|'/g,'');
	return str;
}
```

Differences between Solr and K2 Search Security Scripts

Service Manager applications versions earlier than 9.30 support the K2 search engine. Instructions on how to enable Mandanten security for the Knowledge Management module that uses the K2 search engine can be found in this knowledge document:
https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM436754

For Knowledge Management that uses the Solr search engine, you should follow the instructions in this document. Pay attention to the following differences:

- For the Solr search engine, you no longer need to change the file names for individual libraries, because each knowledgebase record now already contains the record type information, which the search security script will parse as search configuration.
- For the Solr search engine, each search security script already contains the security control defined in Mandanten security groups/ Mandanten security restriction queries. The operator in each query will be parsed based on the mappings listed in the following table to match the Solr query.

K2	Solr
field=value	field:value
filed~=value	NOT field:value
field='value'	field:value
field.fieldext:value	fieldfieldext:value
field isin {value0,value1}	field:(value0, value1) **Note**: There is a whitespace after the comma.
field=value or field=value1	field:value OR field:value1

Searching the Knowledgebases

When searching the knowledgebases, you can perform:

- A **simple search** where you search for a text string;
- An **advanced search** where you can provide several search parameters. In the advanced search you can specify the knowledgebases to search and the document categories to search. You can also specify a set of filtering parameters, such as exact phrase and creation date.
- A search within the search results after doing an initial search or advanced search.

Each of the knowledgebases has different fields that are indexed for searching, so when you search a knowledgebase, provide search parameters that match the fields in the knowledgebase. For example, the knowledge articles have a title and author field. When you view an incident, the out-of-box system displays the incident number, incident description, and solution for closed incidents.

The out-of-box system includes five separate knowledgebases that can be searched collectively or separately, depending upon what information you are searching for. In addition to making your search more efficient by specifying a knowledgebase, it is also best to search with a limited number of document categories. When you search, your log-in profile determines what information you can search and view.

You can use the Knowledgebase Maintenance feature to add additional knowledgebases for searching. These knowledgebases are created from a table in Service Manager (sclib) or by using web crawling to browse and index an external web site (weblib).

For more information, see the Service Manager Help Center.

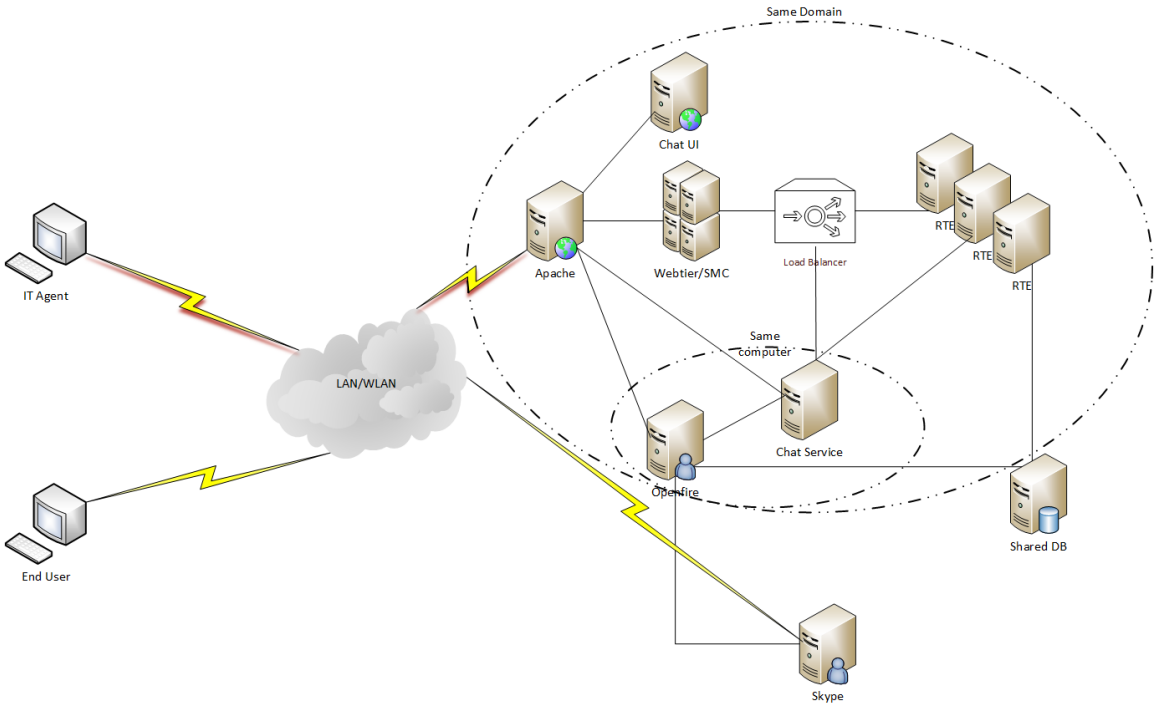
Install Service Manager Collaboration

HPE Service Manager Collaboration is an instant messaging solution combining IT Collaboration and End User Chat. IT Collaboration enables Service Manager IT operators to collaborate in real-time (or anytime) when handling an Interaction, Incident, Incident Task, Request, Request Task, Problem, Problem Task, Change, or Change Task. End User Chat builds a communication channel between the Service Manager Service Portal users or the Employee Self-Service (ESS) portal users and the Service Manager Service Desk agents so as to increase IT efficiency, improve customer satisfaction and reduce IT support costs.

Follow these instructons to install Service Manager Collaboration.

Service Manager Collaboration deployment scenario

The following diagram illustrates a typical HPE Service Manager Collaboration (SMC) deployment scenario.



Service Manager Collaboration cooperates with the following essential factors and Service Manager components:

- Openfire chat server:

  Openfire is a real time collaboration (RTC) server licensed under the Open Source Apache License. Service Manager Collaboration communicates with Openfire by using the widely adopted open protocol XMPP to approach all the operations, such as setting up conversations, posting messages, presence management, notification management and so on. The Openfire server also links Service Manager and other messaging applications, such as Microsoft Skype for Business.

- Apache:

  The Openfire server must be deployed behind the Apache HTTP server and use it as a reverse-proxy to protect the sensitive information of Openfire, such as the IP address, ports, and so on.

- Service Manager web tier:

  Service Manager Collaboration is embedded in Service Manager web tier to access the Openfire server through Apache for instant messaging.

- Chat service:

  Service Manager Chat service provides both the RESTful web service and the virtual agent chat service to the chat clients. It also connects the Openfire chat server to the Service Manager server and manages chat requests between an end user, a virtual agent and a live agent.

- Chat UI

  Deploy the End User Chat window to enable a Service Manager web tier ESS user or a Service Portal user to chat with either a virtual agent or a live agent.

Additionally, Service Manager Collaboration needs the following prerequisites and configurations:

- Light-Weight Single Sign-On (LW-SSO):

  Service Manager Collaboration uses LW-SSO to access and authenticate users. Service Manager Collaboration requires that you configure LW-SSO for the Service Manager web tier and the Openfire chat server.

Prerequisites

The necessary prerequisites for Service Manager Collaboration deployment are described as follows:

- You must have the Apache configuration knowledge.
- You have installed version 9.50 of the Service Manager binaries, applications, and web tier.
- You must know the domain of your Service Manager installation. In the example steps described in this document, the domain is **training.com** and the host name is **sm950.training.com**.
- In the example steps described in this document, chat server, chat service, Apache, Tomcat, and the Service Manager server are all installed on the same host.

Requirements

To deploy Service Manager Collaboration successfully, read through the checklist below and make sure the configurations are completed by following the instructions provided in this document:

- Integrate Tomcat successfully with Apache OpenSSL.
- Deploy Openfire successfully.
- Configure proxy pass correctly in Apache.
- Configure LW-SSO correctly for Service Manager webtier, RTE and Openfire.
- Set the related parameters correctly in Service Manager.

Deploy Service Manager Collaboration with HTTP

The Collaboration deployment with HTTP involves the following tasks. Note that these tasks are described using examples, which you may need to adjust according to your actual environment.

Task 1: Enable LW-SSO on the Service Manager server

For Service Manager Collaboration to function, you need to configure Lightweight Single Sign-On (LW-SSO) on the Service Manager server, Service Manager web tier and Openfire service so that Service Manager users can use Service Manager Collaboration without logging on to the Service Manager server separately.

In this task, you will set up LW-SSO for the Service Manager Server. Follow these steps:

1. Log on to Service Manager as a system administrator.
2. Go to Windows Services, and stop the **HPE Service Manager 9.50 Server** service.
3. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\Server\RUN directory.
4. Make a copy of the lwssofmconf.xml file, and save the copy as lwssofmconf_OOB.xml.
5. Open the lwssofmconf.xml file with a text editor.
6. Locate the `enableLWSSOFramework` parameter, and ensure that it is set to `true`.

   ```
   <enableLWSSO
   enableLWSSOFramework="true"
   enableCookieCreation="true"
   cookieCreationType="LWSSO"/>
   ```

7. Change the `domain` value to `training.com`.

   ```
   <domain>training.com</domain>
          <crypto cipherType="symmetricBlockCipher"
          engineName="AES" paddingModeName="CBC" keySize="256"
          encodingMode="Base64Url"
          initString="This is a shared secret passphrase"/>
   ```

   > **Note:** To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application to the web tier can log in but may be forcibly logged out after a while.

8. Change the `initString` value to `sm950training`.

```
<domain>training.com</domain>
          <crypto cipherType="symmetricBlockCipher"
          engineName="AES" paddingModeName="CBC" keySize="256"
          encodingMode="Base64Url"
          initString="sm950training"/>
```

> **Note:** This value can be set to any string that is at least 12 characters long, as long as you use the same `initString` value for all the products that you want to integrate through LW-SSO.

9. Save and close the lwssofmconf.xml file.
10. Start the **HPE Service Manager 9.50 Server** Windows service.

Task 2: Enable LW-SSO on the Service Manager web tier

In this task, you will enable LW-SSO in the Service Manager web tier so that Service Manager users can use Collaboration without logging on to the Service Manager server separately.

> **Note:** If SAML Single Sign-On (SSO) is enabled for Service Manager, you should configure LW-SSO for SM Collaboration as follows:
>
> - Enable LW-SSO in the SM Server
> - Disable LW-SSO in the SM web tier
> - Enable LW-SSO in the Openfire chat server
> - Enable LW-SSO in the HPE Identity Manager (IdM) service

> **Note:** As an example, this task uses Tomcat 8.0 as the web application server and **Tomcat 8.0_SMWeb** as the name of the Tomcat installation root directory.

Follow these steps:

1. Stop the Tomcat web application server.
2. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF directory.
3. Make a copy of the web tier configuration file (web.xml) and save it as web_OOB.xml.
4. Open the web.xml file with a text editor.
5. Set the `serverHost` parameter to the Service Manager server's FQDN. In the all-in-one example steps described in this document, set this parameter to `sm950.training.com`.

   ```
   <init-param>
   <!-- Specify the HPE Service Manager server host and port location -->
   ```

```
        <param-name>serverHost</param-name>
        <param-value>sm950.training.com</param-value>
</init-param>
```

6. Set the `secureLogin` parameter to `false`.

```
<context-param>
        <param-name>secureLogin</param-name>
        <param-value>false</param-value>
</context-param>
```

7. Set the `isCustomAuthenticationUsed` parameter to `false`.

```
<context-param>
        <param-name>isCustomAuthenticationUsed</param-name>
        <param-value>false</param-value>
</context-param>
```

8. Search for "LWSSO filter".

```
<!-- LWSSO filter for integrations using HP lightweight single sign-on
PLEASE NOTE: Uncomment this filter and the associated filter-mapping,
and see application-context.xml for additional configuration needed
for LWSSO. -->
<!--
        <filter>
        <filter-name>LWSSO</filter-name>
        <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
        </filter>
-->
```

9. Uncomment the LWSSO filter section by removing the comment tags.

```
<filter>
        <filter-name>LWSSO</filter-name>
        <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
</filter>
```

10. Search for "LWSSO filter-mapping".

```
<!-- LWSSO filter-mapping, please read description for LWSSO filter above
before uncommenting this. -->
<!--
        <filter-mapping>
        <filter-name>LWSSO</filter-name>
        <url-pattern>/*</url-pattern>
        </filter-mapping>
-->
```

11. Uncomment the LWSSO filter mapping section by removing the comment tags.

```
<filter-mapping>
       <filter-name>LWSSO</filter-name>
       <url-pattern>/*</url-pattern>
       </filter-mapping>
```

12. Save and close the web.xml file.
13. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF\classes directory.
14. Make a copy of the lwssofmconf.xml file, and save it as lwssofmconf_OOB.xml.
15. Open the lwssofmconf.xml file with a text editor.
16. Set the `enableLWSSOFramework` parameter to `true`.

```
<enableLWSSO
       enableLWSSOFramework="true"
       enableCookieCreation="true"
       cookieCreationType="LWSSO"/>
```

17. Set the `domain` parameter to `training.com`.

```
<lwssoValidation id="ID000001">
       <domain>training.com</domain>
       <crypto cipherType="symmetricBlockCipher"
       engineName="AES" paddingModeName="CBC" keySize="256"
       encodingMode="Base64Url"
       initString="This is a shared secret passphrase"/>
```

18. Set the `initString` parameter to `sm9xxtraining`.

```
<lwssoValidation id="ID000001">
           <domain>training.com</domain>
           <crypto cipherType="symmetricBlockCipher"
           engineName="AES" paddingModeName="CBC" keySize="256"
           encodingMode="Base64Url"
           initString="sm950training"/>
```

19. Set `secureHTTPCookie` to `false`.

```
<creation>
       <lwssoCreationRef useHTTPOnly="true" secureHTTPCookie="false">
       <lwssoValidationRef refid="ID000001"/>
       <expirationPeriod>50</expirationPeriod>
       </lwssoCreationRef>
       </creation>
```

20. In the `multiDomain` section, set the first DNS Domain to `training.com` and the first FQDN to `sm950.training.com`.

```
<multiDomain>
       <trustedHosts>
       <DNSDomain>training.com</DNSDomain>
       <DNSDomain>example1.com</DNSDomain>
       <NetBiosName>myserver</NetBiosName>
       <NetBiosName>myserver1</NetBiosName>
       <IP>xxx.xxx.xxx.xxx</IP>
       <IP>xxx.xxx.xxx.xxx</IP>
       <FQDN>sm950.training.com</FQDN>
       <FQDN>myserver1.example1.com</FQDN>
       </trustedHosts>
</multiDomain>
```

21. Save and close the lwssofmconf.xml file.
22. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF\classes directory, make a copy of the application-context.xml file and save it as application-context_OOB.xml.
23. Open the application-context.xml file with a text editor.
24. Locate the following line:

```
<sec:filter-chain pattern="/**"
filters="securityContextPersistenceFilter,anonymousAuthFilter"/>
```

25. Add `lwSsoFilter` to this line as follows:

```
<sec:filter-chain pattern="/**"
filters="securityContextPersistenceFilter,lwSsoFilter,anonymousAuthFilter"/>
```

> **Caution:** Use the correct case for **lwSsoFilter**.

26. Search for `bean id="lwSsoFilter"` to locate the lwSsoFilter bean.

```
<!--
       <bean id="lwSsoFilter"
class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
       <property name="authenticationManager">
       <ref bean="authenticationManager"/>
       </property>
       <property name="defaultRole">
       <value>ROLE_PRE</value>
       </property>
       </bean>
-->
```

27. Uncomment the lwSsoFilter bean by removing the comment tags shown in the previous step.
28. Save and close the application-context.xml file.

29. Go to Windows Services, and start the **Apache Tomcat 8.0 SMWeb** service.

Task 3: Test LW-SSO with the Service Manager web tier

In this task, you will verify if your Service Manager LW-SSO configuration works.

1. Access your tomcat link with the Tomcat server's FQDN. In the all-in-one example steps described in this document, access http://sm950.training.com:8080/webtier-9.50/index.do in your web browser to display the Service Manager login screen.
2. Log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

   If you are directed to a "Logout Successful" page, there may be issues with your LW-SSO configuration. Check all your files from the previous tasks and then try again.

   > **Caution:** From now on, you must use the fully qualified domain name (FQDN) in the web tier URL when logging on to Service Manager.

Task 4: Install Java for the chat server

In this task, you will install Java (64-bit recommended) and then set the `JAVA_HOME` variable for the chat server. If you are using your own server and already have Java installed, set `JAVA_HOME` to the location of your JDK and follow step 6 only.

Follow these steps:

1. This task uses the latest Java 8. Download the latest version of Java from the Java website.

   > **Note:** This task uses 32-bit Java as an example.

2. The system displays the welcome screen. Click **Next**.
3. Accept the default installation folder (C:\Program Files (x86)\Java\jdk1.8.0_xx), and then click **Next** to start the Java installation process.
4. On the JRE Destination Folder screen, accept the default installation folder (C:\Program Files (x86)\Java\jdk1.8.0_xx) and click **Next**.
5. When the Java installation is complete, click **Close**.
6. Add a new environment variable for the server.

Field	Value
Variable name	JAVA_HOME
Variable value	C:\Program Files (x86)\Java\jdk.1.8.0_xx\

7. Add another new environment variable as shown below.

Field	Value
Variable name	CLASSPATH
Variable value	C:\Program Files (x86)\Java\jdk.1.8.0_xx\lib\

8. Edit the **Path** environment variable to append `;%JAVA_HOME%\bin\` to the end of the variable value.
9. Click **OK** repeatedly to exit.

Task 5: Deploy the chat server

> **Note:**
> - If you upgrade a chat server with version of 9.41, skip this task and refer to the upgrade task "Upgrade the chat server" on page 1.

HPE provides a preconfigured version of Openfire as the Service Manager Collaboration chat server, which is easy to set up and administer and offers rock-solid security and performance. In this task, you will install the Openfire chat server and go through configuration steps for it.

> **Note:**
> - The Openfire chat server can be deployed on the Windows system only, but it works well with the Service Manager servers running on all supported platforms such as Linux.
> - Openfire shares the Service Manager database. You may want to back up the Service Manager database before beginning this task.

Follow these steps:

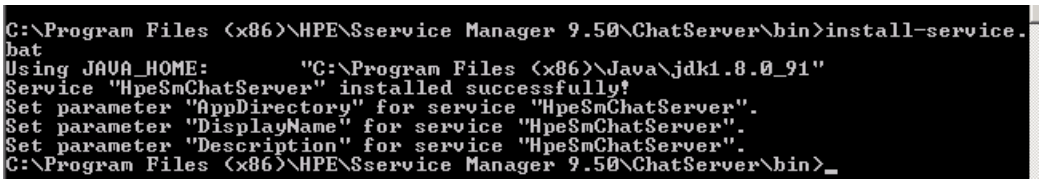
1. Save the chat server installer chat-server-9.50.zip from Service Manager installation package 2 to your computer.
2. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50 folder and create a new directory called ChatServer.
3. Extract the chat-server-9.50.zip file to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer folder.
4. Open a DOS command prompt. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin folder, and then run openfire.bat.

   You can also install the Openfire Chat Server service to start the chat server. Follow the steps:

   a. To install Openfire Chat Server as a Windows service, open a DOS command prompt and change the directory to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin.

```
cd C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin
```

b. Run the **install-service.bat** command to install the Service Manager chat service as a Windows service.

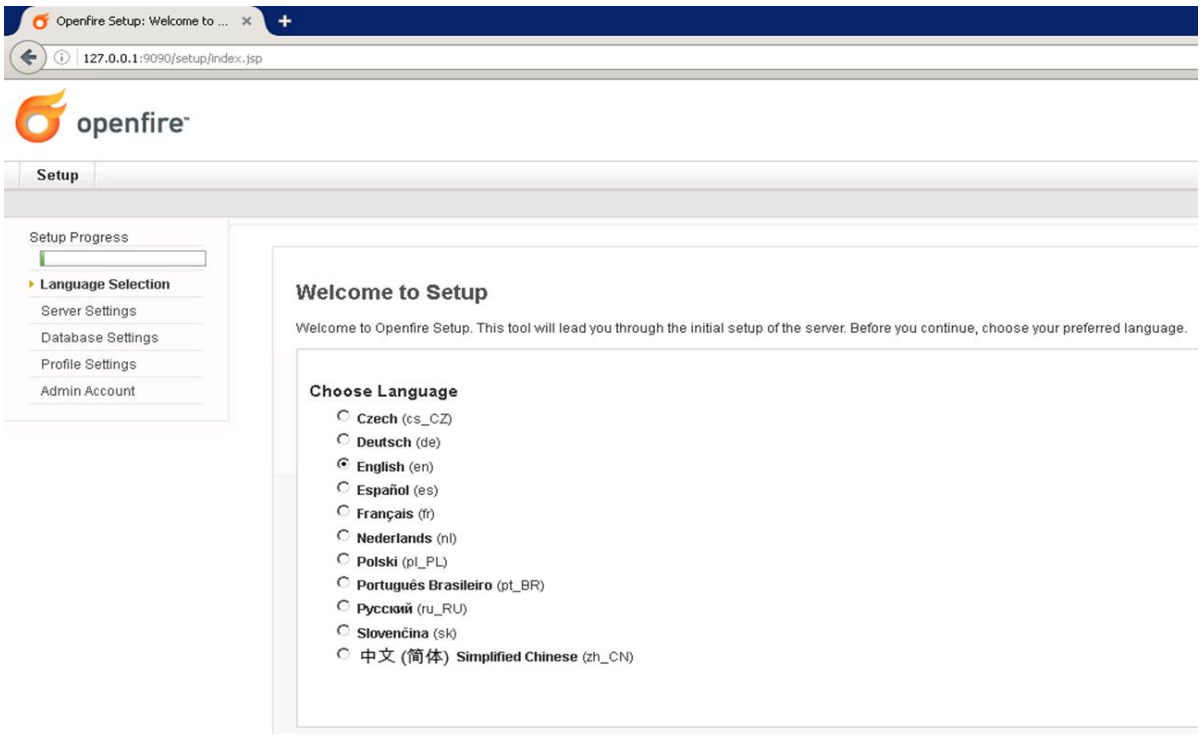


You can run **nssm edit HpeSmChatServer** to edit the corresponding configurations after the Windows service is installed.

> **Tip:** To remove this Windows service, run the **nssm remove HpeSmChatServer** command.

c. Go to Windows Services, and verify that the new **HPE Service Manager 9.50.00xx Chat Server** service has been installed. Then start the service.

5. Access http://localhost:9090/setup/index.jsp from the web browser. The Openfire Setup: Welcome to Setup screen is displayed.



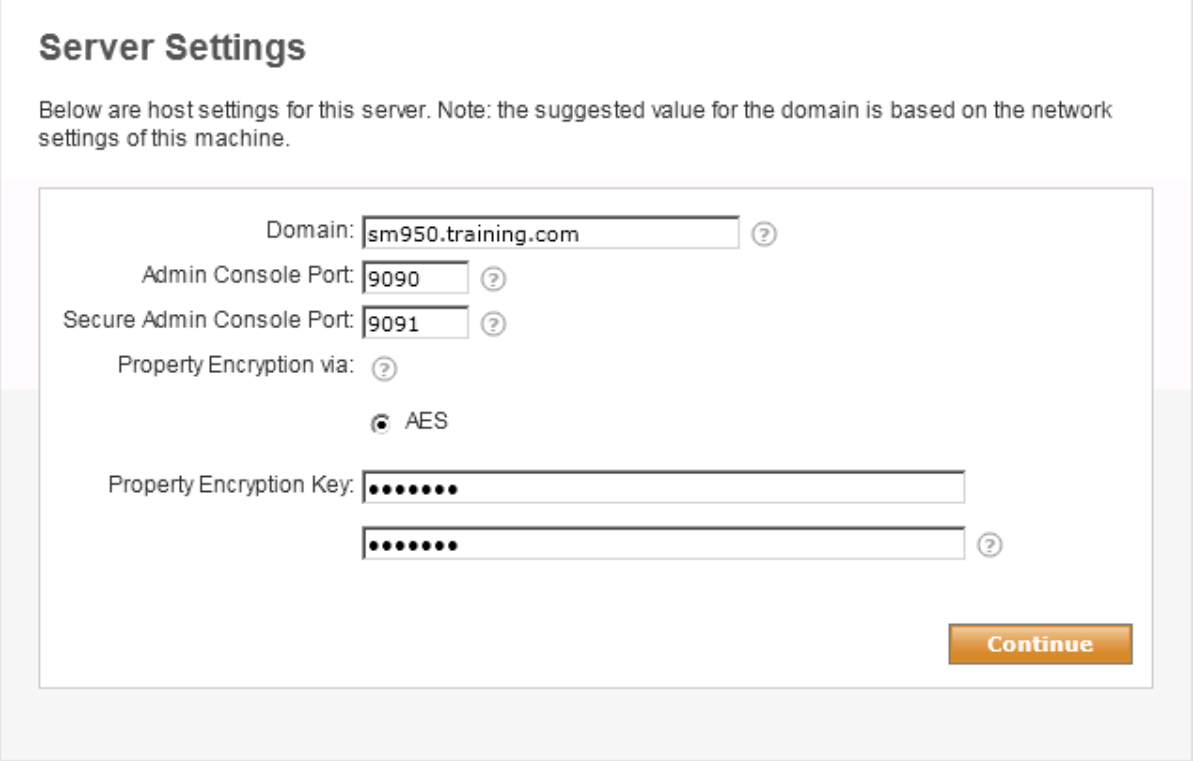
> **Note:** You can also visit http://127.0.0.1:9090/setup/index.jsp or

> http://sm950.training.com:9090/setup/index.jsp to access the Openfire Administrator Console web page at any time.

6. Select **English** and click **Continue**.

   The Openfire Administrator Console supports Czech (cs), German (de), English (en), Spanish (es), French (fr), Dutch (nl), Polish (pl_PL), Brazilian Portuguese (pt_BR), Russian (ru_RU), Slovak (sk), and Simplified Chinese (zh_CN).

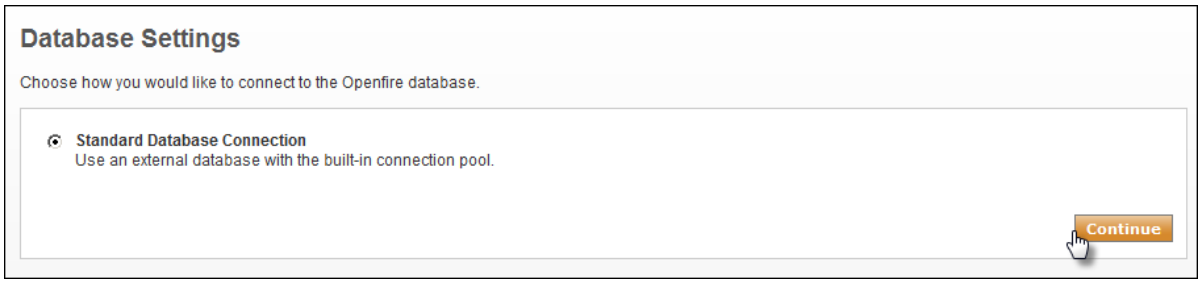
7. You need to specify the database details so that Openfire can connect to your Service Manager database and create the DB tables. Update the fields as illustrated below on the Server Settings screen, and then click **Continue**.



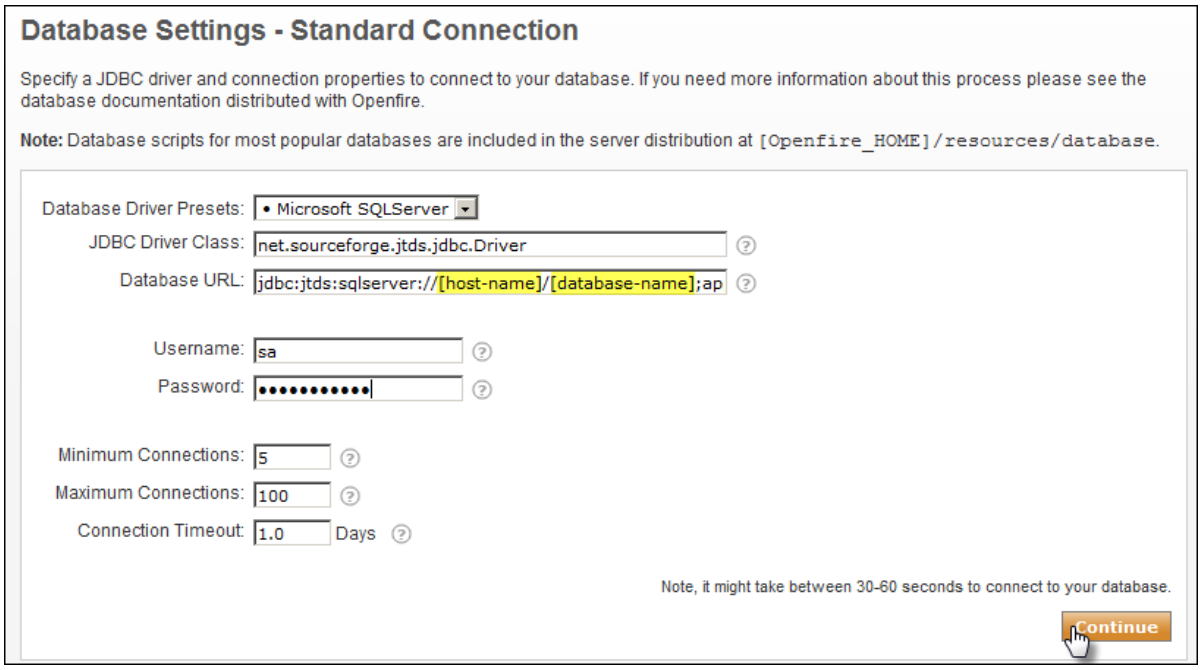
Parameter	Value in this task	Description
Domain	sm950.training.com	Domain name of the Openfire server host. In the all-in-one example, set the domain to sm950.training.com. Note that this domain has no relationship with LW-SSO. You can type any value, including symbols such as underline(_) and hyphen(-). This value is used on the SM collaboration setting page later.

Parameter	Value in this task	Description
Admin Console Port	9090	The port used for unsecured Admin Console access. The default value is 9090. Leave this port to its default value if you do not need to open an HTTP port.
Secure Admin Console Port	9091	The HTTPS port used for secured Openfire Admin Console access. The default value is 9091.
Property Encryption via	AES	The encryption algorithm used by the Openfire server to prevent sensitive data from being exposed. The default option is AES.
Property Encryption Key	sm950training	Specify the AES encryption key. This field is mandatory. You can specify any value in the first field, and then type this value again in the second field.

8. Click **Continue** on the Database Settings screen.



9. Specify a JDBC driver and the connection properties to connect to your database. Update the fields as illustrated below on the Database Settings – Standard Connection screen, and then click **Continue**.



Parameter	Value in this task	Description
Database Driver Presets	Microsoft SQL Server	Select the database type of Service Manager. You can select either SQL server or Oracle.
JDBC Driver Class	Do not modify the default value	Value in this field is populated automatically after the database type is selected.
Database URL	jdbc:jtds:sqlserver://SM950BETA/SM950;appName=jive	Value in this field is populated automatically after the database type is selected. ◦ The default Oracle database URL is `jdbc:oracle:thin:@[host-name]:1521:[SID]`, where [host-name] and [SID] are the actual values of you server. ◦ The default Microsoft

Parameter	Value in this task	Description
		SQL server database URL is `jdbc:jtds:sqlserver://[host-name]/[database-name];appName=jive`, where [host-name] and [database-name] are the actual values of you server. If you have multiple database instances on a SQL server, refer to the **Named and Multiple SQL Server Instances** section on the Building the Connection URL web page for more information about the database URL configuration.
Username	<*Your Service Manager database user name*>	Specify the user name to log on to the Service Manager database.
Password	<*Your Service Manager database password*>	Specify the password to log on to the Service Manager database. HPE suggests that you use a strong password.
Minimum Connections	5	Specify the minimum number of database connections the connection pool should maintain. The default value is 5.
Maximum Connections	100	Specify the maximum number of database connections the connection pool should maintain. The default value

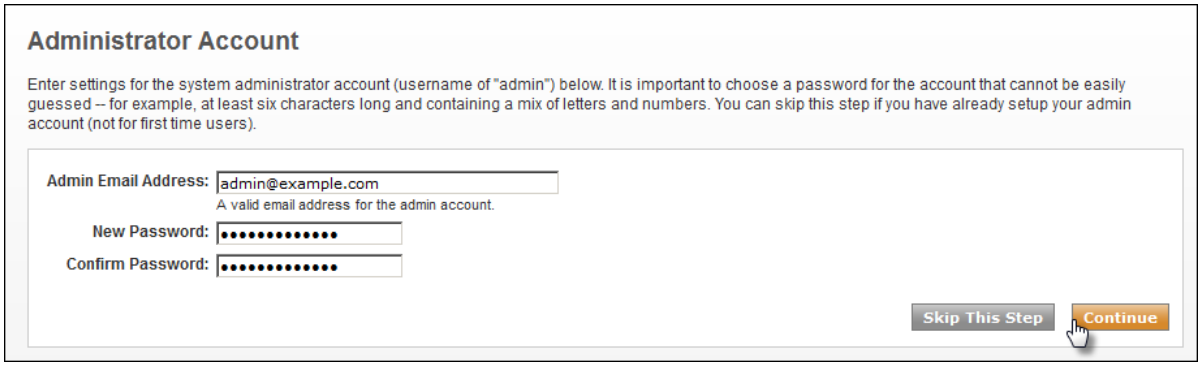
Parameter	Value in this task	Description
		is 100.
Connection Timeout	1.0	Specify the time (in days) before connections in the connection pool are recycled. The default value is 1.0.

Note:

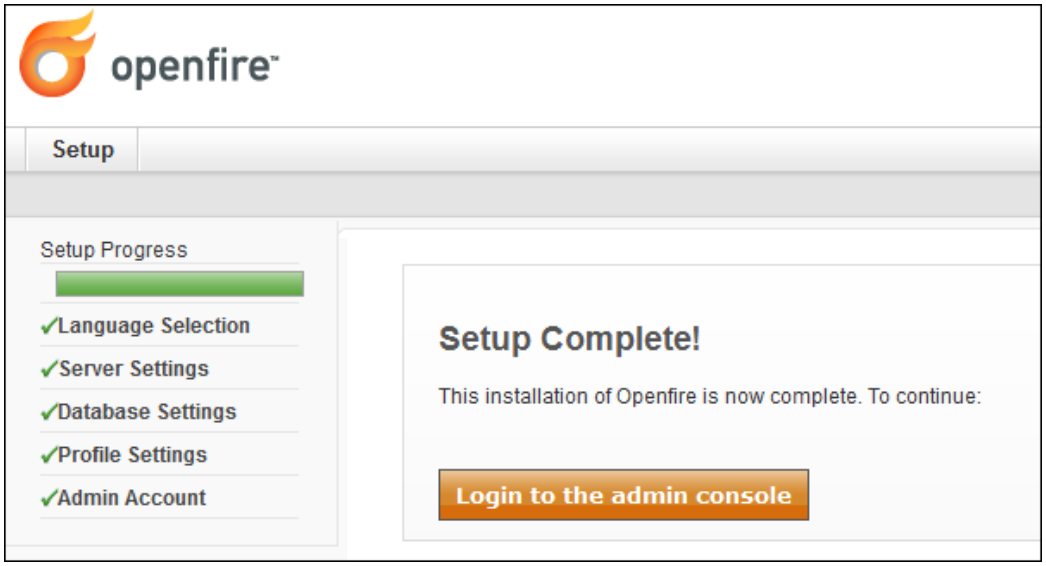
- If you are working with an Oracle database, copy the JDBC driver (for example, ojdbc6.jar) to the <sm9.xx.00xx-ChatServer>\lib directory before starting the chat server.
- Service Manager Collaboration uses the Service Manager database and inserts a number of Openfire tables into the database. Each table name is prefixed with "`of`". Therefore, you need to update the [host-name] with your database host name, and the [database-name] with your Service Manager database name in the Database URL field. It may take a while to connect to the database.

10. Click **Continue** on the Profile Settings screen.

11. Create the user name and password for your Openfire administrator on the Administrator Account screen. Later you will log on to Openfire as `admin` with this password. Click **Continue** to finish the Openfire installation



12. Your Openfire setup is complete now.



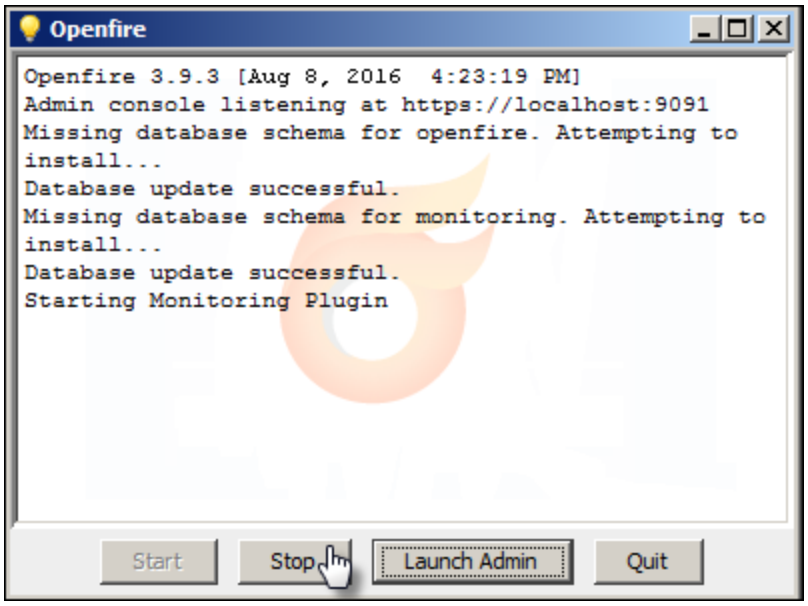
13. Click the **Login to the admin console** button to log on to your Openfire Administration Console.
14. Click **Server** > **Server Manager** > **System Properties**, and then manually add the following properties to the list:

Property name	Description	Property value
xmpp.client.processing.threads	The thread pool of the woker pool in Openfire to process incoming XMPP requests. The default value is 32, which can be increased to 254 for heavy loads.	32
lyncplugin.brokerService.memoryLimit	The total memory size of the message queues between Collaboration and the Lync server when you are integrating Collaboration with Lync. You can increase the value for heavy message queues.	1024
lyncplugin.brokerService.policy.memoryLimit	The memory size of each message queue between Collaboration and the Lync server when you are integrating Collaboration with Lync. You can increase the value when the message queue is considered as a bottleneck.	64

15. Click **Group Chat** > **Group Chat Settings** > **conference** > **Other Settings**.
16. In the **Conversation Logging** section, update the values as follows:

Property	Description	Value
Flush interval (seconds)	The two parameters control the frequency of inserting the chat log to the database. The recommended value is 3000 records per 30s.	30
Batch size		3000

17. Click **Save Settings**.
18. Close the web browser tab.
19. Click **Stop** on the Openfire screen.



Task 6: Deploy the chat service

In this task, you will install the chat service for End User Chat.

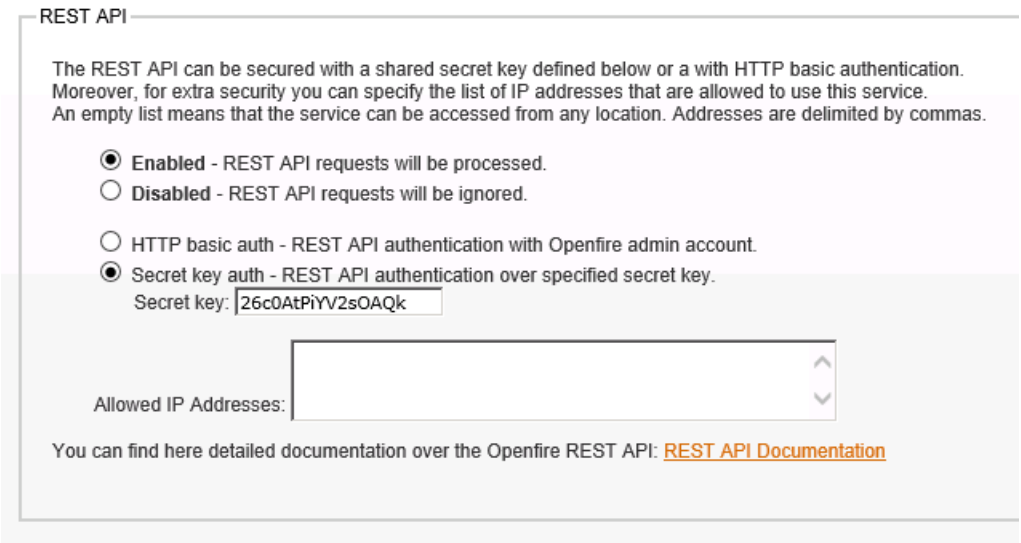
Follow these steps:

1. Save the chat service installer chat-msvc-9.50.zip from Service Manager installation package 2 to the same computer on which the chat server was deployed.
2. Log on to your Openfire Administration Console.
3. Click the **User/Groups** tab and create an Openfire user. For example:

   User name: publishadmin

Password: admin123

4. To enable the virtual agent, click **Server** > **Server Settings** > **REST API**. Enable REST API and record the secret key auth.



5. Save your changes, and then restart the Openfire chat server.
6. Extract chat-msvc-9.50.zip to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService, and then open conf\app.properties with a text editor.
7. Update the related parameters:

```
Factory.password,pubSubServiceConfig.userName,pubSubServiceConfig.password,
chatServerConfig.restApiSecretKey,app.keyStorePassword,app.trustStorePassword
app.encryptionKey=
daoFactory.serviceEndPoint=http://sm950.training.com:13080
daoFactory.userName=falcon
daoFactory.password=
pubSubServiceConfig.userName=publishadmin
pubSubServiceConfig.password=admin123

chatServiceUrl=/chatservice/

chatServerConfig.domain=sm950.training.com
chatServerConfig.host=sm950.training.com
chatServerConfig.port=5222
chatServerConfig.boshUrl=/of-http-bind/
chatServerConfig.pluginUrl=/of-plugins/
chatServerConfig.restApiSecretKey=26o0AtPiYV2sOAQk
```

Parameter	Description
daoFactory.serviceEndPoint	The Service Manager server's URL.
daoFactory.username	The Backend user name for chat service to access Service Manager. **Important:** The backend user must be an SM user with the "system administrator" privilege and the "RESTful API" capability.
daoFactory.password	The daoFactory user password.
pubSubServiceConfig.userName	The user name created in step 3.
pubSubServiceConfig.password	The user password created in step 3.
chatServerConfig.domain	The domain user filled during install chat server.
chatServerConfig.host	The chat server computer name or IP.
chatServerConfig.restApiSecretKey	The secret key you recorded in *step 4*.

8. Save your changes and close this file.
9. To install the chat service as a Windows service, open a DOS command prompt and change the directory to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\bin.
10. Run the **install-service.bat** command to install the Service Manager chat service as a Windows service.

> **Note:** HPE recommends to use 64-bit Java because 32-bit Java may have potential performance limitations. However, if you are working with 32-bit Java, follow these steps so that the Service Manager chat service Windows service can start successfully:
>
> a. Open C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\bin\startup.bat with a text editor.
>
> b. Update the memory setting as follows:
>
> ```
> SET CHAT_SVC_JVM_OPTIONS=-XX:ThreadStackSize=256 -Xms512m -Xmx1024m
> ```
>
> c. Save your changes and close this file.
>
> d. Open C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\bin\ install-service.bat with a text editor.
>
> e. Update the `ThreadStackSize` memory setting to `ThreadStackSize=256 -Xms512m -`

`Xmx1024m`.

f. Save your changes and close this file.

You can run **nssm edit HpeSmChatService** to edit the corresponding configurations after the Windows service is installed.

Tip: To remove this Windows service, run the **nssm remove HpeSmChatService** command.

Task 7: Deploy the End User Chat UI

The End User Chat UI consists of the End User Chat window and the End User Chat button. Follow these steps to deploy the End User Chat UI:

1. Save the End User Chat UI installer chat-ui-9.50.war from Service Manager installation package 2 to your computer.
2. Rename the installer to chatui.war, and then copy it to the same Tomcat on which Service Manager web tier is deployed. For example, C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps.

Task 8: Deploy the Apache HTTP server

In this task, you will deploy and configure the Apache HTTP server for Service Manager Collaboration.

Note: The deployment instructions in this document are for a sample OpenSSL Apache server. If you have profound web server knowledge, you can also customize your web server by following your own business rules.

Follow these steps:

1. Download Apache with OpenSSL (for example, httpd-2.4.xx-x64.zip for Apache 2.4, or httpd-2.2.31-x64-r3.zip for Apache 2.2) from here.

   You can also download a pre-configured Apache 2.4 from HPE Live Network.

   Extract the zip file to C:\. This unzip process creates a new C:\Apache24 directory or a new C:\Apache22 directory.
2. (For Apache 2.4) Navigate to the C:\Apache24\conf folder.

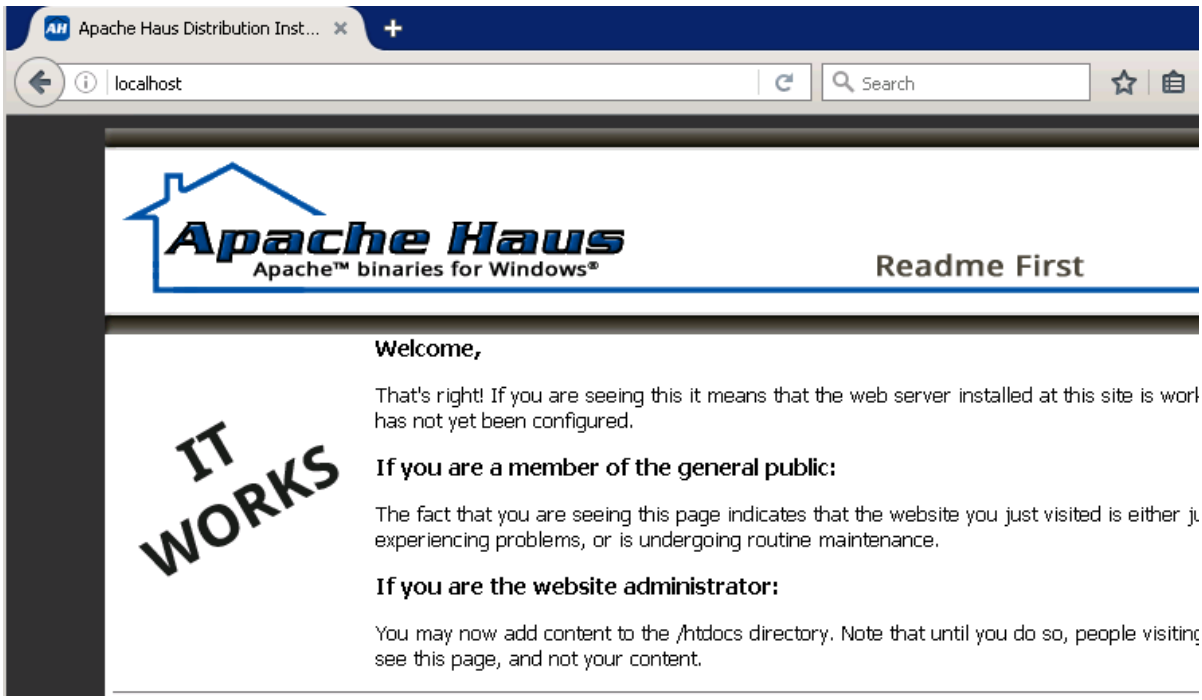
   (For Apache 2.2) Navigate to the C:\Apache22\conf folder.
3. Make a copy of the httpd.conf file and save it as httpd_OOB.conf.
4. Open the httpd.conf file with a text editor.

5. Locate `httpd-vhosts.conf`, and then uncomment `Include conf/extra/httpd-vhosts.conf`.
6. Save and close the httpd.conf file.
7. (For Apache 2.4) Navigate to the C:\Apache24\conf\extra directory.

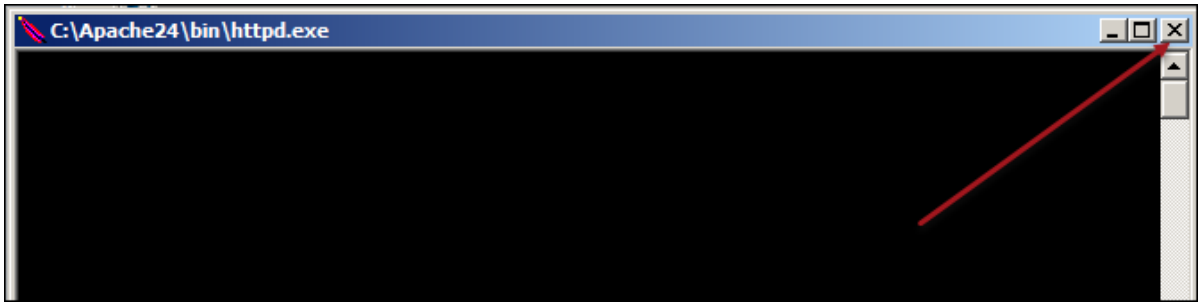
   (For Apache 2.2) Navigate to the C:\Apache22\conf\extra directory.
8. Make a copy of the httpd-vhosts.conf file and save it as httpd-vhosts_OOB.conf.
9. (For Apache 2.4) Navigate to the C:\Apache24\bin folder.

   (For Apache 2.2) Navigate to the C:\Apache22\bin folder.
10. Double-click httpd.exe to start the Apache server.

    The httpd.exe window opens. Click the minimize button to minimize this window.
11. In your web browser, type `http://localhost` and press Enter. The following page is displayed, indicating Apache has started successfully.



12. Close the browser.
13. Close the Apache httpd.exe window.



> **Note:** The steps below will install Apache as a Windows service.

14. (For Apache 2.4) Navigate to the C:\Apache24\bin folder. Open a DOS command prompt and change the directory to C:\Apache24\bin.

    ```
    cd C:\Apache24\bin
    ```

    (For Apache 2.2) Navigate to the C:\Apache22\bin folder. Open a DOS command prompt and change the directory to C:\Apache22\bin.

    ```
    cd C:\Apache22\bin
    ```

15. Run the **httpd –k install** command to install the Windows service.

    For Apache 2.4:

    ```
    C:\Users\Administrator>cd C:\Apache24\bin

    C:\Apache24\bin>httpd -k install
    Installing the 'Apache2.4' service
    The 'Apache2.4' service is successfully installed.
    Testing httpd.conf....
    Errors reported here must be corrected before the service can be started.

    C:\Apache24\bin>
    ```

    For Apache 2.2:

    ```
    C:\Users\Administrator>cd C:\Apache22\bin

    C:\Apache22\bin>httpd -k install
    Installing the Apache2.2 service
    The Apache2.2 service is successfully installed.
    Testing httpd.conf....
    Errors reported here must be corrected before the service can be started.

    C:\Apache22\bin>_
    ```

> **Note:** If you see an error here, navigate to the logs directory and check the error.log file. Depending on the error, you may need to repeat the steps above. To verify whether the error still exists, type **httpd –k start** to start Apache from the command line.

16. (For Apache 2.4) Go to Windows Services, and start the newly installed **Apache2.4** service.

    (For Apache 2.2) Go to Windows Services, and start the newly installed **Apache2.2** service.

Task 9: Connect Apache to Tomcat

In this task, you will set up Apache to connect to Tomcat through the AJP port. Consequently, Secure Sockets Layer (SSL) is open by default. You can perform this step rather than enable full SSL on the Service Manager environment.

Follow these steps:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\conf directory.
2. Open the server.xml file with a text editor.
3. Make sure that the AJP 1.3 Connector port is set to `8009`.

   ```
   <!-- Define an AJP 1.3 Connector on port 8009 -->
   <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
   ```

   > **Note:** If you need to change it to another port, make a note of that port number as you will need it later in this task.

4. Save and close the server.xml file.

Steps for Apache 2.4

> **Note:** If you are using the pre-configured Apache downloaded from HPE Live Network, skip step 1 to 15 and start with step 16.

1. Navigate to the C:\Apache24\conf directory.
2. Open the httpd.conf file with a text editor.

   The next few steps describe how to uncomment a number of `LoadModule` codes in the httpd.conf file.

3. Locate `lbmethod`.

   ```
   #LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
   #LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
   #LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
   #LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
   #LoadModule ldap_module modules/mod_ldap.so
   ```

4. Uncomment two lines as shown below:

   ```
   #LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
   LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
   ```

```
LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
#LoadModule ldap_module modules/mod_ldap.so
```

5. Locate the following section by searching for `proxy_module`.

```
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_html_module modules/mod_proxy_html.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
```

6. Uncomment 8 lines as shown in the following:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
```

7. Locate the following section by searching for `slotmem_shm`.

```
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
```

8. Uncomment the following line:

```
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
```

9. Locate the following section by searching for `xml2enc_module`.

```
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule watchdog_module modules/mod_watchdog.so
#LoadModule xml2enc_module modules/mod_xml2enc.so
<IfModule unixd_module>
```

10. Uncomment the following line:

```
LoadModule xml2enc_module modules/mod_xml2enc.so
```

11. Locate the following section. You may need to search for `mod_proxy_html` twice.

```
# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/httpd-proxy-html.conf
</IfModule>
```

12. If the `Include` line does not contain `Include conf/extra/httpd-proxy-html.conf`, change the `Include` line to `Include conf/extra/httpd-proxy-html.conf`.

13. Browse to the end of the file, and then add the line in bold:

```
<IfModule http2_module>
       ProtocolsHonorOrder On
       Protocols h2 h2c http/1.1
</IfModule>
Include conf/httpd-proxy_ajp_loadbalanced.conf
```

14. Comment out the lines in bold by inserting # in front of each line:

```
#<IfModule http2_module>
       #ProtocolsHonorOrder On
       #Protocols h2 h2c http/1.1
#</IfModule>
Include conf/httpd-proxy_ajp_loadbalanced.conf
```

15. Save and close the httpd.conf file.

16. Navigate to the C:\Apache24\conf directory, and then create a new file called httpd-proxy_ajp_loadbalanced.conf.

```
<Proxy balancer://smcluster>
BalancerMember ajp://localhost:8009 route=161652175430301
Require all granted
</Proxy>
<Location /webtier-9.50>
Options FollowSymLinks
Require all granted
ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
<Location /chatui>
Options FollowSymLinks
Require all granted
ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
```

> **Caution:**

- You must paste `ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid nofailover=On` in one line.
- You must paste `ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid nofailover=On` in one line.

17. The script in the previous step assumes that the web tier directory is webtier-9.50 and the chat UI directory is chatui(see the line below). If your web tier or chat UI uses another name, update the httpd-proxy_ajp_loadbalanced.conf file with the actual name of your web tier.

    ```
    <Location /webtier-9.50>
    balancer://smcluster/webtier-9.50
    <Location /chatui>
    balancer://smcluster/chatui
    ```

18. In step 3 in this task, you configured the `AJP 1.3 Connector` port in the server.xml file. If this port is 8009, continue with the next step; if the connector listens on another port, update the following line in the httpd-proxy_ajp_loadbalanced.conf file with that port number.

    If Apache is deployed on the same computer in the all-in-one example described in this document, use `ajp://localhost:8009`. Otherwise, you need to update this value to the correct IP of Tomcat.

    ```
    BalancerMember ajp://localhost:8009 route=161652175430301
    ```

19. Access Apache's link with Apache's FQDN. In this all-in-one example, access https://sm950.training.com/webtier-9.50/index.do, and then log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

    If you are directed to a Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.

    > **Note:** From now on, you must use HTTPS and the fully qualified domain name (FQDN) in the web tier URL when logging on to the Service Manager web client.

20. Log out from Service Manager.

Steps for Apache 2.2

1. Navigate to the C:\Apache22\conf directory.
2. Open the httpd.conf file with a text editor.

   The next few steps describe how to uncomment a number of `LoadModule` codes in the httpd.conf file.

3. Locate `proxy_module`.

4. Uncomment the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.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
```

5. Browse to the end of the file, and then add the line in bold:

```
<IfModule http2_module>
    ProtocolsHonorOrder On
    Protocols h2 h2c http/1.1
</IfModule>
Include conf/httpd-proxy_ajp_loadbalanced.conf
```

6. Save your changes and close the httpd.conf file.
7. Navigate to the C:\Apache22\conf directory, and then create a new file called httpd-proxy_ajp_loadbalanced.conf.
8. Copy and paste the following codes to the httpd-proxy_ajp_loadbalanced.conf file:

```
<Proxy balancer://smcluster>
BalancerMember ajp://localhost:8009 route=161652175430301
Order allow,deny
Allow from all
</Proxy>
<Location /webtier-9.50>
Options FollowSymLinks
Order allow,deny
Allow from all
ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
<Location /chatui>
Options FollowSymLinks
Order allow,deny
Allow from all
ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
```

> **Caution:**
> - You must paste `ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid nofailover=On` in one line.

- You must paste `ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid nofailover=On` in one line.

9. The script in the previous step assumes that the web tier directory is webtier-9.50 and the chat UI directory is chatui(see the line below). If your web tier or chat UI uses another name, update the httpd-proxy_ajp_loadbalanced.conf file with the actual name of your web tier.

```
<Location /webtier-9.50>
balancer://smcluster/webtier-9.50
<Location /chatui>
balancer://smcluster/chatui
```

10. In step 3 in this task, you configured the `AJP 1.3 Connector` port in the server.xml file. If this port is 8009, continue with the next step; if the connector listens on another port, update the following line in the httpd-proxy_ajp_loadbalanced.conf file with that port number.

    If Apache is deployed on the same computer in the all-in-one example described in this document, use `ajp://localhost:8009`. Otherwise, you need to update this value to the correct IP of Tomcat.

```
BalancerMember ajp://localhost:8009 route=161652175430301
```

11. Access Apache's link with Apache's FQDN. In this all-in-one example, access https://sm950.training.com/webtier-9.50/index.do, and then log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

    If you are directed to a Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.

    Note: From now on, you must use HTTPS and the fully qualified domain name (FQDN) in the web tier URL when logging on to the Service Manager web client.

12. Log out from Service Manager.

Task 10: Enable reverse proxy in Apache

In this task, you will enable the reverse proxy in Apache to protect sensitive information of Openfire (the IP address, ports, and so on). Follow the steps for your Apache version (2.4 or 2.2).

Important: You must use the same Apache server that connects to Tomcat in the previous task.

Steps for Apache 2.4

1. Navigate to the C:\Apache24\conf\extra directory.
2. Open the httpd-vhosts.conf file with a text editor.

3. Locate the following section by searching for "VirtualHost_defualt_:80".

```
<VirtualHost _default_:80>
DocumentRoot "${SRVROOT}/htdocs"
#ServerName www.example.com:80
</VirtualHost>
```

4. Insert the lines in bold to this section as shown below.

   Set the chat server's FQDN for the ProxyPassReverse value of of-http-bind and of-plugin. Set the chat service's FQDN for the ProxyPassReverse value of chatservice. And in this all-in-one example, all these values are sm950.training.com.

```
<VirtualHost _default_:80>
DocumentRoot "${SRVROOT}/htdocs"
#ServerName www.example.com:80
ProxyPass /of-http-bind http://sm950.training.com:7070/http-bind
ProxyPassReverse /of-http-bind http://sm950.training.com:7070/http-bind
ProxyPass /of-plugins http://sm950.training.com:9090/plugins
ProxyPassReverse /of-plugins http://sm950.training.com:9090/plugins
ProxyPass /chatservice http://sm950.training.com:8088
ProxyPassReverse /chatservice http://sm950.training.com:8088
</VirtualHost>
```

5. Save and close the httpd-vhosts.conf file.

Steps for Apache 2.2

1. Navigate to the C:\Apache22\conf\extra directory.
2. Open the httpd-vhosts.conf file with a text editor.
3. Locate the following section by searching for "VirtualHost _defualt_: 80".

```
<VirtualHost _default_:80>
DocumentRoot "${SRVROOT}/htdocs"
#ServerName www.example.com:80
</VirtualHost>
```

4. Insert the lines in bold to this section as shown below:

   Set the chat server's FQDN for the ProxyPassReverse value of of-http-bind and of-plugin. Set the chat service's FQDN for the ProxyPassReverse value of chatservice. And in this all-in-one example, all these values are sm950.training.com.

```
<VirtualHost _default_:80>
DocumentRoot "${SRVROOT}/htdocs"
#ServerName www.example.com:80
ProxyPass /of-http-bind http://sm950.training.com:7070/http-bind
ProxyPassReverse /of-http-bind http://sm950.training.com:7070/http-bind
```

```
ProxyPass /of-plugins http://sm950.training.com:9090/plugins
ProxyPassReverse /of-plugins http://sm950.training.com:9090/plugins
ProxyPass /chatservice http://sm950.training.com:8088
ProxyPassReverse /chatservice http://sm950.training.com:8088
</VirtualHost>
```

5. Save your changes and close the httpd-vhosts.conf file.

Task 11: Define the display of the End User Chat UI in ESS portal

> **Note:** Skip this task if your organization uses Service Manager Service Portal for end users.

An end user needs to click the chat button to open the End User Chat window. In this task, you will configure the webtier.properties to define how the End User Chat window is displayed on the Service Manager Employee Self-Service (ESS) portal.

Follow these steps:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF directory, and then open webtier.properties with a text editor.
2. Locate the `SMC ESS Chat configuration` section, and then update the parameters. See the following table for detailed description:

```
smc.ess.chat.url=http://sm950.training.com/chatui
smc.ess.chat.style.width=300
smc.ess.chat.style.height=400
smc.ess.chat.style.position=br
```

Parameter	Description
smc.ess.chat.url	Specify the absolute URL to the End User Chat UI application. This chat URL is the real URL which you can access through Apache. For example, `http://sm950.training.com/chatui`
smc.ess.chat.style.width	Specify the width of the iFrame which contains the End User Chat window. The unit is pixel.
smc.ess.chat.style.height	Specify the height of the iFrame which contains the End User Chat window. The unit is pixel.
smc.ess.chat.style.position	Specify the position of the End User Chat UI. The available values are `bl` (bottom-left) or `br` (bottom-right).

3. Save your changes and close this file.

Follow these steps to update the chat service URL in Service Manager Chat UI:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\chatui\conf directory, and then open env.js with a text editor.
2. Update the `chatServiceUrl` value, which must be the real URL that you can access through Apache. For example, `http://sm950.training.com/chatservice`

```
hpe.chatui = {
  __env: {
    //The url to access chat service
    chatServiceUrl: 'http://sm950.training.com/chatservice'
  }
};
```

3. Save your changes and close this file.

Task 12: Define the display of the End User Chat UI in Service Manager Service Portal

> **Note:** Skip this task if your organization uses Service Manager ESS portal for end users.

An end user needs to click the chat button to open the End User Chat window. For Service Manager Service Portal, you must access the chat UI's SSL URL through Apache. In this task, you will configure Apache and define the open SSL reverse proxy. Note that the open SSL is established between the Apache server and the web browser only. The chat server, the chat service, and the Service Manager server are still connecting to the Apache server through HTTP.

> **Note:** The Apache server and Service Manager Service Portal must use SSL certificates issued by the same Certificate Authority (CA) and the SSL certificates or the CA must be trusted by the end user's web browser.

Follow these steps:

1. (For Apache 2.4) Navigate to the C:\Apache24\conf\extra directory.

   (For Apache 2.2) Navigate to the C:\Apache22\conf\extra directory.
2. Open the httpd-ahssl.conf file with a text editor.
3. Locate the following section by searching for `ServerName localhost`:

```
<VirtualHost _default_:443>
SSLEngine on
ServerName localhost:443
SSLCertificateFile "${SRVROOT}/conf/ssl/server.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/server.key"
DocumentRoot "${SRVROOT}/htdocs"
# DocumentRoot access handled globally in httpd.conf
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

```
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
</virtualhost>
```

4. Insert the lines in bold to this section as shown below (insert 5 lines below the `SSLEngine on` line and 6 lines between `</Directory>` and `</virtualhost>`).

```
<VirtualHost _default_:443>
SSLEngine on
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ServerName localhost:443
SSLCertificateFile "${SRVROOT}/conf/ssl/server.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/server.key"
DocumentRoot "${SRVROOT}/htdocs"
# DocumentRoot access handled globally in httpd.conf
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
ProxyPass /of-http-bind http://sm950.training.com:7070/http-bind
ProxyPassReverse /of-http-bind http://sm950.training.com: 7070/http-bind
ProxyPass /of-plugins http://sm950.training.com:9090/plugins
ProxyPassReverse /of-plugins http://sm950.training.com:9090/plugins
ProxyPass /chatservice http://sm950.training.com:8088
ProxyPassReverse /chatservice http://sm950.training.com:8088
</virtualhost>
```

> **Note:** `/of-http-bind` is the path of the Openfire HTTP binding (also known as BOSH) reverse configuration, whereas `/of-plugins` is the identifier of the Openfire plugin directory. These two parameters will be used later on the SM Collaboration setting page.

> **Note:** You need to change `sm950.training.com` to your own host name. In addition, 9091 is the secure admin console port for the chat server. If you changed this port from the default value during the chat server installation, you need to update the port number here.

5. Locate the following section by searching for `ServerName serverone.tld`.

```
<VirtualHost *:443>
SSLEngine on
ServerName serverone.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/serverone.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/serverone.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
</virtualhost>
```

6. Insert the lines in bold to this section as shown below (insert 5 lines below the `SSLEngine on` line and 6 lines between `</Directory>` and `</virtualhost>`).

```
<VirtualHost *:443>
SSLEngine on
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ServerName serverone.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/serverone.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/serverone.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
ProxyPass /of-http-bind http://sm950.training.com:7070/http-bind
ProxyPassReverse /of-http-bind http://sm950.training.com: 7070/http-bind
ProxyPass /of-plugins http://sm950.training.com:9090/plugins
ProxyPassReverse /of-plugins http://sm950.training.com:9090/plugins
ProxyPass /chatservice http://sm950.training.com:8088
ProxyPassReverse /chatservice http://sm950.training.com:8088
</virtualhost>
```

7. Locate the following section by searching for `ServerName servertwo.tld`.

```
<VirtualHost *:443>
SSLEngine on
ServerName servertwo.tld:443
```

```
SSLCertificateFile "${SRVROOT}/conf/ssl/servertwo.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/servertwo.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
</virtualhost>
```

8. Insert the lines in bold to this section as shown below (insert 5 lines below the `SSLEngine on` line and 6 lines between `</Directory>` and `</virtualhost>`).

```
<VirtualHost *:443>
SSLEngine on
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ServerName servertwo.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/servertwo.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/servertwo.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
ProxyPass /of-http-bind http://sm950.training.com:7070/http-bind
ProxyPassReverse /of-http-bind http://sm950.training.com: 7070/http-bind
ProxyPass /of-plugins http://sm950.training.com:9090/plugins
ProxyPassReverse /of-plugins http://sm950.training.com:9090/plugins
ProxyPass /chatservice http://sm950.training.com:8088
ProxyPassReverse /chatservice http://sm950.training.com:8088
</virtualhost>
```

9. Save and close the httpd-ahssl.conf file.
10. Restart the Apache service.

Follow these steps to update the chat service URL in Service Manager Chat UI:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_ SMWeb\webapps\chatui\conf directory, and then open env.js with a text editor.

2. Update the `chatServiceUrl` value, which must be the real URL that you can access through Apache. For example, `https://sm950.training.com/chatservice`

```
(function(scope) {
  var hpe = scope.hpe || (scope.hpe = {});
  hpe.chatui = {
    __env: {
      //The url to access chat service
      chatServiceUrl: 'https://sm950.training.com/chatservice'
    }
  };
})(window);
```

3. Save your changes and close this file.

Task 13: Configure LW-SSO for the chat server

In this task, you will set up LW-SSO for the Openfire chat server.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\plugins\lwssoplugin folder.
2. Make a copy of the lwssoconf.xml file and save it as lwssoconf_OOB.xml.
3. Open lwssoconf.xml with a text editor.
4. Locate the `domain` parameter and set it to `training.com`.
5. Locate the `initString` parameter and set it to `sm950training`.
6. Save and close the lwssofmconf.xml file.
7. Go to Windows services and restart the **HPE Service Manager 9.50.00xx Chat Server** Windows service.

Task 14: Configure LW-SSO for the chat service

In this task, you will set up LW-SSO for the chat service.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\conf folder.
2. Make a copy of the lwssoconf.xml file and save it as lwssoconf_OOB.xml.
3. Open lwssoconf.xml with a text editor.
4. Locate the `domain` parameter and set it to `training.com`.

5. Locate the `initString` parameter and set it to `sm950training`.
6. Save and close the lwssofmconf.xml file.
7. Go to Windows services and restart the **HPE Service Manager 9.50.00xx Chat Service** Windows service.

Task 15: Enable Service Manager Collaboration

By default, the Collaboration feature is disabled after applying the Service Manager 9.50 web tier. In this task, you will log on to Service Manager and set up the Collaboration Configuration.

Follow these steps:

1. Access http://sm950.training.com/webtier-9.50/index.do in your web browser, and then log on to Service Manager as a system administrator.
2. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.
3. Select the **Enable Collaboration** check box to enable Service Manager Collaboration.
4. (Optional) Select the **Enable ESS Lync User** check box so that the Skype users can join IT Collaboration conversations by using Skype.
5. Select whether to enable the End User Chat virtual agent or not.

   > **Important:**
   > To enable the End User Chat virtual agent, your enterprise must own an HPE Smart Analytics license and have enabled Smart Analytics. Otherwise, you cannot save your setting in this Enable End User Chat section.

6. Specify field values as described in the following table.

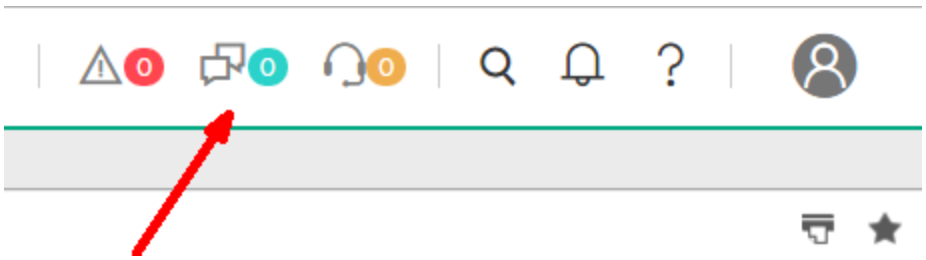
Field	Value in this task	Description
Maximum Participants Per Conversation	200	The maximum number of participants in a conversation. The default value is 200.
Notification Delay Time (Seconds)	30	The maximum time that an online participant has to wait to receive the live conversation notifications. The default value is 30. Notification delay is disabled if this value is set to 0 or minus.
Chat Service	http://sm950.training.com:8088/	The chat service URL.

Field	Value in this task	Description
URL		
Bosh Path	/of-http-bind/	The HTTP binding (also known as BOSH) path for Openfire to send XMPP messages. In the sample reverse proxy configurations in "Task 5: Deploy the chat server" on page 396, this path is `/of-http-bind/`. This field is read-only.
Chat Service Path	/chatservice/	The chat service base path for Restful resources. This field is read-only.
Domain Name	sm950.training.com	Domain name of the Openfire server. This field is read-only.
Plugin Path	/of-plugins/	The Openfire plugin URL. In the sample reverse proxy configurations in "Task 5: Deploy the chat server" on page 396, this value is `/of-plugins/`. This field is read-only.

7. Click **Save** and **OK**. It may take a while for the configurations to take effect.
8. Log out of the web client, and then log on as the system administrator again.

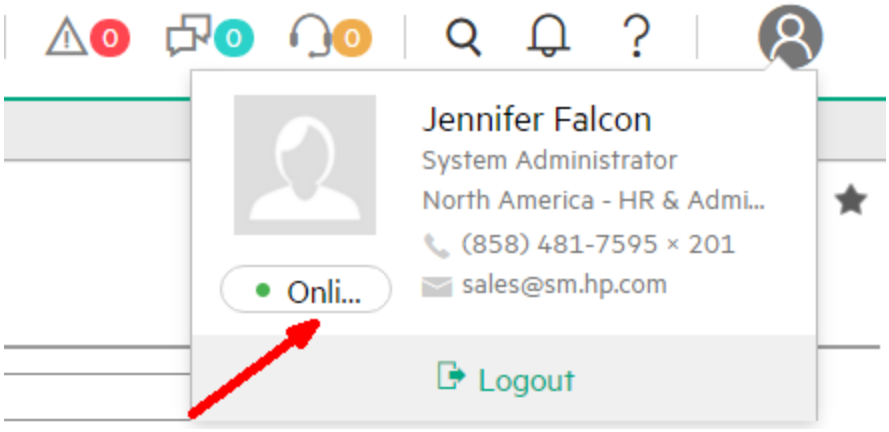
   If the system displays the following error message when you log in, check all your settings and then refer to the "Troubleshooting - Failed to connect to the Collaboration server" section:

9. Verify that a **Chat Notification** button is displayed at the top-right corner of the screen. You are not able to click it because chat notifications are not available yet.

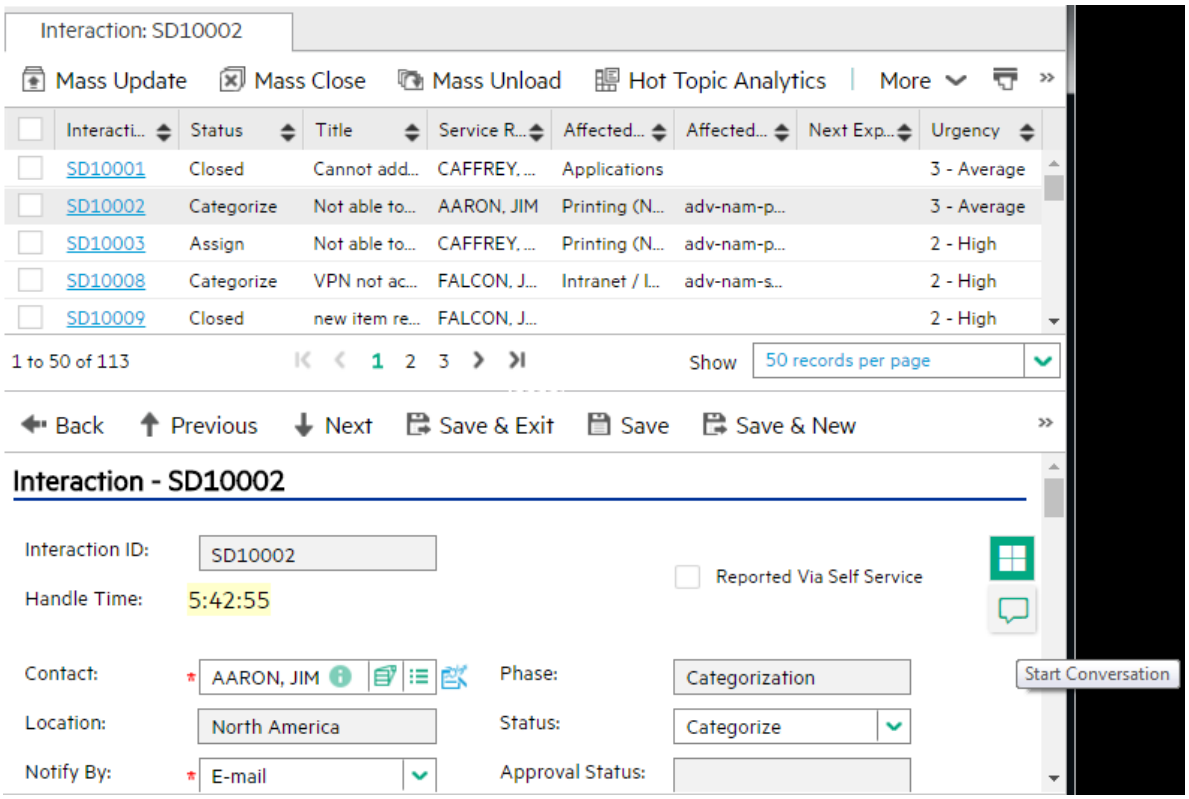


10. Click the **User Information** button to show your User Basic Information Card. Your presence

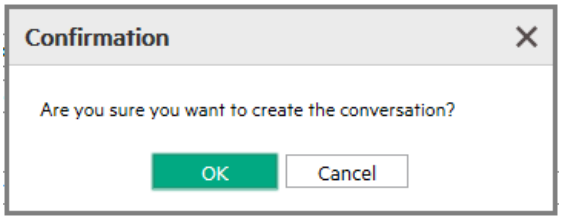
status is now **Online**.



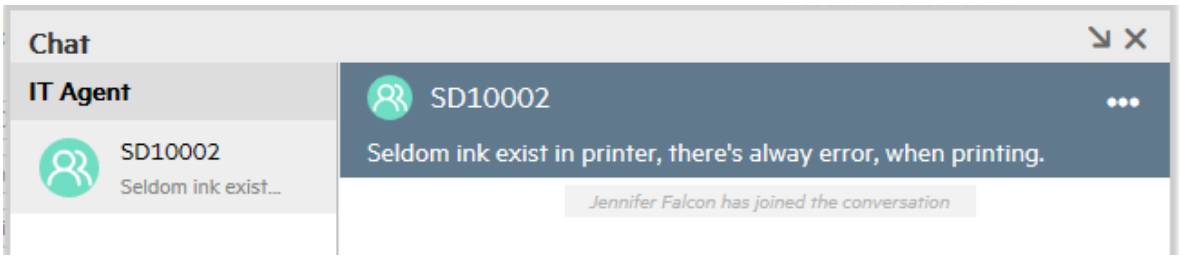
11. Open an interaction record. The **Start Conversation** button floats on the upper-right corner of the detailed view of this record.



12. Click the **Start Conversation** button, and then click **OK** in the confirmation dialog.



13. A conversation starts with the ID and title of the record displayed on the header of the conversation window.



Congratulations! You have successfully deployed Service Manager Collaboration!

Task 16: Select a portal for End User Chat

Service Manager supports the use of one of the following portals for End User Chat:

- Service Manager Service Portal (default): used for Service Manager Service Portal users
- ESS: used for Service Manager Employee Self-Service (ESS) client users

You need to select the right portal depending on which portal is being used for end users in your organization. To do this, follow these steps:

1. Go to **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
2. Select the **Active Integrations** tab.
3. In the **SM Portal** field, select the right portal from the drop-down list.
4. Specify the portal URL for your portal, as described in the following table.

Portal	Steps
ESS	In the **ESS URL** field, type the fully qualified ess.do URL to your web tier. For example: `https://sm950.training.com/webtier-9.50/ess.do`

Portal	Steps

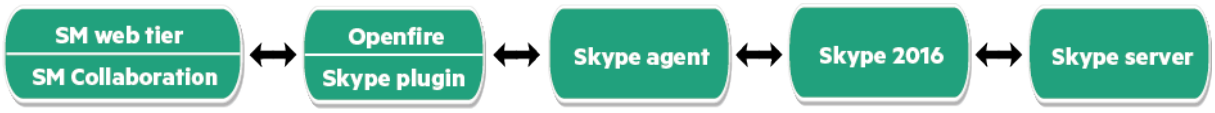
Service Manager Service Portal	**Note:** You must configure both the standard Service Portal URL and the Service Portal support ticket URL in the System Information Record. Both URLs are used as predefined parameters for End User Chat.
	a. In the **Service Manager Service Portal URL** field, enter the following value:
	`https://<Service Manager Service Portal host name>:<port>`
	Where: <*Service Manager Service Portal host name*> represents the fully qualified domain name of the Service Manager Service Portal host, and <*port*> represents the launchpad port of Service Manager Service Portal. The default launch pad port is 9000.
	For example:
	`https://serviceportal.training.com:9000`
	b. In the **Service Manager Service Portal Support Ticket URL** field, enter the following value:
	`https://<Service Manager Service Portal host name>:<port>/support/requests/create`
	Where: <*Service Manager Service Portal host name*> represents the fully qualified domain name of the Service Manager Service Portal host, and <*port*> represents the support ticket port of Service Manager Service Portal. The default support ticket port is 9410.
	For example:
	`https://serviceportal.training.com:9410/support/requests/create`

5. Click **Save**.
6. Restart the chat service.

(Optional) Task 17: Integrate with Microsoft Skype for Business

HPE Service Manager Collaboration provides an out-of-the-box Skype plugin and a Skype agent to integrate with Microsoft Skype for Business. When you start a conversation in Service Manager Collaboration, the Skype plugin that is embedded in the Openfire server monitors all the messages. If a participant does not log on to the Openfire server, the Skype plugin will use the participant's email address as his/her Skype account and then send the message to the Skype server. If the user is available to chat, the Skype agent will launch a conversation with the right user, and then forward the message to him/her on Skype. After the Skype user replies, the Skype Agent will push this message back to the Skype plugin. Consequently, the Skype plugin will poll the in-coming Skype message and then forward it to all the other users in the Collaboration conversation.

The following diagram illustrates a sample message exchange architecture between Service Manager Collaboration and the Skype server:

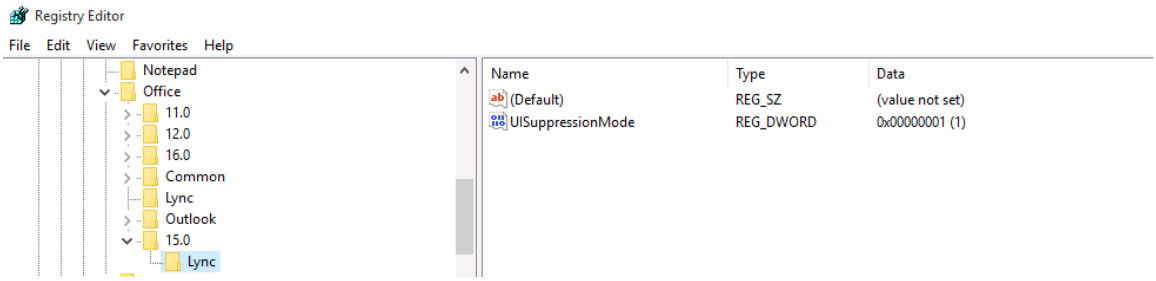


> **Note:**
> Lync users cannot start a conversation with Service Manager Collaboration. Instead, they can be invited to Collaboration conversations only.

In this task, you will integrate Service Manager Collaboration with Microsoft Skype for Business.

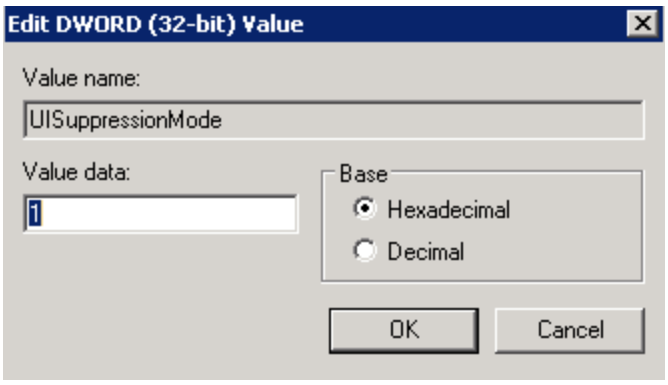
Follow these steps:

1. Download and install Microsoft .NET Framework 4.5 from Microsoft Download Center.
2. Download and install Microsoft Skype for Business 2016 from Microsoft Download Center. Service Manager Collaboration integrates with Microsoft Lync 2016 only.
3. Sign in to Skype by using an IT operator's Skype account. This account transfers the communication between the Openfire server and the Skype server, and hence must be effective and timely.
4. Click Microsoft Skype **Options** > **Personal**, and then select **None** from the **Personal information manager** drop-down menu. Save your changes and then sign out.
5. Create the new UISuppressionMode Windows Registry value.
   a. Open Windows Registry Editor, and then navigate to HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync.
   b. Right-click Lync, and then click **New** > **DWORD (32-bit) value** to create a new registry value.
   c. Set the new value name to UISuppressionMode, and then set the value data to 1.



   d. Navigate to HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Lync.
   e. Right-click Lync, and then click **New** > **DWORD (32-bit) value** to create a new registry value.

f. Set the new value name to UISuppressionMode, and then set the value data to 1.



g. Click **OK**, and then close the Windows Registry Editor.

6. Encrypt the Skype account and update the openfire.xml file.

   a. Stop the Openfire server.

   b. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\conf directory, and then open openfire.xml with a text editor.

   c. Locate the `<lyncIntegration>` section.

   d. Update the `<lyncIntegration>` section as follows:

```
<lyncIntegration>
<enabled>true</enabled>
<auth>
<!-- Put plain lync user name and password here, it will be automatically
encrypted
after server startup and encrypted="true" will be added to the userName and
password
elements. When you change your Lync userName or password, you must remove
encrypted="true" and replace the encrypted string with the new plain string.
-->
<userName><YourLyncAccountName></userName>
<password><YourLyncPassword></password>
</auth>
<startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

> **Note:** You need to enable Skype integration first, and then replace *<YourLyncAccountName>* and *<YourLyncPassword>* with the user account with which you signed in to Skype in step 3.

> **Caution:**

- When the IT operator's Skype password is changed, the <*YourLyncPassword*> value in openfire.xml must be changed accordingly.
- You must not sign out the IT operator's Skype account which transfers the communication between the Openfire server and the Skype server. Otherwise, Service Manager Collaboration does not work.

e. Save and close this file.

f. Start the Openfire server.

See the following screenshot for an example of the encrypted `<lyncIntegration>` section in openfire.xml:

```
<lyncIntegration>
  <enabled>true</enabled>
  <auth>
    <!-- Put plain lync user name and password here, it will be automatically encrypted
         after server startup and encrypted="true" will be added to the userName and password
         elements. When you change your Lync userName or password, you must remove encrypted="true" and
         replace the encrypted string with the new plain string.
      -->
    <userName encrypted="true">B454FAEED3A2E2118C77759EC9E7F4EFA56E051ADB0AB4451A8F8EB2A2357125</userName>
    <password encrypted="true">BA9F849640CAA40D4A69AE8ABCDBAA16</password>
  </auth>
  <startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

7. Enable Service Manager Collaboration to communicate with the Skype server.

a. Log on to Service Manager as a system administrator.

b. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.

c. Select the **Enable ESS Skype User** check box so that the Service Manager Skype users can join Collaboration conversations by using Skype.

Now you can communicate with the Skype users in a Service Manager Collaboration conversation.

Caution: To integrate with Microsoft Skype for Business, follow these steps to specify the log on account for the Openfire service before starting it as a standard Windows service:

1. Right-click the Openfire service in the Windows Services window, and then select **Properties**.
2. Click the **Log On** tab.
3. Select **This account**, and then specify the same IT operator's Skype account used in step 3.
4. Click **Apply** and **OK**.

(Optional) Task 18: Migrate data from EC

In this task, you will migrate existing Enterprise Collaboration (EC) data to Service Manager Collaboration by using a migration tool.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\smcmigration directory, and then double-click startup.bat to start the Service Manager Migration Tool.
2. Select a language, and then click **Start**.
3. Read through the welcome screen, and then click **Next**.
4. Select the database type of your EC server, specify the server name, database name, user name, and password of your EC database, and then click **Next**.

   > **Note:** If you are working with an Oracle database, download the JDBC driver (for example, ojdbc6.jar) from here and then copy this file to the <sm9.xx.00xx-ChatServer>\smcmigration\lib directory.

5. Select the database type of your Service Manager server, specify the server name, database name, user name, and password of your Service Manager database, and then click **Migrate**.

   The Service Manager Migration Tool displays a status bar that the visualizes the data migration progress.

6. When the data migration progress is completed, click **Finish** to quit the tool.

Deploy Service Manager Collaboration with HTTPS

The Collaboration deployment with HTTPS involves the following tasks. Note that these tasks are described using examples, which you may need to adjust according to your actual environment.

Task 1: Enable LW-SSO on the Service Manager server

For Service Manager Collaboration to function, you need to configure Lightweight Single Sign-On (LW-SSO) on the Service Manager server, Service Manager web tier and Openfire service so that Service Manager users can use Service Manager Collaboration without logging on to the Service Manager server separately.

In this task, you will set up LW-SSO for the Service Manager Server. Follow these steps:

1. Log on to Service Manager as a system administrator.
2. Go to Windows Services, and stop the **HPE Service Manager 9.50 Server** service.
3. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\Server\RUN directory.
4. Make a copy of the lwssofmconf.xml file, and save the copy as lwssofmconf_OOB.xml.
5. Open the lwssofmconf.xml file with a text editor.
6. Locate the `enableLWSSOFramework` parameter, and ensure that it is set to `true`.

   ```
   <enableLWSSO
   enableLWSSOFramework="true"
   enableCookieCreation="true"
   cookieCreationType="LWSSO"/>
   ```

7. Change the `domain` value to `training.com`.

   ```
   <domain>training.com</domain>
          <crypto cipherType="symmetricBlockCipher"
          engineName="AES" paddingModeName="CBC" keySize="256"
          encodingMode="Base64Url"
          initString="This is a shared secret passphrase"/>
   ```

   > **Note:** To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application to the web tier can log in but may be forcibly logged out after a while.

8. Change the `initString` value to `sm950training`.

   ```
   <domain>training.com</domain>
              <crypto cipherType="symmetricBlockCipher"
              engineName="AES" paddingModeName="CBC" keySize="256"
              encodingMode="Base64Url"
              initString="sm950training"/>
   ```

   > **Note:** This value can be set to any string that is at least 12 characters long, as long as you use the same `initString` value for all the products that you want to integrate through LW-SSO.

9. Save and close the lwssofmconf.xml file.
10. Start the **HPE Service Manager 9.50 Server** Windows service.

Task 2: Enable LW-SSO on the Service Manager web tier

In this task, you will enable LW-SSO in the Service Manager web tier so that Service Manager users can use Collaboration without logging on to the Service Manager server separately.

Note: If SAML Single Sign-On (SSO) is enabled for Service Manager, you should configure LW-SSO for SM Collaboration as follows:

- Enable LW-SSO in the SM Server
- Disable LW-SSO in the SM web tier
- Enable LW-SSO in the Openfire chat server
- Enable LW-SSO in the HPE Identity Manager (IdM) service

Note: As an example, this task uses Tomcat 8.0 as the web application server and **Tomcat 8.0_SMWeb** as the name of the Tomcat installation root directory.

Follow these steps:

1. Stop the Tomcat web application server.
2. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF directory.
3. Make a copy of the web tier configuration file (web.xml) and save it as web_OOB.xml.
4. Open the web.xml file with a text editor.
5. Set the `serverHost` parameter to the Service Manager server's FQDN. In the all-in-one example steps described in this document, set this parameter to `sm950.training.com`.

```
<init-param>
<!-- Specify the HPE Service Manager server host and port location -->
       <param-name>serverHost</param-name>
       <param-value>sm950.training.com</param-value>
</init-param>
```

6. Set the `secureLogin` parameter to `false`.

```
<context-param>
       <param-name>secureLogin</param-name>
       <param-value>false</param-value>
</context-param>
```

7. Set the `isCustomAuthenticationUsed` parameter to `false`.

```
<context-param>
       <param-name>isCustomAuthenticationUsed</param-name>
       <param-value>false</param-value>
</context-param>
```

8. Search for "LWSSO filter".

```
<!-- LWSSO filter for integrations using HP lightweight single sign-on
PLEASE NOTE: Uncomment this filter and the associated filter-mapping,
and see application-context.xml for additional configuration needed
for LWSSO. -->
<!--
       <filter>
       <filter-name>LWSSO</filter-name>
       <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
       </filter>
-->
```

9. Uncomment the LWSSO filter section by removing the comment tags.

```
<filter>
       <filter-name>LWSSO</filter-name>
       <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
</filter>
```

10. Search for "LWSSO filter-mapping".

```
<!-- LWSSO filter-mapping, please read description for LWSSO filter above
before uncommenting this. -->
<!--
       <filter-mapping>
       <filter-name>LWSSO</filter-name>
       <url-pattern>/*</url-pattern>
       </filter-mapping>
-->
```

11. Uncomment the LWSSO filter mapping section by removing the comment tags.

```
<filter-mapping>
       <filter-name>LWSSO</filter-name>
       <url-pattern>/*</url-pattern>
       </filter-mapping>
```

12. Save and close the web.xml file.
13. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF\classes directory.
14. Make a copy of the lwssofmconf.xml file, and save it as lwssofmconf_OOB.xml.
15. Open the lwssofmconf.xml file with a text editor.
16. Set the `enableLWSSOFramework` parameter to `true`.

```
<enableLWSSO
       enableLWSSOFramework="true"
       enableCookieCreation="true"
       cookieCreationType="LWSSO"/>
```

17. Set the `domain` parameter to `training.com`.

```
<lwssoValidation id="ID000001">
       <domain>training.com</domain>
       <crypto cipherType="symmetricBlockCipher"
       engineName="AES" paddingModeName="CBC" keySize="256"
       encodingMode="Base64Url"
       initString="This is a shared secret passphrase"/>
```

18. Set the `initString` parameter to `sm9xxtraining`.

```
<lwssoValidation id="ID000001">
           <domain>training.com</domain>
           <crypto cipherType="symmetricBlockCipher"
           engineName="AES" paddingModeName="CBC" keySize="256"
           encodingMode="Base64Url"
           initString="sm950training"/>
```

19. Set `secureHTTPCookie` to `false`.

```
<creation>
       <lwssoCreationRef useHTTPOnly="true" secureHTTPCookie="false">
       <lwssoValidationRef refid="ID000001"/>
       <expirationPeriod>50</expirationPeriod>
       </lwssoCreationRef>
       </creation>
```

20. In the `multiDomain` section, set the first DNS Domain to `training.com` and the first FQDN to `sm950.training.com`.

```
<multiDomain>
       <trustedHosts>
       <DNSDomain>training.com</DNSDomain>
       <DNSDomain>example1.com</DNSDomain>
       <NetBiosName>myserver</NetBiosName>
       <NetBiosName>myserver1</NetBiosName>
       <IP>xxx.xxx.xxx.xxx</IP>
       <IP>xxx.xxx.xxx.xxx</IP>
       <FQDN>sm950.training.com</FQDN>
       <FQDN>myserver1.example1.com</FQDN>
       </trustedHosts>
</multiDomain>
```

21. Save and close the lwssofmconf.xml file.
22. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF\classes directory, make a copy of the application-context.xml file and save it as application-context_OOB.xml.
23. Open the application-context.xml file with a text editor.

24. Locate the following line:

```
<sec:filter-chain pattern="/**"
filters="securityContextPersistenceFilter,anonymousAuthFilter"/>
```

25. Add `lwSsoFilter` to this line as follows:

```
<sec:filter-chain pattern="/**"
filters="securityContextPersistenceFilter,lwSsoFilter,anonymousAuthFilter"/>
```

> **Caution:** Use the correct case for **lwSsoFilter**.

26. Search for `bean id="lwSsoFilter"` to locate the lwSsoFilter bean.

```
<!--
       <bean id="lwSsoFilter"
class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
       <property name="authenticationManager">
       <ref bean="authenticationManager"/>
       </property>
       <property name="defaultRole">
       <value>ROLE_PRE</value>
       </property>
       </bean>
-->
```

27. Uncomment the lwSsoFilter bean by removing the comment tags shown in the previous step.
28. Save and close the application-context.xml file.
29. Go to Windows Services, and start the **Apache Tomcat 8.0 SMWeb** service.

Task 3: Test LW-SSO with the Service Manager web tier

In this task, you will verify if your Service Manager LW-SSO configuration works.

1. Access your tomcat link with the Tomcat server's FQDN. In the all-in-one example steps described in this document, access http://sm950.training.com:8080/webtier-9.50/index.do in your web browser to display the Service Manager login screen.
2. Log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

   If you are directed to a "Logout Successful" page, there may be issues with your LW-SSO configuration. Check all your files from the previous tasks and then try again.

   > **Caution:** From now on, you must use the fully qualified domain name (FQDN) in the web tier URL when logging on to Service Manager.

Task 4: Install Java for the chat server

In this task, you will install Java (64-bit recommended) and then set the `JAVA_HOME` variable for the chat server. If you are using your own server and already have Java installed, set `JAVA_HOME` to the location of your JDK and follow step 6 only.

Follow these steps:

1. This task uses the latest Java 8. Download the latest version of Java from the Java website.

   > **Note:** This task uses 32-bit Java as an example.

2. The system displays the welcome screen. Click **Next**.
3. Accept the default installation folder (C:\Program Files (x86)\Java\jdk1.8.0_xx), and then click **Next** to start the Java installation process.
4. On the JRE Destination Folder screen, accept the default installation folder (C:\Program Files (x86)\Java\jdk1.8.0_xx) and click **Next**.
5. When the Java installation is complete, click **Close**.
6. Add a new environment variable for the server.

Field	Value
Variable name	JAVA_HOME
Variable value	C:\Program Files (x86)\Java\jdk.1.8.0_xx\

7. Add another new environment variable as shown below.

Field	Value
Variable name	CLASSPATH
Variable value	C:\Program Files (x86)\Java\jdk.1.8.0_xx\lib\

8. Edit the **Path** environment variable to append `;%JAVA_HOME%\bin\` to the end of the variable value.
9. Click **OK** repeatedly to exit.

Task 5: Deploy the chat server

> **Note:**
> - If you are upgrading the chat server from version 9.41 to 9.50, skip this task and refer to the *Service Manager Upgrade Guide*.

- The Openfire chat server can be deployed on the Windows system only, but it works well with the Service Manager servers running on all supported platforms such as Linux.
- Openfire shares the Service Manager database. You may want to back up the Service Manager database before beginning this task.

Follow these steps:

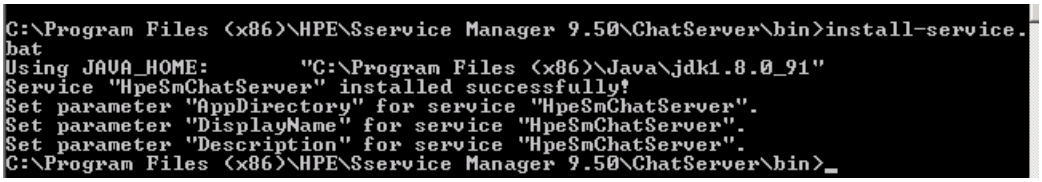
1. Save the chat server installer chat-server-9.50.zip from Service Manager installation package 2 to your computer.
2. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50 folder and create a new directory called ChatServer.
3. Extract the chat-server-9.50.zip file to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer folder.
4. Open a DOS command prompt. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin folder, and then run openfire.bat.

   You can also install the Openfire Chat Server service to start the chat server. Follow the steps:

   a. To install Openfire Chat Server as a Windows service, open a DOS command prompt and change the directory to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin.

      ```
      cd C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin
      ```

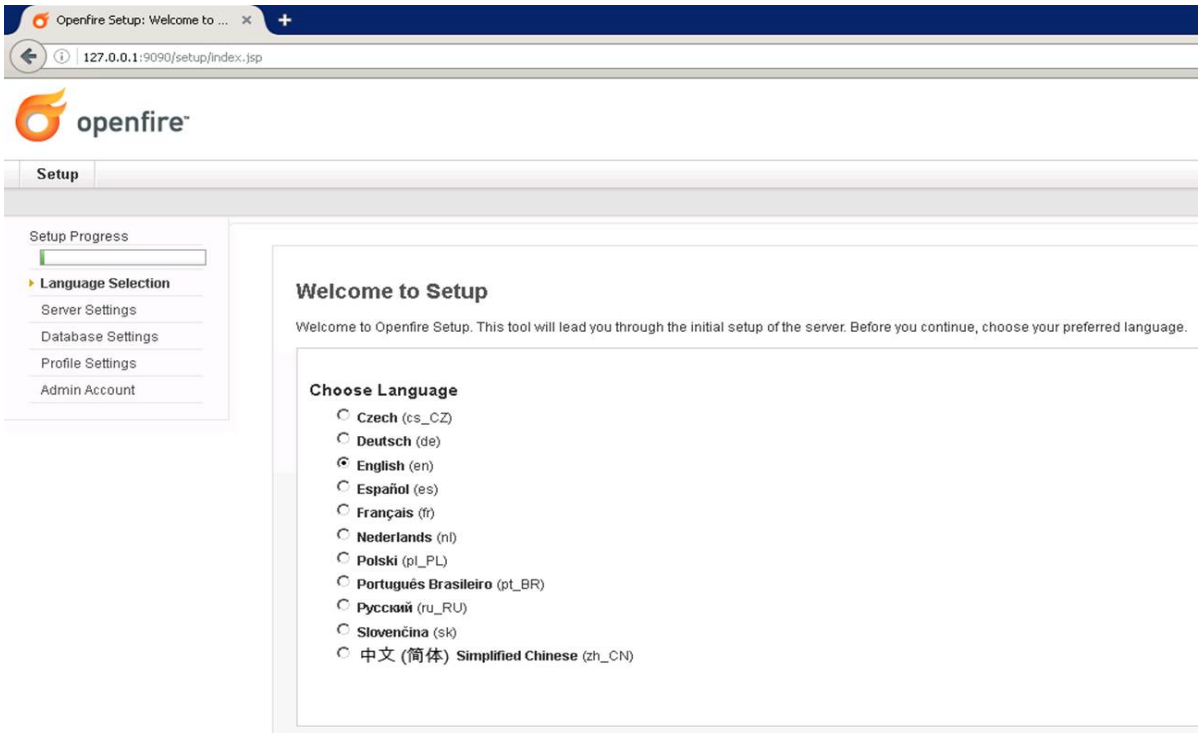
   b. Run the **install-service.bat** command to install the Service Manager chat service as a Windows service.

      You can run **nssm edit HpeSmChatServer** to edit the corresponding configurations after the Windows service is installed.

      > **Tip:** To remove this Windows service, run the **nssm remove HpeSmChatServer** command.

   c. Go to Windows Services, and verify that the new **HPE Service Manager 9.50.00xx Chat Server** service has been installed. Then start the service.
5. Access http://localhost:9090/setup/index.jsp from the web browser. The Openfire Setup: Welcome to Setup screen is displayed.

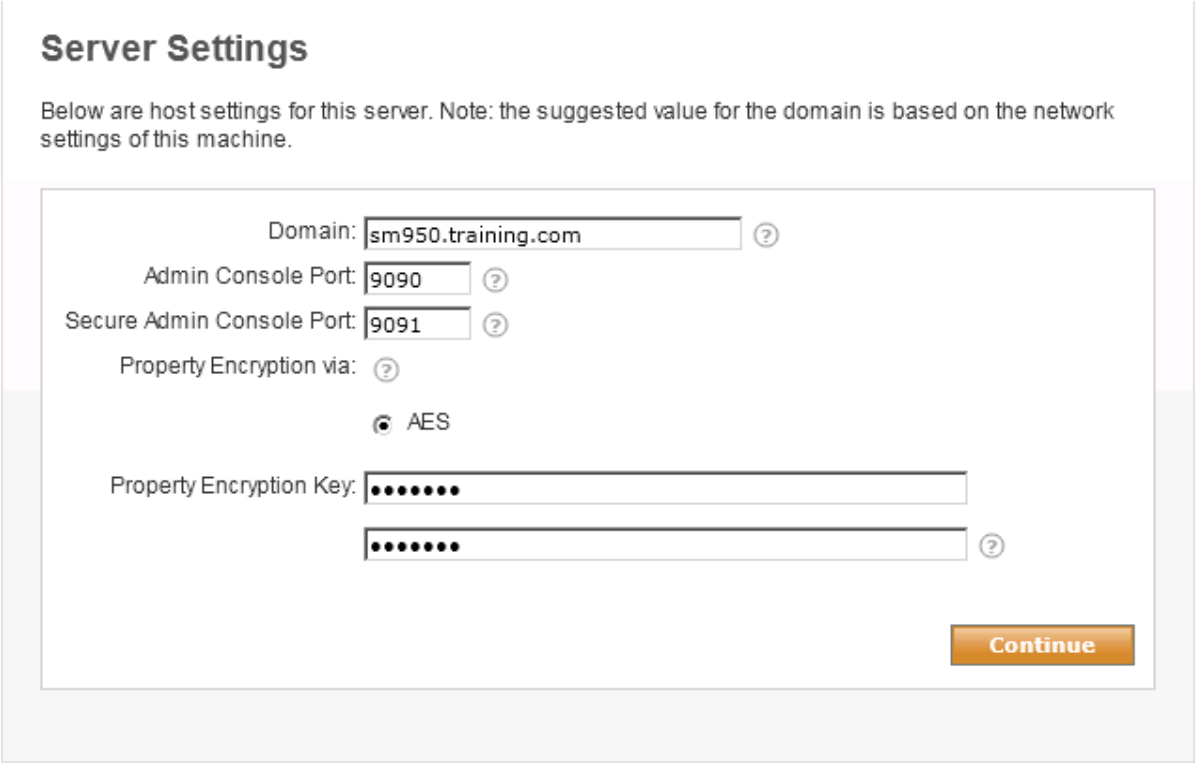


> **Note:** You can also visit http://127.0.0.1:9090/setup/index.jsp or http://sm950.training.com:9090/setup/index.jsp to access the Openfire Administrator Console web page at any time.

6. Select **English** and click **Continue**.

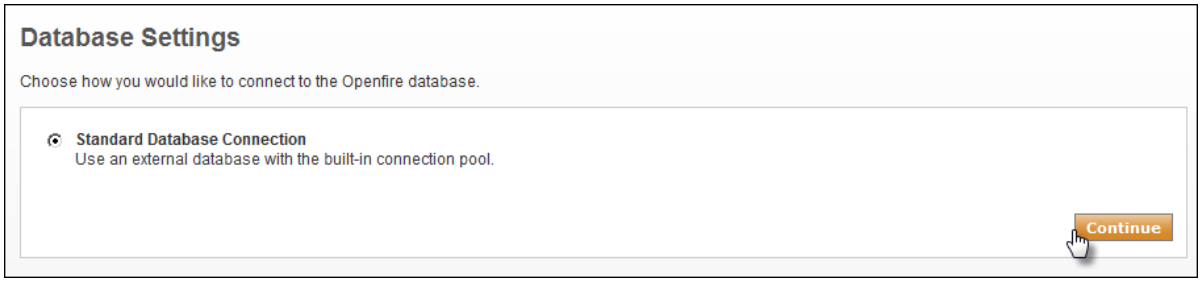
   The Openfire Administrator Console supports Czech (cs), German (de), English (en), Spanish (es), French (fr), Dutch (nl), Polish (pl_PL), Brazilian Portuguese (pt_BR), Russian (ru_RU), Slovak (sk), and Simplified Chinese (zh_CN).

7. You need to specify the database details so that Openfire can connect to your Service Manager database and create the DB tables. Update the fields as illustrated below on the Server Settings screen, and then click **Continue**.

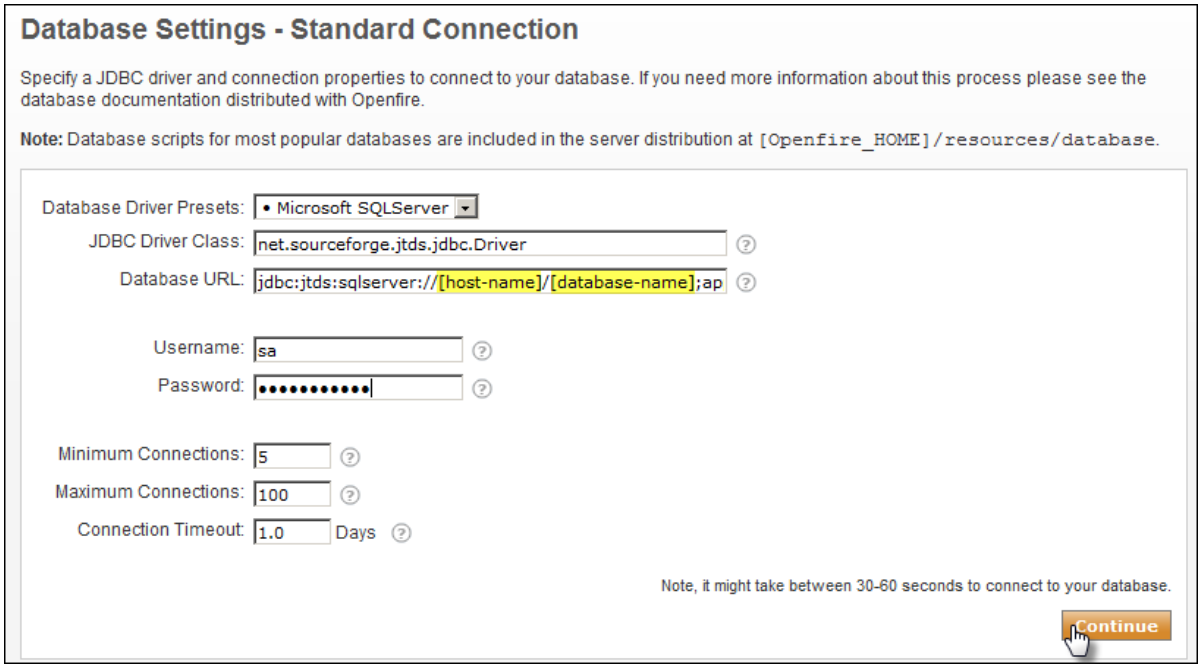


Parameter	Value in this task	Description
Domain	sm950.training.com	Domain name of the Openfire server host. In the all-in-one example, set the domain to sm950.training.com. Note that this domain has no relationship with LW-SSO. You can type any value, including symbols such as underline(_) and hyphen(-). This value is used on the SM collaboration setting page later.
Admin Console Port	9090	The port used for unsecured Admin Console access. The default value is 9090. Leave this port to its default value if you do not need to open an HTTP port.
Secure Admin Console Port	9091	The HTTPS port used for secured Openfire Admin Console access. The default value is 9091.
Property Encryption via	AES	The encryption algorithm used by the Openfire server to prevent sensitive data from being exposed. The default option is AES.
Property Encryption Key	sm950training	Specify the AES encryption key. This field is mandatory. You can specify any value in the first field, and then type this value again in the second field.

8. Click **Continue** on the Database Settings screen.



9. Specify a JDBC driver and the connection properties to connect to your database. Update the fields as illustrated below on the Database Settings – Standard Connection screen, and then click **Continue**.



Parameter	Value in this task	Description
Database Driver Presets	Microsoft SQL Server	Select the database type of Service Manager. You can select either SQL server or Oracle.
JDBC Driver Class	Do not modify the default value	Value in this field is populated automatically after the database type is selected.

Parameter	Value in this task	Description
Database URL	jdbc:jtds:sqlserver://SM950BETA/SM950;appName=jive	Value in this field is populated automatically after the database type is selected. ◦ The default Oracle database URL is `jdbc:oracle:thin:@[host-name]:1521:[SID]`, where [host-name] and [SID] are the actual values of you server. ◦ The default Microsoft SQL server database URL is `jdbc:jtds:sqlserver://[host-name]/[database-name];appName=jive`, where [host-name] and [database-name] are the actual values of you server. If you have multiple database instances on a SQL server, refer to the **Named and Multiple SQL Server Instances** section on the Building the Connection URL web page for more information about the database URL configuration.
Username	<*Your Service Manager database user name*>	Specify the user name to log on to the Service Manager database.
Password	<*Your Service Manager database password*>	Specify the password to log on to the Service Manager database. HPE suggests that you use a

Parameter	Value in this task	Description
		strong password.
Minimum Connections	5	Specify the minimum number of database connections the connection pool should maintain. The default value is 5.
Maximum Connections	100	Specify the maximum number of database connections the connection pool should maintain. The default value is 100.
Connection Timeout	1.0	Specify the time (in days) before connections in the connection pool are recycled. The default value is 1.0.

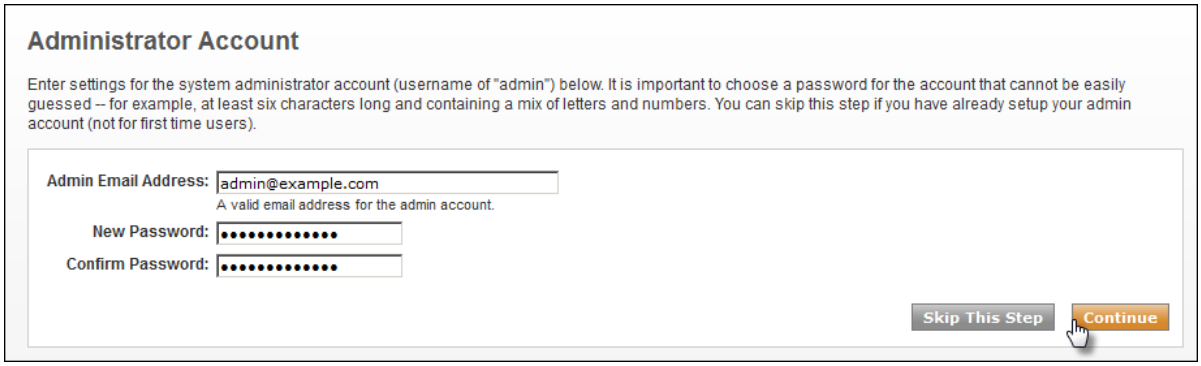
Note:

- If you are working with an Oracle database, copy the JDBC driver (for example, ojdbc6.jar) to the <sm9.xx.00xx-ChatServer>\lib directory before starting the chat server.
- Service Manager Collaboration uses the Service Manager database and inserts a number of Openfire tables into the database. Each table name is prefixed with "`of`". Therefore, you need to update the [host-name] with your database host name, and the [database-name] with your Service Manager database name in the Database URL field. It may take a while to connect to the database.

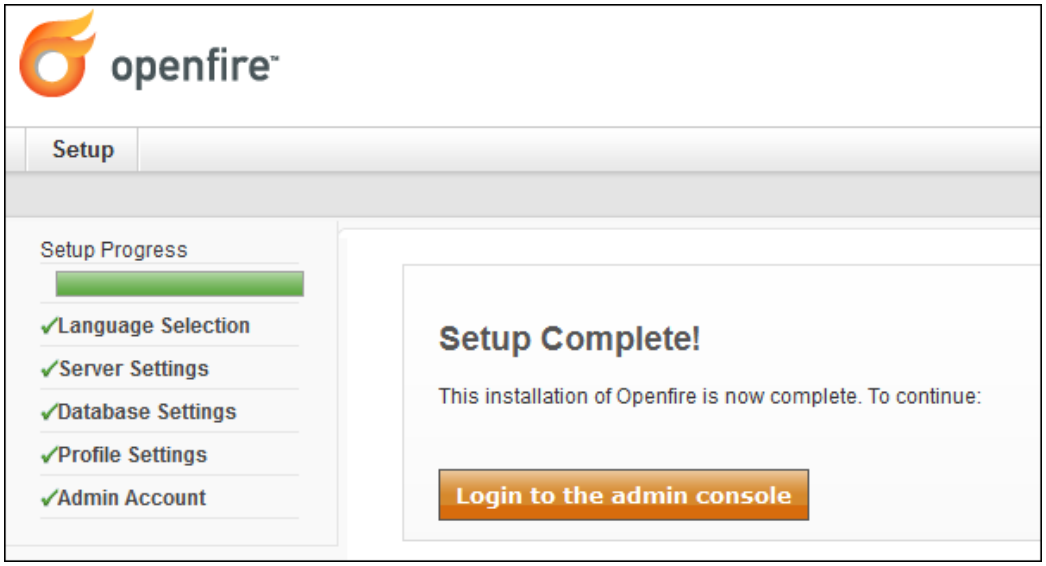
10. Click **Continue** on the Profile Settings screen.

11. Create the user name and password for your Openfire administrator on the Administrator Account screen. Later you will log on to Openfire as `admin` with this password. Click **Continue** to finish the

Openfire installation



12. Your Openfire setup is complete now.



13. Click the **Login to the admin console** button to log on to your Openfire Administration Console.
14. Click **Server** > **Server Manager** > **System Properties**, and then manually add the following properties to the list:

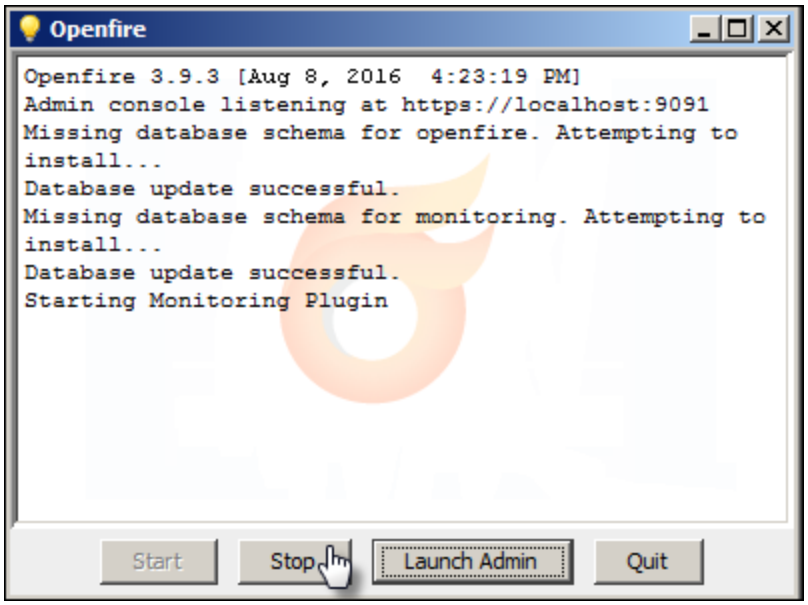
Property name	Description	Property value
xmpp.client.processing.threads	The thread pool of the woker pool in Openfire to process incoming XMPP requests. The default value is 32, which can be increased to 254 for heavy loads.	32

Property name	Description	Property value
lyncplugin.brokerService.memoryLimit	The total memory size of the message queues between Collaboration and the Lync server when you are integrating Collaboration with Lync. You can increase the value for heavy message queues.	1024
lyncplugin.brokerService.policy.memoryLimit	The memory size of each message queue between Collaboration and the Lync server when you are integrating Collaboration with Lync. You can increase the value when the message queue is considered as a bottleneck.	64

15. Click **Group Chat** > **Group Chat Settings** > **conference** > **Other Settings**.
16. In the **Conversation Logging** section, update the values as follows:

Property	Description	Value
Flush interval (seconds)	The two parameters control the frequency of inserting the chat log to the database. The recommended value is 3000 records per 30s.	30
Batch size		3000

17. Click **Save Settings**.
18. Close the web browser tab.
19. Click **Stop** on the Openfire screen.



Replace the server certificate and OpenSSL connection

> **Important:** The *.bat files in the Single Signon Authentication.zip package are used for certificate generation for testing and demonstration purposes on a test environment only. HPE recommends you to use more formal certificates generated by a third party organization so as to meet higher security standards on a production environment.

Follow these steps:

1. Download Single Signon Authentication.zip and save it to your computer. Unzip this package, and then run tso_srv_slvt.bat and tso_cln_slvt.bat to create the following certificate files:

Directory	Files
Certs\	Cacerts clientpubkey.cert mycacert.pem mycacert.srl scclientcert.pem smservercert.pem trustedclients.keystore
Key\	cakey.pem server.keystore <FQDN of the Chat Server host>.keystore

> **Note:**
> - You must set the JAVA_HOME parameter in the two .bat files to the installation path of

the JRE that you want to use. For example, `JAVA_HOME="C:\Program Files (x86)\Java\jdk1.8.0_81\jre"`.

- If this is not the first time that you run these two files, you need to navigate to the %JAVA_HOME%/lib/security directory and then run the **keytool -list -keystore cacerts|findstr servicemanager** command to check whether the cacerts file exists or not. If this file already exists, you may need remove it by running the **keytool -delete -alias servicemanager -keystore cacerts** command before you run the server bat files.
- You must run tso_srv_slvt.bat before tso_cln_slvt.bat. Additionally, make sure that no CA uses `servicemanager` as an alias before running tso_srv_slvt.bat.
- When running tso_srv_slvt.bat, make sure that you type the same FQDN of the chat server host when you are asked to enter the common name of the root CA and of the server certificate.
- When running tso_cln_svlt.bat, you need to append the FQDN of the chat server host as the bat parameter. For example, `tso_cln_svlt.bat sm950.training.com`. Make sure that you type the same FQDN of the chat server host when you are asked to enter your first and last name.

2. Log on to your Openfire Administration Console, and then click **Server** > **Server Manager** > **System Properties**. Alternatively, access https://localhost:9091/server-properties.jsp.
3. Add the following properties:

Property Name	Property Value
xmpp.socket.ssl.storeType	<JKS or PKCS12>
xmpp.socket.ssl.keystore	<path of the keystore, relative to OpenfireHome>
xmpp.socket.ssl.keypass	<password of server.keystore>
xmpp.socket.ssl.truststore	<path of the trust store path>
xmpp.socket.ssl.trustpass	<password of CA truststore>
xmpp.socket.ssl.client.truststore	<path of the trusted client store>
xmpp.socket.ssl.client.trustpass	<password of trustedclients>

Also, you can configuring these SSL keystore related parameters in /conf/openfire.xml. See the following sample default configuration:

```
<securityConfig>
    <ssl>
       <keyStoreType>jks</keyStoreType>
```

```
        <keyStorePath>resources/security/keystore</keyStorePath>
        <keyStorePassword>changeit</keyStorePassword>
        <trustStorePath>resources/security/truststore</trustStorePath>
        <trustStorePassword>changeit</trustStorePassword>

<clientTrustStorePath>
resources/security/client.truststore</clientTrustStorePath>
        <clientTrustStorePassword>changeit</clientTrustStorePassword>
    </ssl>
    …
</ securityConfig>
```

After you have updated these parameters in openfire.xml, save your changes and then restart the chat server to encrypt these sensitive values automatically.

4. Follow these steps to replace the certificate files.
   a. Copy Cacerts, trustedclients.keystore and server.keystore to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\resources\security folder, and delete the original certificate files in this folder.
   b. Rename Cacerts to truststore.
   c. Rename trustedclients.keystore to client.truststore.
   d. Rename server.keystore to keystore.
5. Restart the Openfire chat server.

Task 6: Deploy the chat service

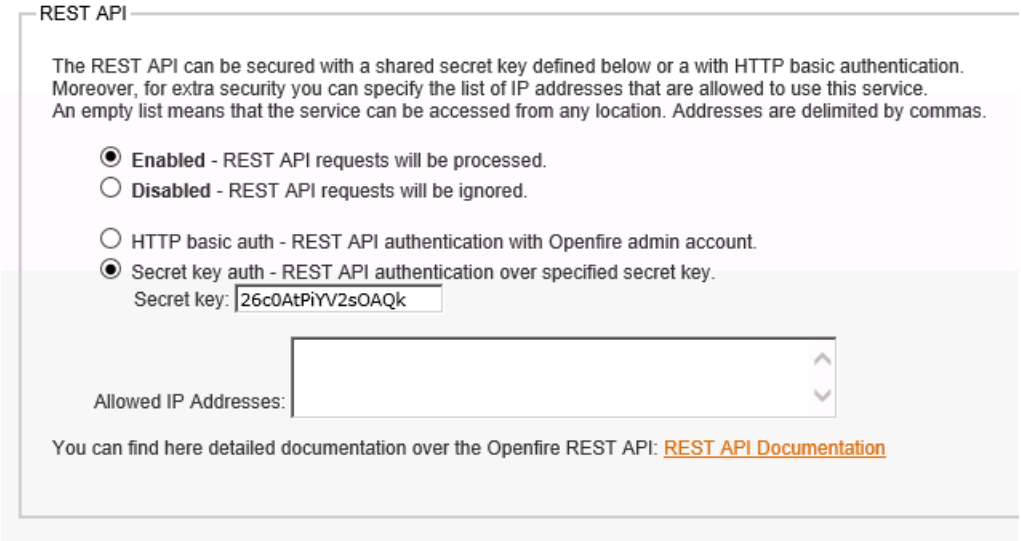
In this task, you will install the chat service for End User Chat.

Follow these steps:

1. Save the chat service installer chat-msvc-9.50.zip from Service Manager installation package 2 to the same computer on which the chat server was deployed.
2. Log on to your Openfire Administration Console.
3. Click the **User/Groups** tab and create an Openfire user. For example:

   User name: publishadmin

   Password: admin123
4. To enable the virtual agent, click **Server** > **Server Settings** > **REST API**. Enable REST API and record the secret key auth.



5. Save your changes, and then restart the Openfire chat server.
6. Run tso_srv_slvt.bat to create the following certificate files:

Directory	Files
Certs\	Cacerts clientpubkey.cert mycacert.pem mycacert.srl scclientcert.pem smservercert.pem trustedclients.keystore
Key\	cakey.pem server.keystore <FQDN of the Chat Service host>.keystore

Note:
- When running tso_cln_svlt.bat, you need to append the FQDN of the Chat Service host as the bat parameter. For example, `tso_cln_svlt.bat sm950.training.com`. Make sure that you type the same FQDN of the Chat Service host when you are asked to enter your first and last name.
- After the client keystore is created, update the new trustedclients.keystore file in C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\resources\security folder and rename the file to client.truststore.

7. Copy the CA certificates file (Cacerts) and the chat service client keystore (<FQDN of the Chat

Service host>.keystore) to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\conf folder.

8. Run tso_2nd_srvs_svlt.bat to generate a second server.keystore by following the instructions as described in *Task 5: Deploy the chat server > Replace the server certificate and OpenSSL connection > step 3* in this document.
9. Configure SSL in the Service Manager server and web tier by following the instructions as described in the "Example: Enabling trusted sign-on" topic in the Service Manager Help Center.
10. Copy app.properties and config.yml from C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\conf\samples\https to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\conf, and replace the original files. Open the chat service configuration file app.properties with a text editor.
11. Update the related parameters:

```
Factory.password,pubSubServiceConfig.userName,pubSubServiceConfig.password,
chatServerConfig.restApiSecretKey,app.keyStorePassword,app.trustStorePassword
app.encryptionKey=
daoFactory.serviceEndPoint=http://sm950.training.com:13080
daoFactory.userName=falcon
daoFactory.password=
pubSubServiceConfig.userName=publishadmin
pubSubServiceConfig.password=admin123

chatServiceUrl=/chatservice/

chatServerConfig.domain=sm950.training.com
chatServerConfig.host=sm950.training.com
chatServerConfig.port=5222
chatServerConfig.boshUrl=/of-http-bind/
chatServerConfig.pluginUrl=/of-plugins/
chatServerConfig.restApiSecretKey=26oOAtPiYV2sQAQk
```

Parameter	Description
daoFactory.serviceEndPoint	The Service Manager server's URL.
daoFactory.username	The Backend user name for chat service to access Service Manager. **Important:** The backend user must be an SM user with the "system administrator" privilege and the "RESTful API" capability.
daoFactory.password	The daoFactory user password.
pubSubServiceConfig.userName	The user name created in step 3.

Parameter	Description
pubSubServiceConfig.password	The user password created in step 3.
chatServerConfig.domain	The domain user filled during install chat server.
chatServerConfig.host	The chat server computer name or IP.
chatServerConfig.restApiSecretKey	The secret key you recorded in *step 4*.

12. Save your changes and close this file.
13. To install the chat service as a Windows service, open a DOS command prompt and change the directory to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\bin.
14. Run the **install-service.bat** command to install the Service Manager chat service as a Windows service.

> **Note:** HPE recommends to use 64-bit Java because 32-bit Java may have potential performance limitations. However, if you are working with 32-bit Java, follow these steps so that the Service Manager chat service Windows service can start successfully:
>
> a. Open C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\bin\startup.bat with a text editor.
>
> b. Update the memory setting as follows:
>
> ```
> SET CHAT_SVC_JVM_OPTIONS=-XX:ThreadStackSize=256 -Xms512m -Xmx1024m
> ```
>
> c. Save your changes and close this file.
>
> d. Open C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\bin\ install-service.bat with a text editor.
>
> e. Update the `ThreadStackSize` memory setting to `ThreadStackSize=256 -Xms512m -Xmx1024m`.
>
> f. Save your changes and close this file.

You can run **nssm edit HpeSmChatService** to edit the corresponding configurations after the Windows service is installed.

> **Tip:** To remove this Windows service, run the **nssm remove HpeSmChatService** command.

Task 7: Deploy the End User Chat UI

The End User Chat UI consists of the End User Chat window and the End User Chat button. Follow these steps to deploy the End User Chat UI:

1. Save the End User Chat UI installer chat-ui-9.50.war from Service Manager installation package 2 to your computer.
2. Rename the installer to chatui.war, and then copy it to the same Tomcat on which Service Manager web tier is deployed. For example, C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps.

Task 8: Deploy the Apache HTTP server

In this task, you will deploy and configure the Apache HTTP server for Service Manager Collaboration.

> **Note:** The deployment instructions in this document are for a sample OpenSSL Apache server. If you have profound web server knowledge, you can also customize your web server by following your own business rules.

Follow these steps:

1. Download Apache with OpenSSL (for example, httpd-2.4.xx-x64.zip for Apache 2.4, or httpd-2.2.31-x64-r3.zip for Apache 2.2) from here.

   You can also download a pre-configured Apache 2.4 from HPE Live Network.

   Extract the zip file to C:\. This unzip process creates a new C:\Apache24 directory or a new C:\Apache22 directory.
2. (For Apache 2.4) Navigate to the C:\Apache24\conf folder.

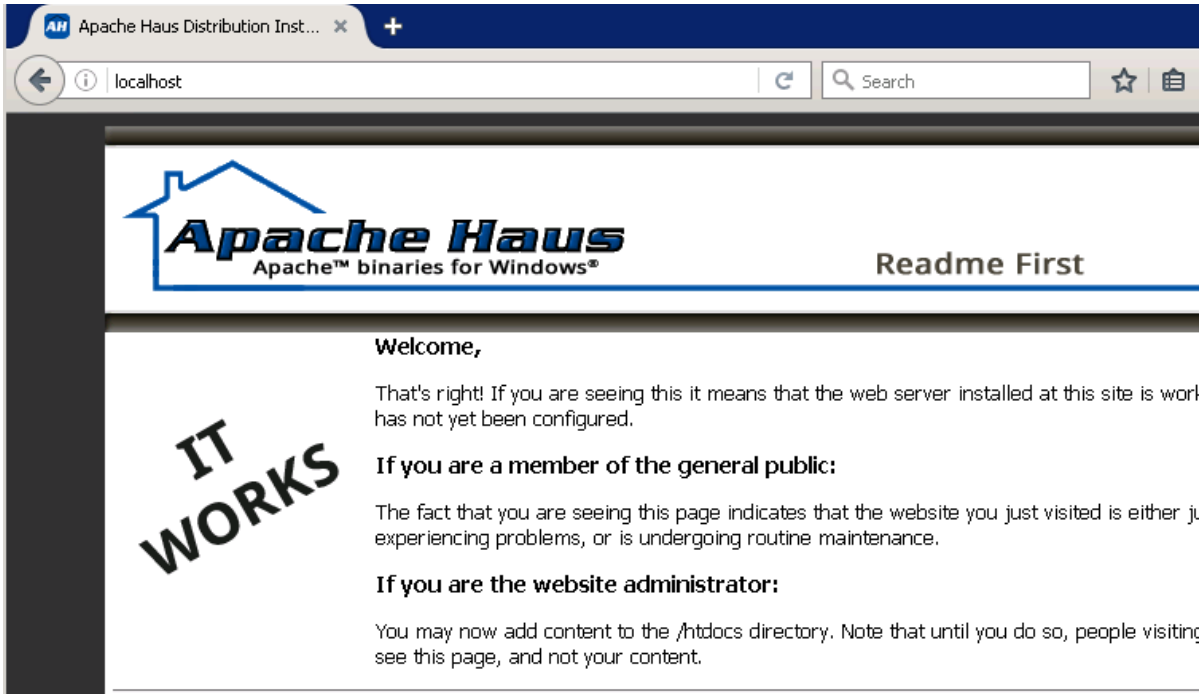
   (For Apache 2.2) Navigate to the C:\Apache22\conf folder.
3. Make a copy of the httpd.conf file and save it as httpd_OOB.conf.
4. Open the httpd.conf file with a text editor.
5. Locate `httpd-vhosts.conf`, and then uncomment `Include conf/extra/httpd-vhosts.conf`.
6. Save and close the httpd.conf file.
7. (For Apache 2.4) Navigate to the C:\Apache24\conf\extra directory.

   (For Apache 2.2) Navigate to the C:\Apache22\conf\extra directory.
8. Make a copy of the httpd-vhosts.conf file and save it as httpd-vhosts_OOB.conf.
9. (For Apache 2.4) Navigate to the C:\Apache24\bin folder.

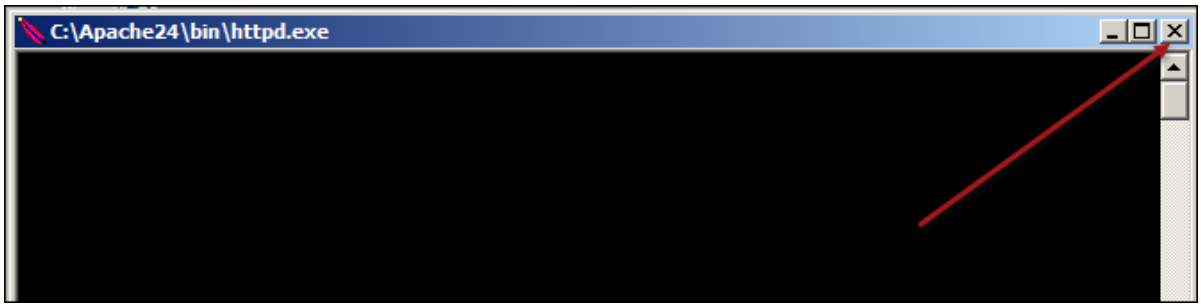
   (For Apache 2.2) Navigate to the C:\Apache22\bin folder.
10. Double-click httpd.exe to start the Apache server.

    The httpd.exe window opens. Click the minimize button to minimize this window.

11. In your web browser, type `http://localhost` and press Enter. The following page is displayed, indicating Apache has started successfully.



12. Close the browser.
13. Close the Apache httpd.exe window.



> **Note:** The steps below will install Apache as a Windows service.

14. (For Apache 2.4) Navigate to the C:\Apache24\bin folder. Open a DOS command prompt and change the directory to C:\Apache24\bin.

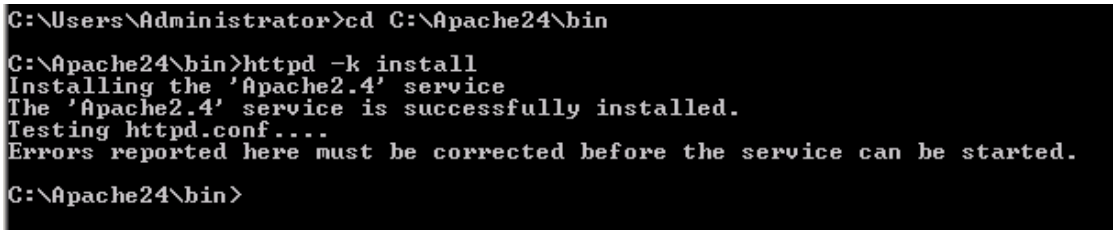
    ```
    cd C:\Apache24\bin
    ```

    (For Apache 2.2) Navigate to the C:\Apache22\bin folder. Open a DOS command prompt and change the directory to C:\Apache22\bin.

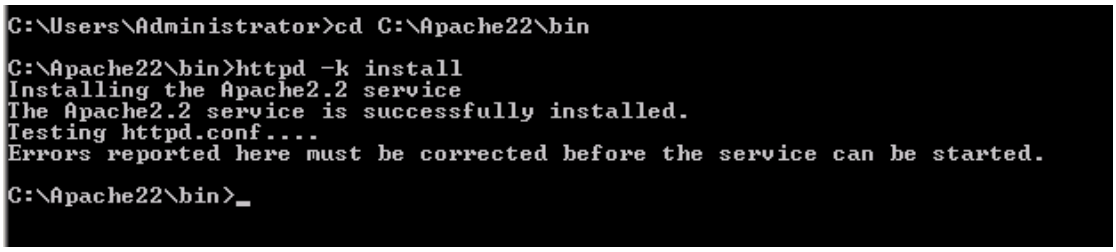
```
cd C:\Apache22\bin
```

15. Run the **httpd –k install** command to install the Windows service.

    For Apache 2.4:



    For Apache 2.2:



    > **Note:** If you see an error here, navigate to the logs directory and check the error.log file. Depending on the error, you may need to repeat the steps above. To verify whether the error still exists, type **httpd –k start** to start Apache from the command line.

16. (For Apache 2.4) Go to Windows Services, and start the newly installed **Apache2.4** service.

    (For Apache 2.2) Go to Windows Services, and start the newly installed **Apache2.2** service.

Open Apache SSL connection

Follow these steps:

1. (For Apache 2.4) Navigate to the C:\Apache24\conf\extra directory.

   (For Apache 2.2) Navigate to the C:\Apache22\conf\extra directory.

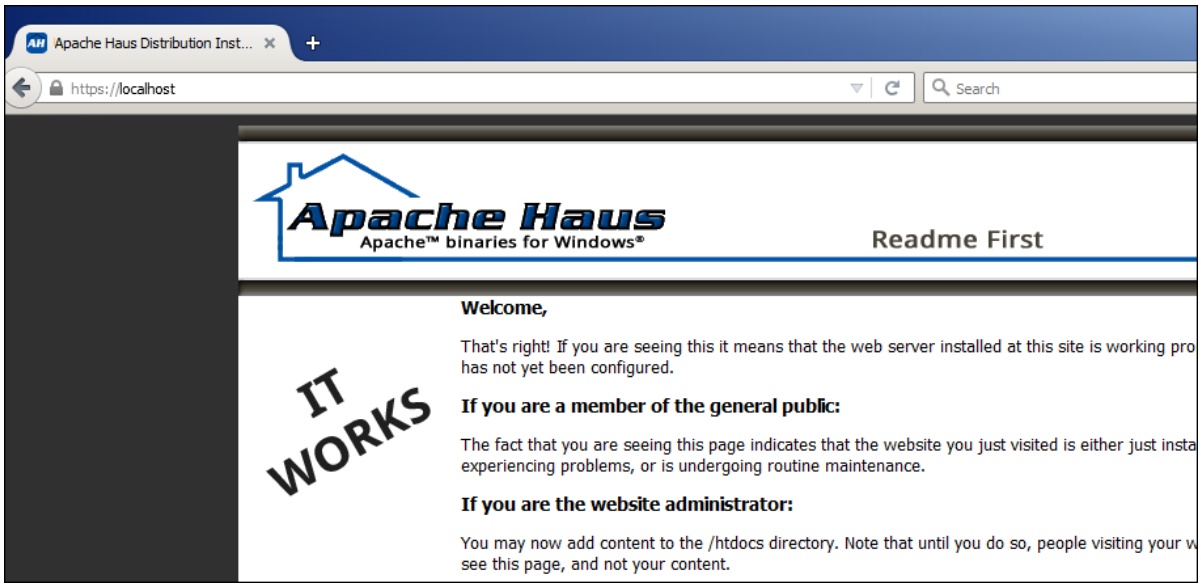
2. Make a copy of the httpd-ahssl.conf file and save it as httpd-ahssl_OOB.conf.
3. Open httpd-ahssl.conf with a text editor.
4. Locate the `SSL Protocols` section.
5. Change `SSLProtocol all` to `SSLProtocol -all +TLSv1 +TLSv1.1 +TLSv1.2` so that only TLS v1.0, TLS v1.1, and TLSv1.2 are enabled on the Apache server.

```
#   SSL Protocols:
#   List the protocols that the client is permitted to negotiate.
```

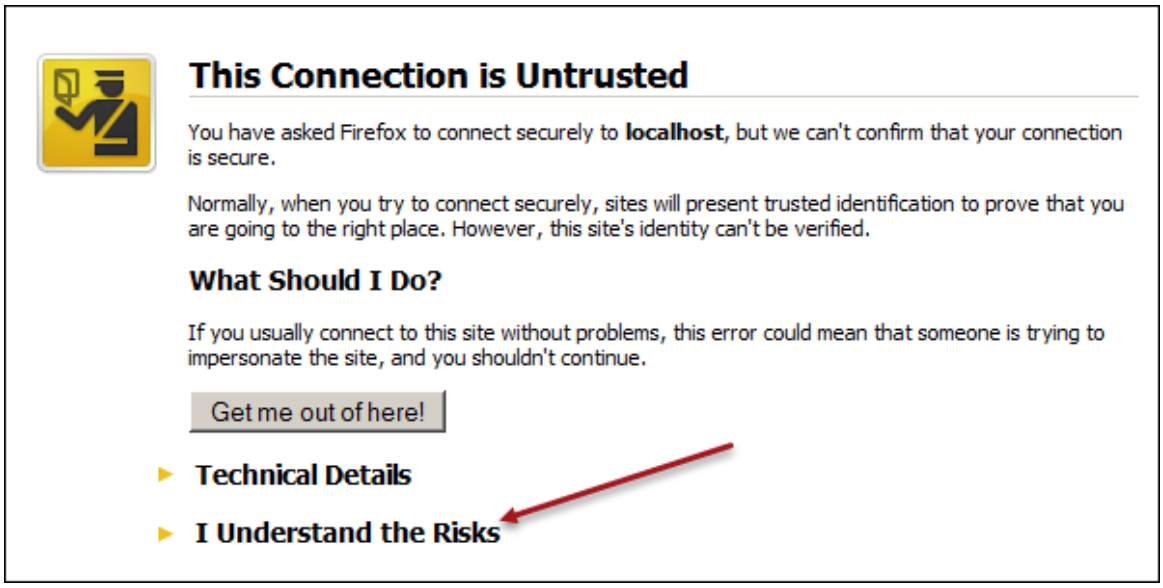
```
#   See the mod_ssl documentation for a complete list.
SSLProtocol all +TLSv1 +TLSv1.1 +TLSv1.2
```

> **Tip:** For more information about Apache SSL configuration, click here.

6. Save and close the httpd-ahssl.conf file.
7. Restart Apache server.
8. In your web browser, type `https://localhost` and press Enter. The following page is displayed, indicating SSL is enabled successfully.



> **Note:** If the following screen is displayed, click **I Understand the Risks** and proceed.



Task 9: Connect Apache to Tomcat

In this task, you will set up Apache to connect to Tomcat through the AJP port. Consequently, Secure Sockets Layer (SSL) is open by default. You can perform this step rather than enable full SSL on the Service Manager environment.

Follow these steps:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\conf directory.
2. Open the server.xml file with a text editor.
3. Make sure that the AJP 1.3 Connector port is set to `8009`.

   ```
   <!-- Define an AJP 1.3 Connector on port 8009 -->
   <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
   ```

   > **Note:** If you need to change it to another port, make a note of that port number as you will need it later in this task.

4. Save and close the server.xml file.

Steps for Apache 2.4

> **Note:** If you are using the pre-configured Apache downloaded from HPE Live Network, skip step 1 to 15 and start with step 16.

1. Navigate to the C:\Apache24\conf directory.
2. Open the httpd.conf file with a text editor.

   The next few steps describe how to uncomment a number of `LoadModule` codes in the httpd.conf file.

3. Locate `lbmethod`.

```
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
#LoadModule ldap_module modules/mod_ldap.so
```

4. Uncomment two lines as shown below:

```
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
#LoadModule ldap_module modules/mod_ldap.so
```

5. Locate the following section by searching for `proxy_module`.

```
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_html_module modules/mod_proxy_html.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
```

6. Uncomment 8 lines as shown in the following:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
```

7. Locate the following section by searching for `slotmem_shm`.

```
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
```

8. Uncomment the following line:

```
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
```

9. Locate the following section by searching for `xml2enc_module`.

```
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule watchdog_module modules/mod_watchdog.so
#LoadModule xml2enc_module modules/mod_xml2enc.so
<IfModule unixd_module>
```

10. Uncomment the following line:

```
LoadModule xml2enc_module modules/mod_xml2enc.so
```

11. Locate the following section. You may need to search for `mod_proxy_html` twice.

```
# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/httpd-proxy-html.conf
</IfModule>
```

12. If the `Include` line does not contain `Include conf/extra/httpd-proxy-html.conf`, change the `Include` line to `Include conf/extra/httpd-proxy-html.conf`.

13. Browse to the end of the file, and then add the line in bold:

```
<IfModule http2_module>
       ProtocolsHonorOrder On
       Protocols h2 h2c http/1.1
</IfModule>
Include conf/httpd-proxy_ajp_loadbalanced.conf
```

14. Comment out the lines in bold by inserting # in front of each line:

```
#<IfModule http2_module>
       #ProtocolsHonorOrder On
       #Protocols h2 h2c http/1.1
#</IfModule>
Include conf/httpd-proxy_ajp_loadbalanced.conf
```

15. Save and close the httpd.conf file.

16. Navigate to the C:\Apache24\conf directory, and then create a new file called httpd-proxy_ajp_loadbalanced.conf.

```
<Proxy balancer://smcluster>
BalancerMember ajp://localhost:8009 route=161652175430301
Require all granted
</Proxy>
<Location /webtier-9.50>
Options FollowSymLinks
Require all granted
ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
<Location /chatui>
Options FollowSymLinks
Require all granted
ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
```

> **Caution:**
> - You must paste `ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid nofailover=On` in one line.
> - You must paste `ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid nofailover=On` in one line.

17. The script in the previous step assumes that the web tier directory is webtier-9.50 and the chat UI directory is chatui(see the line below). If your web tier or chat UI uses another name, update the httpd-proxy_ajp_loadbalanced.conf file with the actual name of your web tier.

    ```
    <Location /webtier-9.50>
    balancer://smcluster/webtier-9.50
    <Location /chatui>
    balancer://smcluster/chatui
    ```

18. In step 3 in this task, you configured the `AJP 1.3 Connector` port in the server.xml file. If this port is 8009, continue with the next step; if the connector listens on another port, update the following line in the httpd-proxy_ajp_loadbalanced.conf file with that port number.

    If Apache is deployed on the same computer in the all-in-one example described in this document, use `ajp://localhost:8009`. Otherwise, you need to update this value to the correct IP of Tomcat.

    ```
    BalancerMember ajp://localhost:8009 route=161652175430301
    ```

19. Access Apache's link with Apache's FQDN. In this all-in-one example, access https://sm950.training.com/webtier-9.50/index.do, and then log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

If you are directed to a Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.

20. Log out from Service Manager.

Steps for Apache 2.2

1. Navigate to the C:\Apache22\conf directory.
2. Open the httpd.conf file with a text editor.

   The next few steps describe how to uncomment a number of `LoadModule` codes in the httpd.conf file.

3. Locate `proxy_module`.
4. Uncomment the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.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
```

5. Browse to the end of the file, and then add the line in bold:

```
<IfModule http2_module>
    ProtocolsHonorOrder On
    Protocols h2 h2c http/1.1
</IfModule>
Include conf/httpd-proxy_ajp_loadbalanced.conf
```

6. Save your changes and close the httpd.conf file.
7. Navigate to the C:\Apache22\conf directory, and then create a new file called httpd-proxy_ajp_loadbalanced.conf.
8. Copy and paste the following codes to the httpd-proxy_ajp_loadbalanced.conf file:

```
<Proxy balancer://smcluster>
BalancerMember ajp://localhost:8009 route=161652175430301
Order allow,deny
Allow from all
</Proxy>
<Location /webtier-9.50>
Options FollowSymLinks
Order allow,deny
Allow from all
ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid
nofailover=On
```

```
</Location>
<Location /chatui>
Options FollowSymLinks
Order allow,deny
Allow from all
ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid
nofailover=On
</Location>
```

> **Caution:**
> - You must paste `ProxyPass balancer://smcluster/webtier-9.50 stickysession=JSESSIONID|jsessionid nofailover=On` in one line.
> - You must paste `ProxyPass balancer://smcluster/chatui stickysession=JSESSIONID|jsessionid nofailover=On` in one line.

9. The script in the previous step assumes that the web tier directory is webtier-9.50 and the chat UI directory is chatui(see the line below). If your web tier or chat UI uses another name, update the httpd-proxy_ajp_loadbalanced.conf file with the actual name of your web tier.

   ```
   <Location /webtier-9.50>
   balancer://smcluster/webtier-9.50
   <Location /chatui>
   balancer://smcluster/chatui
   ```

10. In step 3 in this task, you configured the `AJP 1.3 Connector` port in the server.xml file. If this port is 8009, continue with the next step; if the connector listens on another port, update the following line in the httpd-proxy_ajp_loadbalanced.conf file with that port number.

    If Apache is deployed on the same computer in the all-in-one example described in this document, use `ajp://localhost:8009`. Otherwise, you need to update this value to the correct IP of Tomcat.

    ```
    BalancerMember ajp://localhost:8009 route=161652175430301
    ```

11. Access Apache's link with Apache's FQDN. In this all-in-one example, access https://sm950.training.com/webtier-9.50/index.do, and then log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

    If you are directed to a Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.

    > **Note:** From now on, you must use HTTPS and the fully qualified domain name (FQDN) in the web tier URL when logging on to the Service Manager web client.

12. Log out from Service Manager.

Open SSL connection to Webtier

1. Open the web.xml file with a text editor.
2. Locate the `secureLogin` parameter and set it to `true`.
3. Save and close the web.xml file.
4. Go to Windows Services and restart the **HPE Service Manager 9.50 Server** service.
5. Access https://sm950.training.com/webtier-9.50/index.do, and then log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

   If you are directed to a Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.

   > **Note:** From now on, you must use HTTPS and the fully qualified domain name (FQDN) in the web tier URL when logging on to the Service Manager web client.

6. Log out from Service Manager.

Task 10: Enable reverse proxy in Apache

In this task, you will enable the reverse proxy in Apache to protect sensitive information of Openfire (the IP address, ports, and so on). Follow the steps for your Apache version (2.4 or 2.2).

> **Important:** You must use the same Apache server that connects to Tomcat in the previous task.

Open Apache 2.4 SSL reverse proxy connection

Follow these steps:

1. Navigate to the C:\Apache24\conf\extra directory.
2. Open the httpd-ahssl.conf file with a text editor.
3. Locate the following section by searching for "`ServerName localhost`".

```
<VirtualHost _default_:443>
SSLEngine on
ServerName localhost:443
SSLCertificateFile "${SRVROOT}/conf/ssl/server.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/server.key"
DocumentRoot "${SRVROOT}/htdocs"
# DocumentRoot access handled globally in httpd.conf
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
```

```
Require all granted
</Directory>
</virtualhost>
```

4. Insert the lines in bold to this section as shown below (insert 5 lines below the "`SSLEngine on`" line and 6 lines between `</Directory>` and `</virtualhost>`).

```
<VirtualHost _default_:443>
SSLEngine on
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ServerName localhost:443
SSLCertificateFile "${SRVROOT}/conf/ssl/server.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/server.key"
DocumentRoot "${SRVROOT}/htdocs"
# DocumentRoot access handled globally in httpd.conf
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
ProxyPass /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPass /of-plugins https://sm950.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm950.training.com:9091/plugins
ProxyPass /chatservice https://sm950.training.com:8488
ProxyPassReverse /chatservice https://sm950.training.com:8488
</virtualhost>
```

   - `/of-http-bind` is the path of the Openfire HTTP binding (also known as BOSH) reverse configuration, whereas `/of-plugins` is the identifier of the Openfire plugin directory. These two parameters will be used later on the SM collaboration setting page.
   - You need to change `sm950.training.com` to your own host name. In addition, 9091 is the secure admin console port for the chat server. If you changed this port from the default value during the chat server installation, you need to update the port number here.

5. Locate the following section by searching for "`ServerName serverone.tld`" .

```
<VirtualHost *:443>
SSLEngine on
ServerName serverone.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/serverone.crt"
```

```
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/serverone.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
</virtualhost>
```

6. Insert the lines in bold to this section as shown below (insert 5 lines below the "`SSLEngine on`" line and 6 lines between `</Directory>` and `</virtualhost>`).

```
<VirtualHost *:443>
SSLEngine on
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ServerName serverone.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/serverone.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/serverone.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
ProxyPass /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPass /of-plugins https://sm950.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm950.training.com:9091/plugins
ProxyPass /chatservice https://sm950.training.com:8488
ProxyPassReverse /chatservice https://sm950.training.com:8488
</virtualhost>
```

7. Locate the following section by searching for "`ServerName servertwo.tld`".

```
<VirtualHost *:443>
SSLEngine on
ServerName servertwo.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/servertwo.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/servertwo.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
```

```
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
</virtualhost>
```

8. Insert the lines in bold to this section as shown below (insert 5 lines below the "`SSLEngine on`" line and 6 lines between `</Directory>` and `</virtualhost>`).

```
<VirtualHost *:443>
SSLEngine on
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ServerName servertwo.tld:443
SSLCertificateFile "${SRVROOT}/conf/ssl/servertwo.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/servertwo.key"
DocumentRoot "${SRVROOT}/htdocs"
CustomLog "${SRVROOT}/logs/ssl_request.log" \
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Directory "${SRVROOT}/htdocs">
Options Indexes Includes FollowSymLinks
AllowOverride AuthConfig Limit FileInfo
Require all granted
</Directory>
ProxyPass /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPass /of-plugins https://sm950.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm950.training.com:9091/plugins
ProxyPass /chatservice https://sm950.training.com:8488
ProxyPassReverse /chatservice https://sm950.training.com:8488
</virtualhost>
```

9. Save and close the httpd-ahssl.conf file.

Open Apache 2.2 SSL reverse proxy connection

Follow these steps:

1. Navigate to the C:\Apache22\conf\extra directory.
2. Open the httpd-ahssl.conf file with a text editor.
3. Locate `SSLEngine`.
4. Add the following lines below `SSLEngine on`.

```
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
```

5. Add the following lines below `</Directory>` but before `</virtualhost>`.

   ```
   ProxyPass /of-http-bind https://sm950.training.com:7443/http-bind
   ProxyPassReverse /of-http-bind https://sm950.training.com:7443/http-bind
   ProxyPass /of-plugins https://sm950.training.com:9091/plugins
   ProxyPassReverse /of-plugins https://sm9450.training.com:9091/plugins
   ```

   `/of-http-bind` is the path of the Openfire HTTP binding (also known as BOSH) reverse configuration, whereas `/of-plugins` is the identifier of the Openfire plugin directory. These two parameters are used on the SM collaboration setting page later.

   > **Note:** You can change `sm950.training.com` to your host name. In addition, 9091 is the secure admin console port for the chat server. If you changed this port from the default value during the chat server installation, you need to update the port number here.

6. Locate `SSLEngine` again.
7. Add the following codes below `SSL Engine on`.

   ```
   SSLProxyEngine On
   SSLProxyVerify none
   SSLProxyCheckPeerCN off
   SSLProxyCheckPeerExpire off
   ```

8. Add the following lines below `</Directory>` but before `</virtualhost>`.

   ```
   ProxyPass /of-http-bind https://sm950.training.com:7443/http-bind
   ProxyPassReverse /of-http-bind https://sm950.training.com:7443/http-bind
   ProxyPass /of-plugins https://sm950.training.com:9091/plugins
   ProxyPassReverse /of-plugins https://sm950.training.com:9091/plugins
   ProxyPass /chatservice https://sm950.training.com:8488
   ProxyPassReverse /chatservice https://sm950.training.com:8488
   ```

9. Locate `SSLEngine` one more time.
10. Add the following lines below `SSL Engine on`.

    ```
    SSLProxyEngine On
    SSLProxyVerify none
    SSLProxyCheckPeerCN off
    SSLProxyCheckPeerExpire off
    ```

11. Add the following lines below `</Directory>` but before `</virtualhost>`.

```
ProxyPass /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm950.training.com:7443/http-bind
ProxyPass /of-plugins https://sm950.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm950.training.com:9091/plugins
ProxyPass /chatservice https://sm950.training.com:8488
ProxyPassReverse /chatservice https://sm950.training.com:8488
```

12. Save and close the httpd-ahssl.conf file.

Task 11: Define the display of the End User Chat UI in ESS portal

> **Note:** Skip this task if your organization uses Service Manager Service Portal for end users.

An end user needs to click the chat button to open the End User Chat window. In this task, you will configure the webtier.properties to define how the End User Chat window is displayed on the Service Manager Employee Self-Service (ESS) portal.

Follow these steps:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.50\WEB-INF directory, and then open webtier.properties with a text editor.
2. Locate the `SMC ESS Chat configuration` section, and then update the parameters. See the following table for detailed description:

```
smc.ess.chat.url=http://sm950.training.com/chatui
smc.ess.chat.style.width=300
smc.ess.chat.style.height=400
smc.ess.chat.style.position=br
```

Parameter	Description
smc.ess.chat.url	Specify the absolute URL to the End User Chat UI application. This chat URL is the real URL which you can access through Apache. For example, `https://sm950.training.com/chatui`
smc.ess.chat.style.width	Specify the width of the iFrame which contains the End User Chat window. The unit is pixel.
smc.ess.chat.style.height	Specify the height of the iFrame which contains the End User Chat window. The unit is pixel.
smc.ess.chat.style.position	Specify the position of the End User Chat UI. The available values are `bl` (bottom-left) or `br` (bottom-right).

3. Save your changes and close this file.

Follow these steps to update the chat service URL in Service Manager Chat UI:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\chatui\conf directory, and then open env.js with a text editor.
2. Update the `chatServiceUrl` value, which must be the real URL that you can access through Apache. For example, `https://sm950.training.com/chatservice`

```
(function(scope) {
  var hpe = scope.hpe || (scope.hpe = {});
  hpe.chatui = {
    __env: {
      //The url to access chat service
      chatServiceUrl: 'https://sm950.training.com/chatservice'
    }
  };
})(window);
```

3. Save your changes and close this file.
4. Restart Tomcat.

Task 12: Define the display of the End User Chat UI in Service Manager Service Portal

> **Note:** Skip this task if your organization uses Service Manager ESS portal for end users.

An end user needs to click the chat button to open the End User Chat window. In this task, you will configure the env.js file to define how the End User Chat window is displayed on the Service Manager Service Portal.

> **Note:** The Apache server and Service Manager Service Portal must use SSL certificates issued by the same Certificate Authority (CA) and the SSL certificates or the CA must be trusted by the end user's web browser.

Follow these steps to update the chat service URL in Service Manager Chat UI:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\chatui\conf directory, and then open env.js with a text editor.
2. Update the `chatServiceUrl` value, which must be the real URL that you can access through Apache. For example, `https://sm950.training.com/chatservice`

```
(function(scope) {
  var hpe = scope.hpe || (scope.hpe = {});
  hpe.chatui = {
    __env: {
      //The url to access chat service
      chatServiceUrl: 'https://sm950.training.com/chatservice'
    }
  };
})(window);
```

3. Save your changes and close this file.

Task 13: Configure LW-SSO for the chat server

In this task, you will set up LW-SSO for the Openfire chat server.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\plugins\lwssoplugin folder.
2. Make a copy of the lwssoconf.xml file and save it as lwssoconf_OOB.xml.
3. Open lwssoconf.xml with a text editor.
4. Locate the `domain` parameter and set it to `training.com`.
5. Locate the `initString` parameter and set it to `sm950training`.
6. Save and close the lwssofmconf.xml file.
7. Go to Windows services and restart the **HPE Service Manager 9.50.00xx Chat Server** Windows service.

Task 14: Configure LW-SSO for the chat service

In this task, you will set up LW-SSO for the chat service.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatService\conf folder.
2. Make a copy of the lwssoconf.xml file and save it as lwssoconf_OOB.xml.
3. Open lwssoconf.xml with a text editor.
4. Locate the `domain` parameter and set it to `training.com`.
5. Locate the `initString` parameter and set it to `sm950training`.
6. Save and close the lwssofmconf.xml file.

7. Go to Windows services and restart the **HPE Service Manager 9.50.00xx Chat Service** Windows service.

Task 15: Enable Service Manager Collaboration

By default, the Collaboration feature is disabled after applying the Service Manager 9.50 web tier. In this task, you will log on to Service Manager and set up the Collaboration Configuration.

Follow these steps:

1. Access https://sm950.training.com/webtier-9.50/index.do in your web browser, and then log on to Service Manager as a system administrator.
2. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.
3. Select the **Enable Collaboration** check box to enable Service Manager Collaboration.
4. (Optional) Select the **Enable ESS Lync User** check box so that the Skype users can join IT Collaboration conversations by using Skype.
5. Select whether to enable the End User Chat virtual agent or not.

   > **Important:**
   > To enable the End User Chat virtual agent, your enterprise must own an HPE Smart Analytics license and have enabled Smart Analytics. Otherwise, you cannot save your setting in this Enable End User Chat section.

6. Specify field values as described in the following table.

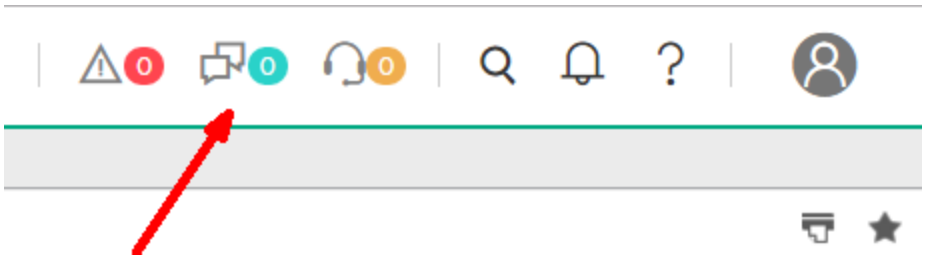
Field	Value in this task	Description
Maximum Participants Per Conversation	200	The maximum number of participants in a conversation. The default value is 200.
Notification Delay Time (Seconds)	30	The maximum time that an online participant has to wait to receive the live conversation notifications. The default value is 30. Notification delay is disabled if this value is set to 0 or minus.
Chat Service URL	https://sm950.training.com:8448/	The chat service URL.
BOSH Path	/of-http-bind/	The HTTP binding (also known as BOSH) path for Openfire to send XMPP messages.

Field	Value in this task	Description
		In the sample reverse proxy configurations in "Task 5: Deploy the chat server" on page 437, this path is `/of-http-bind/`. This field is read-only.
Chat Service Path	/chatservice/	The chat service base path for Restful resources. This field is read-only.
Domain Name	sm950.training.com	Domain name of the Openfire server. This field is read-only.
Plugin Path	/of-plugins/	The Openfire plugin URL. In the sample reverse proxy configurations in "Task 5: Deploy the chat server" on page 437, this value is `/of-plugins/`. This field is read-only.

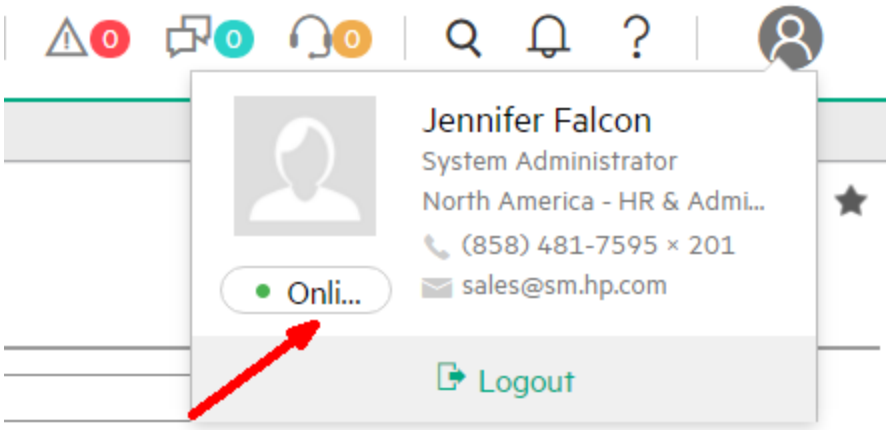
7. Click **Save** and **OK**. It may take a while for the configurations to take effect.
8. Log out of the web client, and then log on as the system administrator again.

   If the system displays the following error message when you log in, check all your settings and then refer to the "Troubleshooting - Failed to connect to the Collaboration server" section:

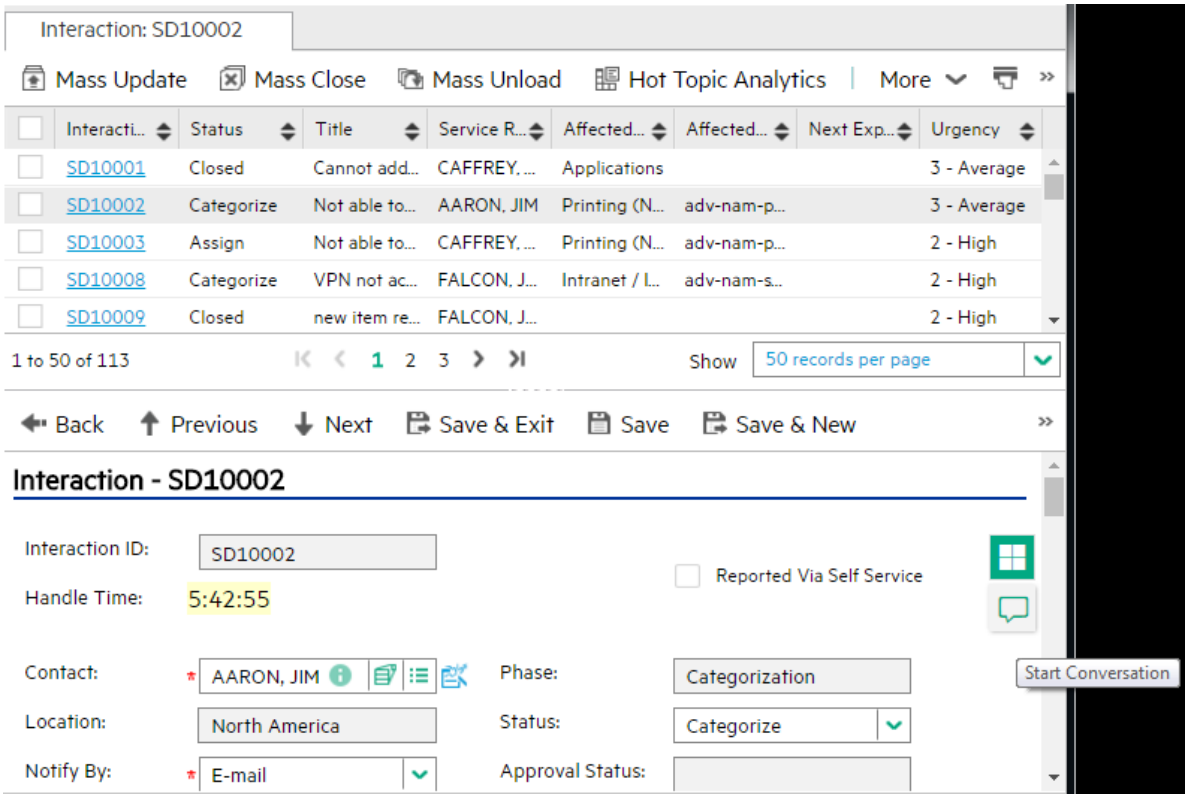
9. Verify that a **Chat Notification** button is displayed at the top-right corner of the screen. You are not able to click it because chat notifications are not available yet.



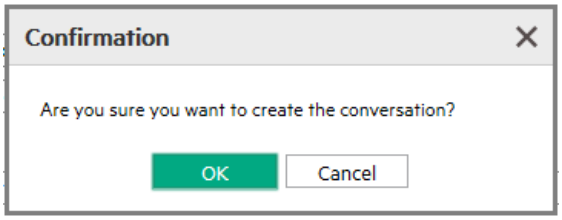
10. Click the **User Information** button to show your User Basic Information Card. Your presence status is now **Online**.



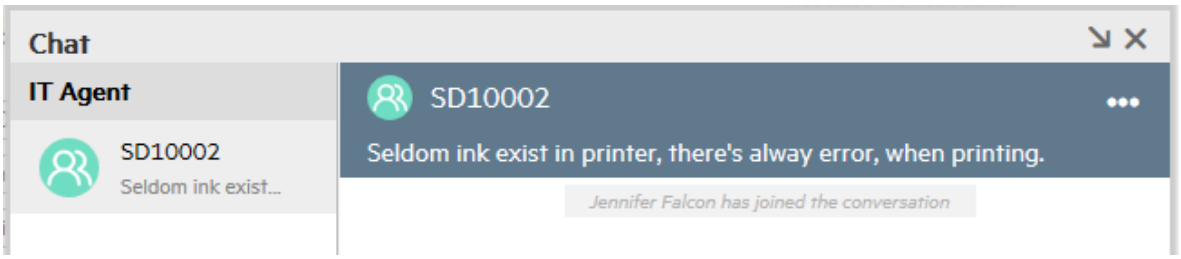
11. Open an interaction record. The **Start Conversation** button floats on the upper-right corner of the detailed view of this record.



12. Click the **Start Conversation** button, and then click **OK** in the confirmation dialog.



13. A conversation starts with the ID and title of the record displayed on the header of the conversation window.



Congratulations! You have successfully deployed Service Manager Collaboration!

Create SSL profile for two-way authentication between the chat service and the Service Manager server

Follow these steps:

1. Log on to Service Manager as a system administrator.
2. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.
3. Update the value in the Chat Service Domain and Port field to SSL link `https://<FQDN of Chat Service>:8448/`.
4. Save your changes.

Task 16: Select a portal for End User Chat

Service Manager supports the use of one of the following portals for End User Chat:

- Service Manager Service Portal (default): used for Service Manager Service Portal users
- ESS: used for Service Manager Employee Self-Service (ESS) client users

You need to select the right portal depending on which portal is being used for end users in your organization. To do this, follow these steps:

1. Go to **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
2. Select the **Active Integrations** tab.
3. In the **SM Portal** field, select the right portal from the drop-down list.
4. Specify the portal URL for your portal, as described in the following table.

Portal	Steps
ESS	In the **ESS URL** field, type the fully qualified ess.do URL to your web tier. For example: `https://sm950.training.com/webtier-9.50/ess.do`

Service Manager Service Portal	**Note:** You must configure both the standard Service Portal URL and the Service Portal support ticket URL in the System Information Record. Both URLs are used as predefined parameters for End User Chat.
	a. In the **Service Manager Service Portal URL** field, enter the following value:
	`https://<Service Manager Service Portal host name>:<port>`
	Where: <*Service Manager Service Portal host name*> represents the fully qualified domain name of the Service Manager Service Portal host, and <*port*> represents the launchpad port of Service Manager Service Portal. The default launch pad port is 9000.
	For example:
	`https://serviceportal.training.com:9000`
	b. In the **Service Manager Service Portal Support Ticket URL** field, enter the following value:
	`https://<Service Manager Service Portal host name>:<port>/support/requests/create`
	Where: <*Service Manager Service Portal host name*> represents the fully qualified domain name of the Service Manager Service Portal host, and <*port*> represents the support ticket port of Service Manager Service Portal. The default support ticket port is 9410.
	For example:
	`https://serviceportal.training.com:9410/support/requests/create`

5. Click **Save**.
6. Restart the chat service.

(Optional) Task 17: Integrate with Microsoft Skype for Business

HPE Service Manager Collaboration provides an out-of-the-box Skype plugin and a Skype agent to integrate with Microsoft Skype for Business. When you start a conversation in Service Manager Collaboration, the Skype plugin that is embedded in the Openfire server monitors all the messages. If a participant does not log on to the Openfire server, the Skype plugin will use the participant's email address as his/her Skype account and then send the message to the Skype server. If the user is available to chat, the Skype agent will launch a conversation with the right user, and then forward the message to him/her on Skype. After the Skype user replies, the Skype Agent will push this message back to the Skype plugin. Consequently, the Skype plugin will poll the in-coming Skype message and then forward it to all the other users in the Collaboration conversation.

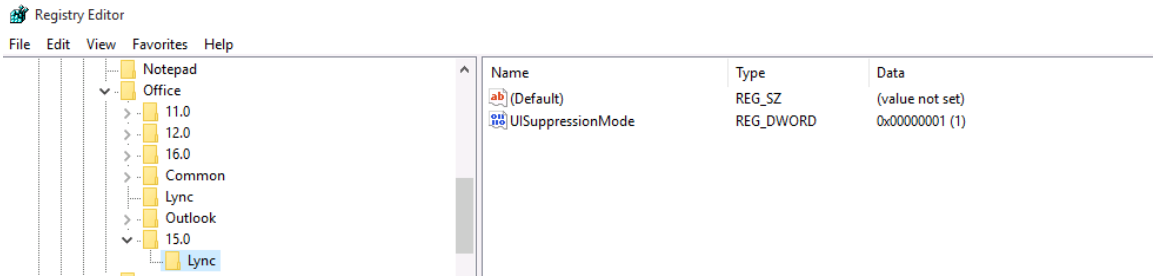
The following diagram illustrates a sample message exchange architecture between Service Manager Collaboration and the Skype server:

> **Note:**
> Lync users cannot start a conversation with Service Manager Collaboration. Instead, they can be invited to Collaboration conversations only.

In this task, you will integrate Service Manager Collaboration with Microsoft Skype for Business.

Follow these steps:

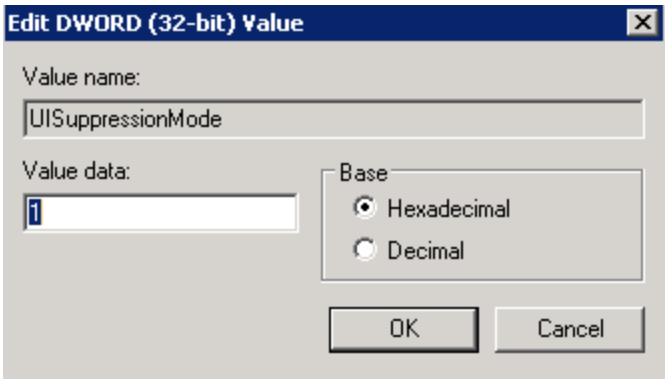
1. Download and install Microsoft .NET Framework 4.5 from Microsoft Download Center.
2. Download and install Microsoft Skype for Business 2016 from Microsoft Download Center. Service Manager Collaboration integrates with Microsoft Lync 2016 only.
3. Sign in to Skype by using an IT operator's Skype account. This account transfers the communication between the Openfire server and the Skype server, and hence must be effective and timely.
4. Click Microsoft Skype **Options** > **Personal**, and then select **None** from the **Personal information manager** drop-down menu. Save your changes and then sign out.
5. Create the new UISuppressionMode Windows Registry value.
   a. Open Windows Registry Editor, and then navigate to HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync.
   b. Right-click Lync, and then click **New** > **DWORD (32-bit) value** to create a new registry value.
   c. Set the new value name to UISuppressionMode, and then set the value data to 1.



d. Navigate to HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Lync.

e. Right-click Lync, and then click **New** > **DWORD (32-bit) value** to create a new registry value.

f. Set the new value name to UISuppressionMode, and then set the value data to 1.



g. Click **OK**, and then close the Windows Registry Editor.

6. Encrypt the Skype account and update the openfire.xml file.

a. Stop the Openfire server.

b. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\conf directory, and then open openfire.xml with a text editor.

c. Locate the `<lyncIntegration>` section.

d. Update the `<lyncIntegration>` section as follows:

```
<lyncIntegration>
<enabled>true</enabled>
<auth>
<!-- Put plain lync user name and password here, it will be automatically
encrypted
after server startup and encrypted="true" will be added to the userName and
password
elements. When you change your Lync userName or password, you must remove
encrypted="true" and replace the encrypted string with the new plain string.
-->
```

```
<userName><YourLyncAccountName></userName>
<password><YourLyncPassword></password>
</auth>
<startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

> **Note:** You need to enable Skype integration first, and then replace *<YourLyncAccountName>* and *<YourLyncPassword>* with the user account with which you signed in to Skype in step 3.

> **Caution:**
> - When the IT operator's Skype password is changed, the <*YourLyncPassword*> value in openfire.xml must be changed accordingly.
> - You must not sign out the IT operator's Skype account which transfers the communication between the Openfire server and the Skype server. Otherwise, Service Manager Collaboration does not work.

e. Save and close this file.

f. Start the Openfire server.

See the following screenshot for an example of the encrypted `<lyncIntegration>` section in openfire.xml:

```
<lyncIntegration>
  <enabled>true</enabled>
  <auth>
    <!-- Put plain lync user name and password here, it will be automatically encrypted
         after server startup and encrypted="true" will be added to the userName and password
         elements. When you change your Lync userName or password, you must remove encrypted="true" and
         replace the encrypted string with the new plain string.
      -->
    <userName encrypted="true">B454FAEED3A2E2118C77759EC9E7F4EFA56E051ADB0AB4451A8F8EB2A2357125</userName>
    <password encrypted="true">BA9F849640CAA40D4A69AE8ABCDBAA16</password>
  </auth>
  <startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

7. Enable Service Manager Collaboration to communicate with the Skype server.

a. Log on to Service Manager as a system administrator.

b. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.

c. Select the **Enable ESS Skype User** check box so that the Service Manager Skype users can join Collaboration conversations by using Skype.

Now you can communicate with the Skype users in a Service Manager Collaboration conversation.

> **Caution:** To integrate with Microsoft Skype for Business, follow these steps to specify the log on

account for the Openfire service before starting it as a standard Windows service:

1. Right-click the Openfire service in the Windows Services window, and then select **Properties**.
2. Click the **Log On** tab.
3. Select **This account**, and then specify the same IT operator's Skype account used in step 3.
4. Click **Apply** and **OK**.

(Optional) Task 18: Migrate data from EC

In this task, you will migrate existing Enterprise Collaboration (EC) data to Service Manager Collaboration by using a migration tool.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\smcmigration directory, and then double-click startup.bat to start the Service Manager Migration Tool.
2. Select a language, and then click **Start**.
3. Read through the welcome screen, and then click **Next**.
4. Select the database type of your EC server, specify the server name, database name, user name, and password of your EC database, and then click **Next**.

   Note: If you are working with an Oracle database, download the JDBC driver (for example, ojdbc6.jar) from here and then copy this file to the <sm9.xx.00xx-ChatServer>\smcmigration\lib directory.
5. Select the database type of your Service Manager server, specify the server name, database name, user name, and password of your Service Manager database, and then click **Migrate**.

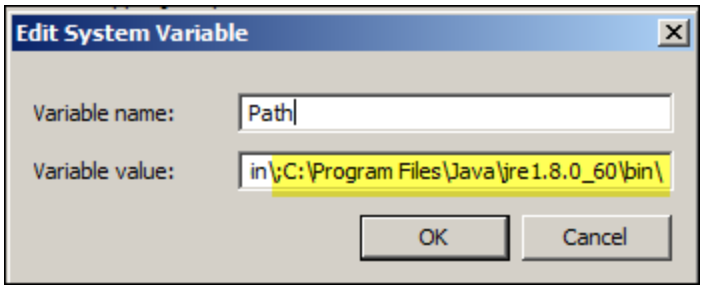
   The Service Manager Migration Tool displays a status bar that the visualizes the data migration progress.
6. When the data migration progress is completed, click **Finish** to quit the tool.

(Optional) Task 19: Configure Tomcat for HTTPS support

This task is required only if SSL has been configured between Apache and Tomcat. If you are using `mod_jk` for communications between Apache and Tomcat (as described in *Task 8: Deploy the Apache HTTP server*) or the proxy balancer, you do not need to perform the steps in this task.

Follow these steps:

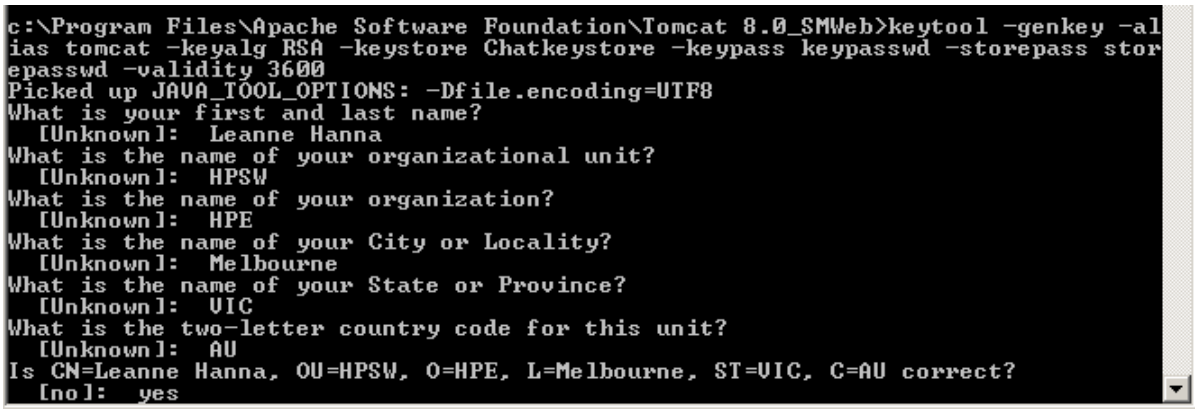
1. Navigate to the C:\Program Files\Java\jre1.8.0_xx\bin directory, and then make sure that keytool.exe is stored in this directory.
2. Copy the directory path (C:\Program Files\Java\jre1.8.0_xx\bin) to your clipboard or paste it to Notepad, as you will need it in the next steps .
3. Add this path to the Path environment variable.



4. Click **OK** repeatedly to exit.
5. Open a DOS command prompt and change the directory to C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb.
6. Run the following command to generate the keystore file and set passwords for this keystore file by using the Java keytool:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore Chatkeystore -keypass
    keypasswd -storepass storepasswd -validity 3600
```

7. The system prompts a series of question, including your first and last name, organizational unit, organization, city, state, and country code. Provide answers to these information and then press Enter, respectively.
8. Finally you are presented with the values for the keytool. Type `yes` and then press Enter.

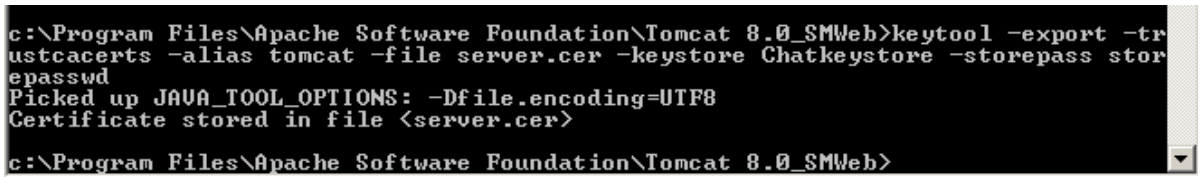


This command line returns.

9. Run the following command to generate the certificate file for the keystore:

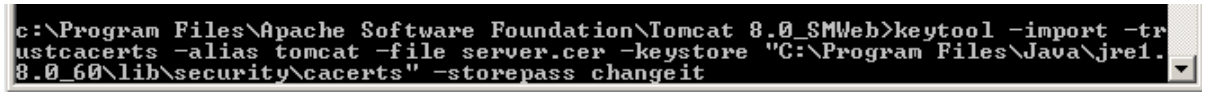
   ```
   keytool -export -trustcacerts -alias tomcat -file server.cer -keystore
   Chatkeystore -storepass storepasswd
   ```

10. The server.cer certificate file is generated.



11. Run the following command to import the self-signed certificate to the Java security folder:

    ```
    keytool -import -trustcacerts -alias tomcat -file server.cer -keystore
    "C:\Program Files\Java\jre1.8.0_60\lib\security\cacerts" -storepass changeit
    ```



    The system starts to the certificate and prompts you to answer a number of questions.

    > **Note:** The certificate password for cacerts is changeit.

12. The system asks if you trust this certificate. Type `yes` and then press Enter:

```
c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -import -tr
ustcacerts -alias tomcat -file server.cer -keystore "C:\Program Files\Java\jre1.
8.0_60\lib\security\cacerts" -storepass changeit
Picked up JAVA_TOOL_OPTIONS: -Dfile.encoding=UTF8
Owner: CN=Leanne Hanna, OU=HPSW, O=HPE, L=Melbourne, ST=VIC, C=AU
Issuer: CN=Leanne Hanna, OU=HPSW, O=HPE, L=Melbourne, ST=VIC, C=AU
Serial number: 52305d8c
Valid from: Wed Oct 21 08:55:28 AEDT 2015 until: Fri Aug 29 07:55:28 AEST 2025
Certificate fingerprints:
         MD5:  EF:89:72:2E:76:44:9C:60:0F:1A:60:BE:EB:18:F5:43
         SHA1: 1F:1C:09:3E:1F:67:17:09:6C:55:D5:C2:01:EA:B7:0D:39:D1:BD:8E
         SHA256: 6F:3C:AE:C0:DC:5B:4E:AE:68:31:1C:B3:5C:A6:06:7C:F9:65:C8:97:EC:
DB:98:7E:B7:EF:94:C6:00:19:98:AE
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 00 F2 CF 80 A5 C5 E5 6E   05 5B DE BB 5B 02 B2 13  .......n.[..[...
0010: 67 9C 5D 65                                        g.]e
]
]

Trust this certificate? [no]:  yes
```

The certificate is added to the keystore:

```
Trust this certificate? [no]:  yes
Certificate was added to keystore

c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>_
```

13. Close the DOS command window.
14. Navigate to the C:\Program Files\Java\jre1.8.0_xx\lib\security directory to verify that the cacerts file is generated.
15. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb directory to verify that the Chatkeystore and server.cer files are generated.
16. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\conf directory.
17. Copy the server.xml file and save it as server_OOB.xml.
18. Open the server.xml file with a text editor.
19. Browse to the bottom of the file and insert a few blank lines above `</Host>`.

```
134             Note: The pattern used is equivalent to using pattern="common" -->
135           <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
136                  prefix="localhost_access_log" suffix=".txt"
137                  pattern="%h %l %u %t &quot;%r&quot; %s %b" />
138
139
140
141       </Host>
142     </Engine>
143   </Service>
```

20. Insert the following codes above `</Host>`:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="Chatkeystore"
keystorePass="storepasswd"/>
```

```
137                  pattern="%h %l %u %t &quot;%r&quot; %s %b" />
138
139           <Connector protocol="org.apache.coyote.http11.Http11Protocol"
140           port="8443" minSpareThreads="5" maxSpareThreads="75"
141           enableLookups="true" disableUploadTimeout="true"
142           acceptCount="100" maxThreads="200"
143           scheme="https" secure="true" SSLEnabled="true"
144           clientAuth="false" sslProtocol="TLS"
145           keystoreFile="Chatkeystore"
146           keystorePass="storepasswd"/>
147
148
149       </Host>
150     </Engine>
151   </Service>
```

21. Save your changes and close the server.xml file.

Troubleshoot the Service Manager Collaboration deployment

This section provides information that can assist you in troubleshooting issues that are associated with Service Manager Collaboration.

Troubleshooting - Failed to start the chat server

Description

Failed to restart the Openfire chat server.

Root cause

Some related processes still exist.

Solution

Check the openfire.exe process, the LyncAgent.exe process, and the Lync.exe process in Windows Task Manager when restarting the Openfire chat server. If these processes still exist after the Openfire service is stopped, you must end these processes manually before starting the Openfire chat server.

> **Note:**
> The LyncAgent.exe process and the Lync.exe process exist only when you have integrated Collaboration with Microsoft Skype for Business.

Troubleshooting - Failed to connect to the Collaboration server

Description

When you log on to the Service Manager web client by using https, the system displays the following error:

Root cause

The Openfire service is not started, or Service Manager Collaboration lost connection to the Openfire server, or Service Manager Collaboration is not properly configured.

Solution

Perform the following tasks:

Task 1. Make sure that the Openfire Windows service is started

Go to **Control Panel** to check that the Openfire service is started.

Task 2. Try to reconnect to the Openfire server

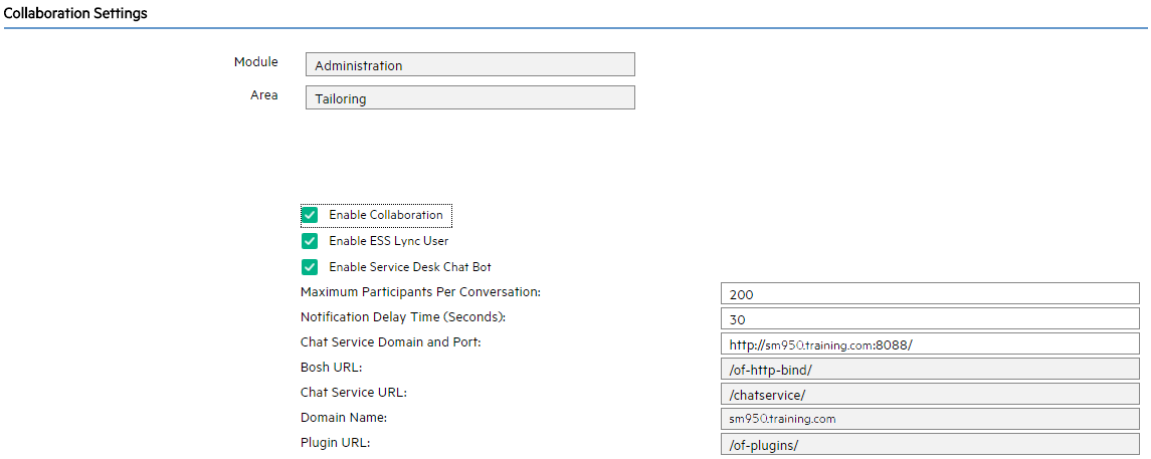
Click the **Notifications** button to try to reconnect to the Openfire server.

Task 3. Verify the Service Manager Collaboration configurations

Follow these steps to verify the Service Manager Collaboration configurations:

1. Log on to Service Manager as a system administrator.
2. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration**.
3. Ensure the following fields are configured correctly, as described in the following table.

Field	Value
Chat Service Domain and Port	http://sm950.training.com:8088
Bosh URL	/of-http-bind/
Chat Service URL	/chatservice/
Domain Name	Set it to the Openfire Domain that you set up in *Task 5: Deploy the chat server*. In our example steps, it is sm950.training.com.
Plugin URL	/of-plugins/



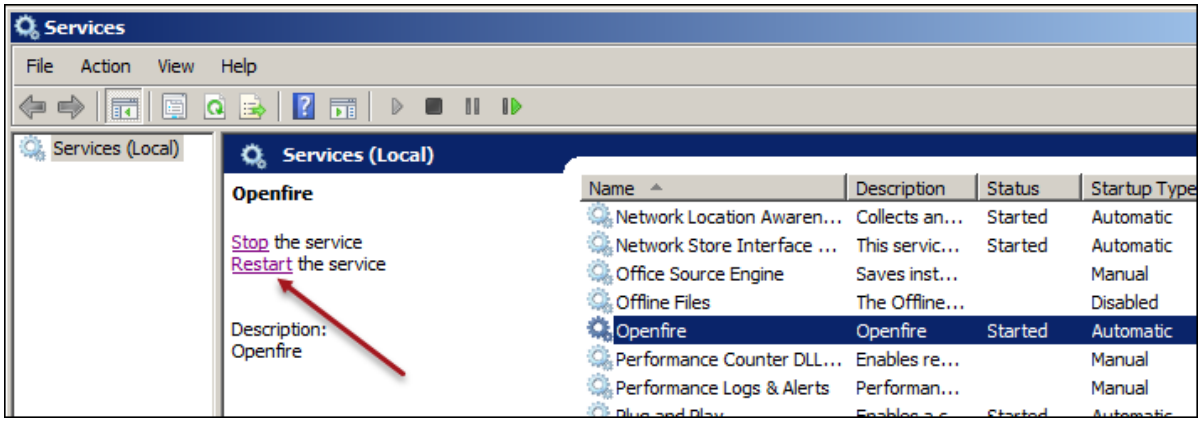
4. Log out from Service Manager.
5. To verify your Openfire configurations, go to your web browser and access https://localhost:9091. The Openfire Administration Console page opens.

6. Log in with username `admin` and password `SM950training`. The system displays the Server Information page.
7. On this Server Information page, verify the Server Name (domain name) of the Openfire server.
8. To update the server name, go to the bottom of this page and click **Edit Properties**.
9. Edit the Server Name as appropriate.

   > **Note:**
   > The **Admin Console Port** field is empty on this page. Set the value to 9090 if you want to use the default value or to the value you choose.

10. Click **Save Properties**.
11. Ensure you receive a message that indicates the server properties were successfully updated.

12. Restart the Openfire service in Windows services.



13. Log on to Service Manager again to check whether Collaboration works. If it does not, proceed to the next task.

Task 4. Reinstall Openfire

You may need to reinstall Openfire if you have checked all your settings but still see the following error message:

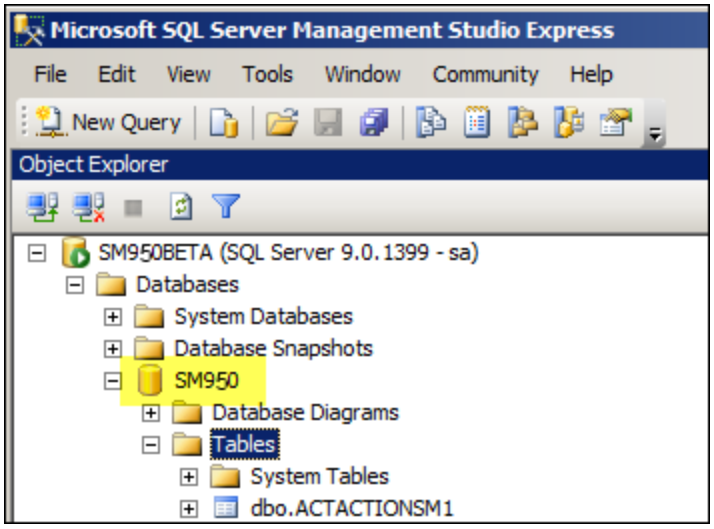
Follow these steps to reinstall Openfire:

1. Log out from Service Manager.
2. Stop the Windows service named **Openfire**.
3. Open a DOS command prompt and change the directory to C:\Program Files (x86)\HPE\Service Manager 9.50\ChatServer\bin.
4. Run the **openfire-service /uninstall** command to uninstall the Windows service. The following messages are displayed:

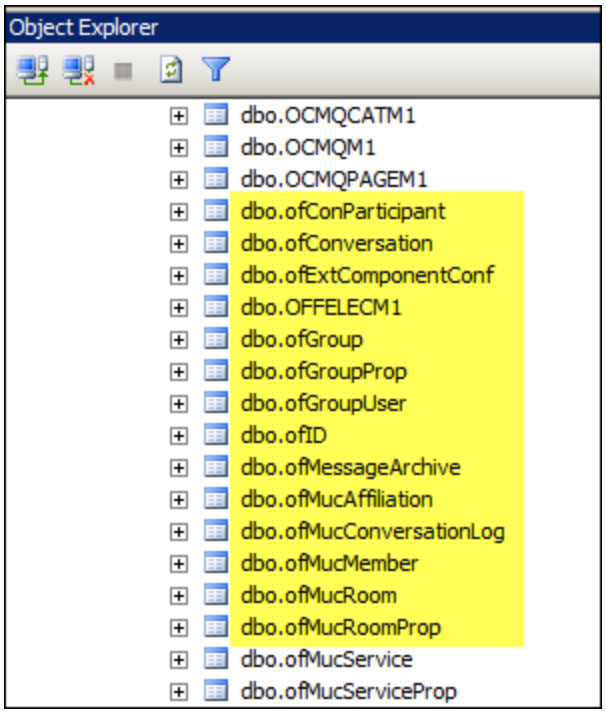
   ```
   Service is already stopped.

   Uninstalled service 'Openfire'.
   ```

5. Navigate to the C:\Program Files(x86)\HPE\Service Manager 9.50 directory, and then remove the ChatServer directory.
6. Log on to your Service Manager database and list the tables.

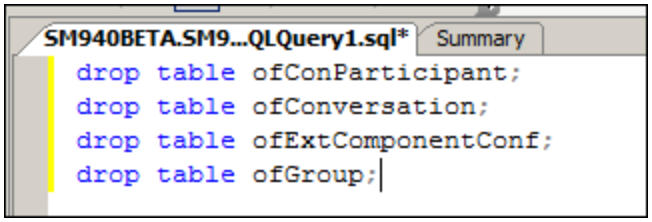


7. Locate the tables prefixed with '**of**' in the list.



   All tables prefixed with lowercase '**of**' need to be dropped.

8. Drop the tables until all tables prefixed with '**of**' are removed.



9. Reinstall the Openfire chat server. For detailed instructions, see *Task 5: Deploy the chat server*.
10. Configure LW-SSO for the chat server. For details, see *Task 13: Configure LW-SSO for the chat server*.
11. Log on to Service Manager again to check whether Collaboration works.

Set up a replicated reporting database

The Service Manager Reporting module provides reports and dashboards with active operational data to achieve faster analysis and improved time to resolution. Since Reporting consumes additional system resources (memory and CPU), Service Manager enables you to optionally use a replicated database for reporting, which helps preserve the performance of your production database.

If you want to use a replicated database for the Service Manager Reports functionality, perform the following tasks.

Task 1. Prepare a replicated database

1. Prepare a database with the same database type and version as your production database. Follow the same instructions for your database type in the *Prepare an RDBMS to support Service Manager* section of this document.

   > **Note:** The two databases can reside on the same server or on different servers.

2. Perform periodic database synchronization between your production database and replicated database by using the standard database synchronization mechanism. For detailed instructions, refer to your specific database documentation.

Task 2. Configure a database connection between the Service Manager server and replicated database

Service Manager connects to the database through your RDBMS client (for example, Windows ODBC DSN defined for SQL Server). To set up the connection between your Service Manager application server and replicated database, know the name of the database and the login ID and password required to connect to the database server that you created above.

Configure the connection on the Service Manager Server host. In a horizontally scaled environment, you must do so on each of the Service Manager Server hosts. For example, if you use SQL Server, in addition to the ODBC Driver data source you configured for the production database, configure another ODBC Driver data source as a System DSN for the replicated database.

Task 3. Update the Service Manager server configuration file (sm.ini)

To do this, follow these steps:

1. In the sm.ini file, add the following parameters (the parameter values are for demonstration purposes only):

   > **Caution:** The last four lines must be inserted as a group. Do not insert any other lines

between them.

For SQL Server:

```
[sqlserver]
sqldb:940pd
sqllogin:pdadmin/passw0rd
[sqlserver_replicate]
sqldb:940rp
sqllogin:rpadmin/passw0rd
dashboardonreplicatedb
```

For Oracle:

```
[oracle]
sqldb:940pd
sqllogin:pdadmin/passw0rd
[oracle_replicate]
sqldb:940rp
sqllogin:rpadmin/passw0rd
dashboardonreplicatedb
```

For DB2:

```
[db2universal]
sqldb:940pd
sqllogin:pdadmin/passw0rd
[db2universal_replicate]
sqldb:940rp
sqllogin:rpadmin/passw0rd
dashboardonreplicatedb
```

Parameter	Description
[sqlserver]	This parameter creates a section header in the initialization file for information about an Microsoft™ SQL Server database. You only need to provide this parameter if you have set sqldictionary and are using a SQL Server database.
[sqlserver_replicate]	This parameter creates a section header in the initialization file for information about a replicated Microsoft™ SQL Server database. You only need to provide this parameter if you have created a replicated SQL Server reporting database.
[oracle]	This parameter creates a section header in the initialization file for information about an Oracle™ database. You only need to provide this parameter if you have set sqldictionary and are using an Oracle database.

Parameter	Description
[oracle_replicate]	This parameter creates a section header in the initialization file for information about a replicated Oracle™ database. You only need to provide this parameter if you have created a replicated Oracle reporting database.
sqllogin	This parameter defines the user name and password that HPE Service Manager uses to authenticate connections to the RDBMS. You must use a slash character to separate the user name and password. If you omit this parameter, then the server attempts to authenticate the connection using the user name and password of the user who started the HPE Service Manager Server, however this feature requires the HPE Service Manager Server and the RDBMS server to use the same operating system. If the HPE Service Manager Server and the RDBMS server use different operating systems, then you must specify a sqllogin value.
dashboardonreplicatedb	This parameter creates a section footer in the initialization file for information about a replicated reporting database.

2. (Optional) Add the following parameters to the sm.ini file of each Service Manager server:

```
dashboardquerycache_enable:1
dashboardquerycache_dbtime:100
dashboardquerycache_expire:10
```

Parameter	Description
dashboardquerycache_enable	Enables Service Manager to cache report query results in the database.
dashboardquerycache_dbtime	Defines a threshold for report query execution time that will trigger query caching (default: 100 milliseconds). Only when a query's execution time reaches or exceeds this threshold, the query results are cached in the database.
dashboardquerycache_expire	Defines how long cached report query results will be expired in the database (default: 10 minutes). When the specified time is reached, the cached query results are expired and will be refreshed at a later time.

> **Note:** The query cache resides on the production database. It stores the results of queries against both the production database and replicated database.

3. Save the configuration file, and restart the Service Manager server.

In a horizontally scaled system, you need to repeat this task on each of the Service Manager server.

Task 4. Configure the Reporting module to use the replicated database

To do this, follow these steps:

1. Log in to Service Manager as a system administrator.
2. Go to **Reporting** > **Administration** > **Report Settings**.
3. Select the **Use Replicated Database by default when users create reports** option.

   If this option is selected, the **Use Replicated Database** setting is enabled by default in each new report that users create. However, users can disable the **Use Replicated Database** setting in an individual report.
4. Select the **Use Production Database when Replicated Database is disabled** option.

   Select this option so that Service Manager can still use the production database to generate reports when the replicated database is not enabled or the database connection parameters are not defined correctly in the server configuration file (sm.ini).
5. Click **Save**.

Set up legacy integrations

A legacy integration is any integration that depends on SCCL32 or the Service Manager ODBC driver. These products include Connect-It and Crystal Reports. Using legacy integrations with the Service Manager Server requires you to set up a read-only legacy ServiceCenter listener.

Follow these instructions to set up legacy integrations.

Set up a legacy listener

The out-of-box server sc.ini file is configured to connect to the sample database. To connect to another RDBMS, edit the parameters in the sc.ini file.

To set up a legacy listener on a Window or UNIX server:

1. Edit the legacy sc.ini file:
   a. Log in to the Service Manager server with an administrator account.
   b. Open a command prompt and navigate to the RUN folder in the LegacyIntegration folder in the Service Manager Server directory. For example, <Service Manager installation path>\Server\LegacyIntegration\RUN.
   c. Open sc.ini with a text editor.
   d. To connect to your Service Manager RDBMS, add the database connectivity settings. Make sure that these settings match the settings that you used when you set up your RDBMS connection.

      If the legacy listener will connect to a case-insensitive Oracle database, add the parameter **sql_oracle_binary_ci** to the sc.ini file.

e. (For Windows) Add the following parameter on its own line: **ntservice:<*Service Manager Legacy Read-only Service Name*>**.

f. Save and close the sc.ini file.

2. (For Windows) Install the Windows service:

   a. Log on to the Windows server as a user with local administrator privileges.

   b. Open a command prompt and navigate to <Service Manager installation path>\Server\LegacyIntegration\RUN.

   c. Type **scservic -install**.

      This command creates a Windows service with the name specified by the ntservice parameter in the sc.ini file.

3. (For Unix) Run the `scstart` script in the <Service Manager installation path>\Server\LegacyIntegration\RUN folder.

Install the ODBC driver

To install the Service Manager ODBC driver, follow these steps:

1. Log on to the Windows server as a user with local administrator privileges.
2. Extract the SM9.50-2.zip file into the appropriate drive of the server.
3. Navigate to the \Reporting directory.
4. Run the **ServiceManager ODBC Driver-9.50.exe** file.
5. Click **Next** to read and accept the licensing agreement. The **Next** button becomes active.
6. Click **Next** to select your installation folder. The default installation location is C:\Program Files (x86)\HPE\Service Manager 9.50\ODBC. Click **Choose** to select a different location.
7. Click **Next** to prepare the installation process.
8. Click **Install** to begin copying the installation files. A dialog box opens when the installation is complete.
9. Click **Done**.

Configure the ODBC driver

The default installation sets up the ODBC DSN to connect to the default legacy listener on the local

host. Configure the legacy ODBC driver to connect to the legacy read-only listener:

1. From the Windows **Start** menu, click **Control Panel** > **Administrative Tools** > **Data Source (ODBC)**.
2. Open the System DSN tab.
3. Select **sc_report_odbc** and click **Configure**.
4. Configure the ODBC driver by using the following parameters:
   - Data Source Name: sc_report_odbc
   - Server: The host where the legacy ServiceCenter listener is running. The default setting is localhost.
   - Port: The port the legacy server is set to use. The default setting is 12690.

Start the legacy listener

For a UNIX server, perform the following steps:

1. Navigate to <Service Manager installation path>\Server\legacyintegration\RUN.
2. Run the scstart script.

For a Windows server, perform the following steps:

1. From the Windows **Start** menu, select **Control Panel** > **Administrative Tools** > **Services**. select the service that you installed when you set up the legacy listener, and then click **Start**.

   You can start the listener as an application rather than as a service. To do so, go to the <Service Manager installation path>\Server\ LegacyIntegration\RUN directory and run the following command using the Windows command prompt: `scenter -listener:<port number> -RPCReadOnly`.
2. Verify that the ODBC driver can connect. To test the connection, use any ODBC query tool. For example, in Excel, open: **Data** > **Get External Data** > **New Database Query**. Select the ServiceCenter ODBC driver as your data source. If it connects, it displays the Service Manager tables.

RPC read-only mode parameter

You must start a legacy listener with the RPC read-only mode parameter. This parameter allows a Service Manager server to connect to a Service Manager database without interfering with the Service

Manager server (it does not create a system lock).

The RPC read-only parameter prevents Service Manager clients (Windows, web tier, and web services) from connecting to the Service Manager server. The only connections the ServiceCenter 6.2 RPCReadOnlyMode listener accepts are connections from the Service Manager ODBC driver or Connect-It.

- If you use Connect-It 3.81 or later, you must provide the host name and port for both the Service Manager and ServiceCenter 6.2 ReadOnly listener. Connect-It requires this information to use the RPC functions for reading the event services and other Service Manager information. The connector writes data to Service Manager through web services.
- You can also use the legacy listener to run reports or SQL queries against your Service Manager data without affecting the Service Manager performance.

Install Crystal Reports for use with Service Manager

You can use Crystal Reports to view, update, and develop new reports with Service Manager.

Follow these steps to install Crystal Reports 2013 SP3 for use with Service Manager:

1. If Crystal Reports 2008 with or without SP1 or SP3 has been installed before, use **Uninstall or change a program** from the Windows Control Panel to uninstall Crystal Reports 2008 with the service packs and all associated Language Packs.
2. Make sure that the Service Manager ODBC Driver is installed.
3. Log in to the Windows server as a user with local administrator privileges.
4. Extract the SM9.50-2.zip file into the appropriate drive of the server.
5. Navigate to the \Reporting\CrystalReports directory.
6. Right-click **SilentInstall.bat** and then select **Run as administrator**.

   The installation wizard starts.
7. Restart your computer when the installation is complete. You must restart your computer before opening Crystal Reports 2013.
8. Start the legacy listener.

Download reports for Service Manager

Service Manager9.50 installation file SM9.50-2.zip file comes with out-of-box reports that you can run using Crystal Reports. Using these reports requires the Service Manager ODBC driver and requires that the legacy listener is started.

1. Make sure that the Service Manager ODBC driver is installed.
2. Log in to the Windows server as a user with local administrator privileges.
3. Extract the SM9.50-2.zip file into the appropriate drive of the server.
4. Navigate to the \Reporting\OperationalReports directory.
5. Copy the desired reports to your local directory.

See the *Service Manager Operational Reports Guide* for more information.

Install and configure the HPE Identity Manager service

Service Manager (SM) leverages HPE Identity Manager (IdM) to support Single Sign-On (SSO) using SAML 2.0. To set up SAML SSO for Service Manager, you need to deploy the IdM service and create a trust relationship with a third-party identity provider (IdP). In the SAML SSO process, the IdM service acts as a service provider (SP) to the IdP.

- For SM SAML SSO, you can use only the IdM service package released as a web archive (WAR) file, which is version 1.10.2. Currently, you must not use the IdM service bundled in Service Manager Service Portal, which is not supported for SAML SSO. For more information about how to set up SAML SSO for Service Manager, see the "SAML Single Sign-On" section in the Help Center.
- Currently, only Microsoft ADFS 2.0 or 3.0 is supported as an identity provider (IdP) for IdM.

Prerequisite

You must have a third-party identity provider (that is, ADFS 2.0 or 3.0) installed in your system.

To deploy a single IdM instance, complete the following tasks.

Task 1. Deploy a web application server for the IdM service

You can deploy the IdM service on Tomcat 7.x or 8.x.

Note: The following steps use Tomcat as an example. Version 8.x is recommended.

To do this, follow these steps:

1. Install JDK 1.8 or later .
2. Install Tomcat 8.x.

   Caution: The Tomcat installation path must not contain any white spaces.
3. If using Tomcat 8.5 or later, perform the following steps:
   a. Open the <Tomcat>/conf/context.xml file in a text editor.
   b. Insert the following line inside the <Context> tag pair:

      ```
      <CookieProcessor
      ```

```
    className="org.apache.tomcat.util.http.LegacyCookieProcessor"/>
```

c. Save the file.

Task 2 Configure SSL in the IdM web application server

The IdM service requires the use of SSL connections. Once you have completed the deployment of the IdM web application server (Tomcat), you need to configure SSL for it.

To configure SSL for Tomcat, follow these steps:

1. Run the following keytool command to create a keystore file:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keystore tomcat.keystore
   ```

   Follow the screen prompts to enter required information.

   > **Note:** When asked for your first and last names, enter the fully qualified domain name (FQDN) of the Tomcat server. For example: myhost.mycompany.net.

   The following is an example.

   ```
   C:\Tomcat\tomcat_9443>keytool -genkey -alias tomcat -keyalg RSA -keystore
   tomcat.keystore
   Enter keystore password:

   Re-enter new password:

   What is your first and last name?

     [Unknown]:  myhost.mycompany.net
   What is the name of your organizational unit?

   [Unknown]:  software

   What is the name of your organization?

    [Unknown]:  hpe

   What is the name of your City or Locality?

     [Unknown]:  shanghai

   What is the name of your State or Province?

     [Unknown]:  shanghai

   What is the two-letter country code for this unit?
   ```

```
  [Unknown]:  CN

Is CN=myhost.mycompany.net, OU=software, O=hpe, L=shanghai, ST=shanghai, C=CN
correct?

  [no]:  yes

Enter key password for <tomcat>

        (RETURN if same as keystore password):

Re-enter new password:
```

2. Run the following command to export a certificate from the keystore:

   ```
   keytool -keystore tomcat.keystore -export -alias tomcat -file tomcat.cer
   ```

3. Run the following command to import the certificate into JDK:

   ```
   keytool -import -alias idm -file tomcat.cer -keystore  cacerts
   ```

   Follow the screen prompts to enter required information. The following is an example.

   > **Note:** The default keystore password is **changeit**.

   ```
   C:\Program Files\Java\jdk1.8.0_91\jre\lib\security>keytool -import -alias idm -
   file tomcat.cer -keystore  cacerts

   Enter keystore password:

   Owner: CN=myhost.mycompany.net, OU=software, O=hpe, L=shanghai, ST=shanghai,
   C=CN

   Issuer: CN=myhost.mycompany.net, OU=software, O=hpe, L=shanghai, ST=shanghai,
   C=CN

   Serial number: 5acc6d54

   Valid from: Fri Jun 03 10:00:26 CST 2016 until: Thu Sep 01 10:00:26 CST 2016

   Certificate fingerprints:

            MD5:  52:9F:9E:57:63:11:26:DB:0A:D4:99:0D:44:1B:A8:65

            SHA1: 47:8E:26:C2:CA:0E:C2:B0:3C:D8:54:4F:70:93:44:F5:D6:6E:D6:1D

            SHA256:
   5C:B0:98:10:7D:13:BE:D2:24:2C:C0:EF:F0:C5:F1:7F:87:6C:E7:0B:FA:22:4C:94:DE:46:E
   F:6C:0E:55:61:9B
   ```

```
         Signature algorithm name: SHA256withRSA

         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 9D DB 0D 2A 12 B9 41 6B   3D C7 66 86 3B 63 9E 98  ...*..Ak=.f.;c..

0010: 02 D7 38 CE                                        ..8.

]

]

Trust this certificate? [no]:  yes

Certificate was added to keystore
```

4. Configure the https port and keystore in the server.xml file in the <Tomcat>/conf folder:

```
<Connector port="9443" protocol="org.apache.coyote.http11.Http11NioProtocol"

   maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

       clientAuth="false" sslProtocol="TLS"
keystoreFile="/conf/tomcat.keystore" keystorePass="!qaz2wsx3edc"

         truststoreFile="/conf/tomcat.keystore" storePass="!qaz2wsx3edc" />
```

> **Caution:** Be sure to enter the correct path of the tomcat.keytore file.

(Optional) Task 3. Create an IdM client trust store

This is an optional task. Perform this task only if you want the IdM client (SM Web Tier, SRC, or Mobility Client) to verify the IdM server certificate. If you want the IdM clients to perform this verification, you need to do the following:

1. Create an IdM client trust store.
2. Copy the trust store file to the IdM client (SM Web Tier, SRC, and Mobility Client).

3. On the IdM client side, set the **idm.ssl.trustAll** parameter to **false** (default) and specify the trust store file and password for the IdM client. For details, see the *SAML Single Sign-On setup* section in the Service Manager Help Center.

In the previous task ("Task 2 Configure SSL in the IdM web application server"), you have already created a certificate file (tomcat.cer) and keystore file (tomcat.keystore) for the web application server. Now, you need to create a truststore using these two files.

To create an IdM client trust store, follow these steps:

1. Generate a trustStore.keystore file, by running the following command:

   ```
   keytool -genkey -alias tomcat1 -keyalg RSA -keysize 1024 -keypass tomcat1 -validity 365 -keystore trustStore.keystore -storepass tomcat1
   ```

2. Import the IdM public key to the trustStore.keystore file, by running the command below:

   ```
   keytool -import -alias tomcat -file tomcat.cer -keystore trustStore.keystore -storepass tomcat1
   ```

> **Note:** Now, the trust store file is generated. The file name is `trustStore.keystore`, and its password is `tomcat1`.

Task 4. Deploy the IdM service and configure SAML SSO

To do this, follow these steps:

1. Copy the idm-service-1.10.2.war file from the SM9.50-2.zip file to the <Tomcat>/webapps folder.
2. Deploy the .war file.
3. Update the IdM service configuration base for SP-initiated web SSO.

   Step 1. Configure SP-Initiated SSO: Redirect/POST Binding

   a. In the <idm-service>/WEB-INF/web.xml file, uncomment the following line:

      ```
      /WEB-INF/spring/applicationContext-saml.xml
      ```

      > **Note:** The applicationContext-saml.xml file includes Spring beans for SAML.

   b. In the <idm-service>/WEB-INF/spring/applicationContext-security.xml file, enable SAML Web SSO with HP SSO.

      By default, the SAML Web SSO with HP SSO section is commented out. Remove the comment tags highlighted below to enable the feature.

```
<!-- START SAML Web SSO with HP SSO -->
    <!--
       ...
       ...
       ...
    -->
<!-- END SAML Web SSO with HP SSO -->
```

> **Note:** SAML Web SSO without HP SSO authenticates the user and provides user access to protected resources in one application; SAML Web SSO with HP SSO writes the HPE SSO cookie after the user is authenticated, and therefore provides single sign-on to other applications. HP SSO provides single sign-on capability across HPE software products. To be compatible with LW-SSO, you must enable SAML Web SSO with HP SSO. This means when SAML is enabled in SM and LW-SSO is enabled in another application, users can access SM without login, and vise versa.

c. Update the <idm-service>/WEB-INF/spring/applicationContext-security.xml file.

   i. Open the file with a text editor.

   ii. Search for "START HP SSO Configuration". This section is commented out by default.

   iii. Uncomment this section, except the normal HPSSO login and logout filters, as shown below.

```
<!-- START HP SSO Configuration -->
    <!--
    <security:http pattern="/idm/v0/login" use-expressions="true" auto-
config="false">
        <security:csrf disabled="true" />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST" />
        <security:custom-filter ref="hpssoProvidedFilter" before="PRE_
AUTH_FILTER" />
        <security:custom-filter ref="hpssoIntegrationFilter"
after="PRE_AUTH_FILTER" />
        <security:custom-filter ref="noPromptFilter" before="FORM_
LOGIN_FILTER" />
        <security:http-basic />
    </security:http>

    <security:http pattern="/idm/v0/logout" use-expressions="true"
auto-config="false">
        <security:csrf disabled="true" />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST" />
        <security:custom-filter ref="hpssoProvidedFilter" before="PRE_
```

```
AUTH_FILTER" />
        <security:custom-filter ref="hpssoIntegrationFilter"
after="PRE_AUTH_FILTER" />
        <security:http-basic />
    </security:http>
       -->
       ...
       ...
       ...
       </bean>
<!-- END HP SSO Configuration -->
```

d. Configure HP SSO.

   i. Open the <idm-service>/WEB-INF/web.xml file with a text editor.

   ii. Search for "START HP SSO Configuration". This section is commented out by default.

   iii. Uncomment this section by removing the comment tags.

   iv. Specify the location of the HP SSO configuration file as "/WEB-INF/hpssoConfig.xml".

```
<!-- START HP SSO Configuration -->
    <listener>
        <listener-
class>com.hp.ccue.identity.hpssoImpl.HpSsoContextListener</listener-
class>
    </listener>

    <context-param>
        <param-
name>com.hp.sw.bto.ast.security.lwsso.conf.fileLocation</param-name>
        <param-value>/WEB-INF/hpssoConfig.xml</param-value>
    </context-param>
<!-- END HP SSO Configuration -->
```

   v. In the <idm-service>\WEB-INF\spring\applicationContext-v0.xml file, uncomment the tokenWriter property setting in the HP SSO Configuration section, as shown below.

```
<!--Authentication API -->
    <bean id="authenticationApiController"
class="com.hp.ccue.identity.web.api.AuthenticationController">
        <property name="tokenService" ref="tokenService"/>
        <property name="identityService" ref="identityService"/>
        <property name="sessionStateService"
ref="sessionStateService"/>
        <!-- START HP SSO Configuration -->
                <property name="tokenWriter" ref="hpssoTokenWriter" />
        <!-- END HP SSO Configuration -->
    </bean>
```

vi. Edit the <idm-service>\WEB-INF\hpssoConfig.xml file as described below.

- Specify the domain name of the IdM server (for example, the Tomcat server). The domain name must match the DNS domain name of the system on which the IDM service is deployed, because the HP SSO cookies are domain-specific.

  > **Note:** All components that participate in SAML except the SM Server (the IdM service, SM web tier, SRC, and Mobility Client) must be in the same domain, because HP SSO cookies are domain-specific.

- Change secureHTTPCookie (default: false) to **true** if SSL is enabled between the user's browser and the web application server of the SM web tier, SRC, or Mobility Client.

See the following for an example.

```
<creation tokenGlobalTimeout="480" tokenIdleTimeout="30"
secureHTTPCookie="true">
        <!-- lwsso is required -->
        <lwsso>
            <!-- domain is required
                HPSSO 1.0 version supports a single domain only.
                All servers using HPSSO should have the same domain and
it should be denoted in this tag
            -->
            <creationDomains>
                <!-- for development environments only! -->
                <domain>mycompany.net</domain>
            </creationDomains>
        </lwsso>
 </creation>
```

Step 2. Configure SP-Initiated SSO: POST/Artifact Bindings

For POST/Artifact Bindings, in addition to the configuration in the previous step, you need to make sure that the applicationContext-saml.xml file contains the following property setting (default).

> **Note:** This file is located in the following folder: <*idm-service*>/WEB-INF/spring.

```
<property name="bindingsSSO">
        <list>
            <value>post</value>
            <value>artifact</value>
            <value>paos</value>
        </list>
</property>
```

Step 3. Disable ECP

ADFS does not support ECP; however, the IdM metadata includes the AssertionConsumerService for ECP. Therefore, this step is required.

To disable ECP, follow these steps:

a. Open the <idm-service>WEB-INF\spring\applicationContext-saml.xml file with a text editor.

b. Search for the following line, and comment it out.

```
<value>paos</value>
```

c. Search for the following line, and comment it out.

```
<property name="ecpEnabled" value="true"/>
```

Task 5. Configure a tenant and specify the ADFS metadata URL

A tenant is a data space in IdM. IdM user authentication is based on a tenant. For Service Manager users, a tenant must be specified in a .json file.

The federation metadata URL of the identity provider (that is, ADFS) is required for you to add the IdM service as a replying party trust later.

To configure a tenant and specify the ADFS metadata URL, follow these steps:

1. Locate the <idm-service>\WEB-INF\classes\seeded\samples\com.hpe.tenant1__1.3.2.1__Add_Update_Saml_Configuration.json.template file.
2. Copy the file to the seeded directory (<idm-service>\WEB-INF\classes\seeded\) and then remove the `.template` extension from the file name.
3. Open the com.hpe.tenant1__1.3.2.1__Add_Update_Saml_Configuration.json file in a text editor.

   > **Note:** The file has already a sample tenant named `IdmDemoOrg1` defined. You may want to update it to your own tenant name.

4. Update this file so that its content resembles the following example (in this example, a tenant name of **IDM-SM** is specified):

```
[
    {
        "operation":"ADD_OR_UPDATE",
        "type":"organization",
        "attributes":{
            "name":"IDM-SM",
            "displayName":"IDM-SM"
        }
},
```

```
    {
        "operation":"ADD",
        "type":"samlConfiguration",
        "names":{
            "organizationName":"IDM-SM"
        },
        "attributes":{
            "name":"IdmSamlConfiguration1",
            "displayName":"IdmSamlConfiguration1",
            "entityUrl":"https://localhost/2007-06/federationmetadata.xml"

        }
    }
]
```

- Specify the same organization name for both the **name** attribute in the ADD_OR_UPDATE operation and the **organizationName** attribute in the ADD operation.
- For the ADD_OR_UPDATE operation, the **name** and **displayName** attributes are mandatory.
- For the Add operation, the **organizationName**, **name**, and **displayName** attributes are mandatory. The **name** attribute serves as the unique key for your SAML configuration.
- The federation metadata URL of ADFS uses this format: https://<ADFS host>/federationmetadata/2007-06/federationmetadata.xml

Note that when the IdM service is started, the content of the .json file is loaded into IdM. Once the tenant is already created, you cannot update the organization name (the **name** and **organizationName** attributes), unless you want to create a new tenant. However, you can update the **entityUrl** attribute of the existing tenant. Make sure the content of the updated .json file resembles the following example:

```
[
    {
        "operation":"ADD_OR_UPDATE",
        "type":"organization",
        "attributes":{
            "name":"IDM-SM"
        }
},
    {
        "operation":"UPDATE",
        "type":"samlConfiguration",
        "names":{
            "organizationName":"IDM-SM",
            "samlConfigurationName":"IdmSamlConfiguration2"
```

```
            },
            "attributes":{
                "displayName":"IdmDemoSamlConfiguration2",
                "entityUrl":"https://mynewhost/2007-06/federationmetadata.xml"
            }
        }
    ]
```

Caution: After making any updates to the .json file, you must do the following:

1. Rename the file to increase its version number. For example, rename it from com.hpe.tenant1__1.3.2.1__Add_Update_Saml_Configuration.json to com.hpe.tenant1__1.3.2.2__Add_Update_Saml_Configuration.json. If you do not increase the version number, when the IdM service is restarted, the updated content will not be loaded and hence your changes will not take effect.
2. Restart the IdM service for the changes to take effect.

Note: After you have completed the IdM service deployment and setup, you will also need to specify the same tenant on the Service Manager side. For details, search for *SAML Single Sign-On setup* in the Service Manager Help Center.

Next, you need to create a database and configure the database connection for the IdM service.

Task 6. Create an empty database for IdM

You need to create an empty database for the IdM service.

Tip: During the creation of the database, make note of the following database connection information, which you will need to configure in the next task:

- Database server host and port
- Database name
- Database login credentials

  Note: Use an administrative user account to connect to the IdM database.

Supported databases

Currently, the supported database types include SQL Server, Oracle, and PostgreSQL. For information about their supported versions, see the Service Manager Support Matrix.

Tip: You may want to use the same database type for both Service Manager and IdM. Currently, the supported database types for Service Manager are SQL Server and Oracle.

Create a SQL Server or Oracle database

Follow exactly the same instructions for creating a database for Service Manager. See the "Prepare an RDBMS to support Service Manager" section in this document.

Create a PostgreSQL database

To create an empty PostgreSQL database, follow these steps:

1. Install PostgreSQL 9.40 or later by using the default options.
2. Create a role and password with login privileges.

   You can do this by using the following sql statement:

   ```
   create role <idmdbuser> with login password '<idmdbuser>';
   ```

3. Create an empty database and set the owner to the role created in the previous step. For example, an empty database named **IDM-SM**.

   You can do this by using the following sql statement:

   ```
   create database <idmdb> owner <idmdbuser> template template0 encoding 'UTF8';
   ```

Task 7. Configure database connection in the IdM service

Now, you need to configure database connection according to the IdM database that you created previously. The example database name **IDM-SM** is used in the following steps.

To do this, follow these steps:

1. Open the <idm-service>/WEB-INF/spring/applicationContext.properties file with a text editor.
2. Uncomment your database section, and comment out the other database sections.

   By default, the PostgreSQL database type is used and other database types are commented out.

3. Configure the database connection.

   SQL Server

   IdM needs a SQL Server JDBC driver to connect to the database. To configure the database connection using a SQL Server JDBC driver, follow these steps:

   a. Download Microsoft JDBC Driver 6.0 for SQL Server (or a higher version) from the Microsoft website.

   b. Extract the downloaded file, and then copy the sqljdbc42.jar file to the <idm-service>\WEB-INF\lib directory.

   > **Tip:** If the sqljdbc42.jar file cannot be found, copy a higher version of the sqljdbcxx.jar

file.

c. Set the idm.persistence.hbm2ddl.auto parameter to **false**.

```
idm.persistence.hbm2ddl.auto = false
```

d. Update the SQL Server database connection parameters as described in the following table.

Parameter	Description
idm.persistence.flyway.type	Set it to **sqlserver**.
idm.persistence.dialect	Change it to **sqlserver.db.specific.IdmSQLServer2012Dialect**.
idm.persistence.connection.driver.class	Change it to **com.microsoft.sqlserver.jdbc.SQLServerDriver**.
idm.persistence.connection.url	Enter a value with this format: jdbc:sqlserver://<IdM database server host>:<port>;DatabaseName=<IdM database name> For example: jdbc:sqlserver://localhost:1433;DatabaseName=IDM-SM
idm.persistence.connection.username idm.persistence.connection.password	Enter the login credentials that you specified for the IdM database.

Oracle

Perform the following steps:

a. From the Oracle website, download the Oracle JDBC driver appropriate for your database.

b. Copy the driver to the <idm service>\WEB-INF\lib folder.

c. Update the Oracle database connection parameters.

Parameter	Description
idm.persistence.flyway.type	Set it to **oracle**.
idm.persistence.dialect	Set it to

Parameter	Description
	org.hibernate.dialect.Oracle10gDialect.
idm.persistence.connection.driver.class	Set it to **oracle.jdbc.OracleDriver**.
idm.persistence.connection.url	Enter a value with this format: jdbc:oracle:thin:@<IdM database server host>:<port>:<IdM database name> For example: jdbc:oracle:thin:@localhost:1521:IDM-SM
idm.persistence.connection.username idm.persistence.connection.password	Enter the login credentials that you specified for the IdM database.

d. Add a key to the applicationContext.xml file.
   i. Open the <idm service>\WEB-INF\spring\applicationContext.xml file in a text editor.
   ii. Add the **hibernate.default_schema** key to the following property, as shown below:

```
<property name="hibernateProperties" >
    <props>
        <prop key="hibernate.jdbc.batch_
size">${idm.persistence.jdbc.batch_size}</prop>
        <prop key="hibernate.dialect">${idm.persistence.dialect}</prop>
        <prop key="hibernate.cache.provider_
class">${idm.persistence.cache.provider_class}</prop>
        <prop key="hibernate.show_sql">${idm.persistence.show_sql}
</prop>
        <prop
key="hibernate.hbm2ddl.auto">${idm.persistence.hbm2ddl.auto}</prop>
        <prop key="hibernate.connection.pool_
size">${idm.persistence.connection.pool_size}</prop>
        <prop key="hibernate.enable_lazy_load_no_trans">true</prop>
       <prop key="hibernate.default_schema"><db username></prop>
    </props>
</property>
```

   Where: <*db username*> should be replaced with the login account user name of the IdM database. For example:

```
<prop key="hibernate.default_schema">IDM-SM</prop>
```

PostgreSQL

Update the following PostgreSQL database connection parameters.

Parameter	Description
idm.persistence.flyway.type	Set it to **postgresql**.
idm.persistence.dialect	Set it to **org.hibernate.dialect.PostgreSQL9Dialect**.
idm.persistence.connection.driver.class	Set it to **org.postgresql.Driver**.
idm.persistence.connection.url	Specify a value that uses the following format: jdbc:postgresql://<*PostgreSQL database server host*>:<*port*>/<*IdM database name*> **Tip:** The default port of PostgreSQL is 5432. Example value: jdbc:postgresql://localhost:5432/IDM-SM
idm.persistence.connection.username idm.persistence.connection.password	Enter the login credentials that you created for the PostgreSQL database.

4. Check the log for errors.
   a. Open the <idm-service>\WEB-INF\classes\log4j.properties file in a text editor.
   b. Locate the following line:

      ```
      log4j.rootLogger=INFO, consoleAppender, jettyAppender
      ```

   c. Change **jettyAppender** to **tomcatAppender**, as shown below:

      ```
      log4j.rootLogger=INFO, consoleAppender, tomcatAppender
      ```

      Note: This will make IdM logging information be written to the following log file defined in the log4j.properties file:

      log4j.appender.tomcatAppender.File=${catalina.home}/logs/hpcloud-idm-service.log

   d. Start the Tomcat instance on which the IdM service is deployed.
   e. Open the hpcloud-idm-service.log file in a text editor to check for errors, and fix them if any.

Task 8. Download the IdM metadata

After the IdM server is started, the IdM metadata is generated and can be downloaded from the IdM service URL.

To download the IdM metadata, follow these steps:

1. Open the <idm-service>\WEB-INF\web.xml file in a text editor.
2. Comment out the following servlet.

```
<servlet>
     <servlet-name>default</servlet-name>
     <servlet-class>org.eclipse.jetty.servlet.DefaultServlet</servlet-class>
     <init-param>
        <param-name>dirAllowed</param-name>
        <param-value>false</param-value>
     </init-param>
     <load-on-startup>0</load-on-startup>
</servlet>
```

3. Start the IdM service web application server. In this example, start Tomcat.
4. Open the IdM service URL in a browser:

   https://<*IdM host FQDN*>:<*https port*>/*idm-service*/saml/metadata

   For example: https://myhost.mycompany.net:9443/idm-service/saml/metadata

   If the IdM service deployment is successful, the IdM metadata is displayed correctly, as shown in the following figure.

5. Download the metadata as **metadata.xml** from the browser.

> **Note:** Later, you will need to import the metadata to the IdP when creating a trust relationship with the IdP.

Task 9. Configure the IdM service for LW-SSO compatibility

> **Caution:** If you skip this task, SAML SSO is not compatible with the legacy LW-SSO solution.

Step 1. Specify the IdM tenant for LW-SSO

Once you have specified a tenant in the .json file, you need to specify this tenant in the LW-SSO configuration of IdM.

To specify the tenant for LW-SSO, follow these steps:

1. Open the <idm-service>\WEB-INF\hpssoConfig.xml file in a text editor.
2. Search for the following text to locate the LW-SSO section, which is below this text line:

   ```
   <lwsso  tenant="Tenant1">
   ```

3. Update the lwsso tag to include the tenant name that you specified in the .json file:

   ```
   <lwsso tenant="IDM-SM">
         ...
         <crypto initString="Init string must be replaced for production"
   cipherType="symmetricBlockCipher" engineName="AES"
                       paddingMode="CBC" keySize="256" encodingMode="Base64Url"
   algorithmPaddingName="PKCS7Padding" checkIntegrity="disabled"
                       cryptoSource="lw" directKeyEncoded="false"
   directKeyEncoding="Hex" jcePbeAlgorithmName="PBEWithHmacSHA1"
                       jcePbeMacAlgorithmName="PBEWithHmacSHA1"
   macAlgorithmName="SHA1" macKeySize="256" macPbeCount="20" macType="hmac"
                       pbeCount="20" pbeDigestAlgorithm="SHA1"/>

          ...
   </lwsso>
   ```

Step 2. Configure LW-SSO settings

You need to specify the domain and initString settings in the IdM service.

To do this, follow these steps:

1. Open the <idm-service>\WEB-INF\hpssoConfig.xml file in a text editor.
2. Check that you have already specified the domain name of the IdM server (for example, the Tomcat server). The domain name must match the DNS domain name of the system on which the IDM service is deployed, because the HP SSO cookies are domain-specific.

   > **Note:** All components that participate in SAML except the SM Server (the IdM service, SM web tier, SRC, and Mobility Client) must be in the same domain, because HP SSO cookies are domain-specific.

3. Change the initString value to match the one specified in other HPE applications that will participate in LW-SSO.

```
<lwsso>
       <!-- crypto is required.
         It defines how to encrypt the tokens and how to decrypt them
            All inline attributes have default values (denoted here) save initString.
                initString - is the key for decryption of the lwsso token. This is the
shared secret of all servers
                protected by lwsso and connected to the same authentication point server;
therefore, it
                must be identical in all configurations of all servers in the system.
                (all other values are defaults)
                   -->
            <crypto initString="Init string must be replaced for production"
cipherType="symmetricBlockCipher" engineName="AES"
                    paddingMode="CBC" keySize="256" encodingMode="Base64Url"
algorithmPaddingName="PKCS7Padding" checkIntegrity="disabled"
                    cryptoSource="lw" directKeyEncoded="false"
directKeyEncoding="Hex" jcePbeAlgorithmName="PBEWithHmacSHA1"
                    jcePbeMacAlgorithmName="PBEWithHmacSHA1"
macAlgorithmName="SHA1" macKeySize="256" macPbeCount="20" macType="hmac"
                    pbeCount="20" pbeDigestAlgorithm="SHA1"/>

            <!-- Optional tag. however, if configured, then it must be
configured on all entities in the system.-->
            <!--
            <sign lookForKeyStoreInClasspath="false"
algorithmName="SHA256withRSA" keyStorePassword="topazPwd"
                  privateKeyPassword="mercuryPwd" keyStorePath="C:\MSM"
privateKeyDefaultAliasName="lwsso"
                  certificateDefaultAliasName="lwsso" keyStoreName="lwsso"
keyStoreType="JKS"
                  providerName="Default Provider Name" />
            -->
 </lwsso>
```

Task 10. Specify an IdM token signing key

You need to specify a key for signing IdM tokens.

1. Open the \WEB-INF\spring\applicationContext.properties file in a text editor.
2. Specify a key in the idm.encryptedSigningKey parameter.

   For example, specify the following key:

   ```
   idm.encryptedSigningKey=awscd456!
   ```

> **Note:** There is no restriction on the length and characters of this key. When the IdM service deployment is complete, you will need to specify the same key on the Service Manager side. For details, search for *SAML Single Sign-On setup* in the Service Manager Help Center.

(Optional) Task 11. Specify an IdM user account for Service Manager

Each IdM client (the SM Web Tier, SRC, or Mobility Client) needs an IdM user account to access the IdM service.

By default, the IdM service has a user account defined: idmTransportUser (user name) and idmTransportUser (password). You can skip this task and simply specify this default user account in the SM Web Tier, SRC, and Mobility Client. For details, see the *SAML Single Sign-On setup* section in the Service Manager Help Center.

You cannot change the user name. However, you can change the password as you like. To change the IdM user account password, follow these steps:

1. Open the <idm-service>WEB-INF\classes\integrationusers.properties file in a text editor.
2. Locate the line with an encrypted string:

   idmTransportUser=ENC(xxxx)

   Where: xxxx represents an encrypted string.
3. Change this line to the following:

   idmTransportUser=idmTransportUser,ROLE_ADMIN,PERM_IMPERSONATE,enabled

   Where:

   - "idmTransportUser" on the left side of the equals sign (=) is the user name, which must not be changed.
   - On the right side of the equals sign (=), "idmTransportUser" is the default password and the rest of the string are other properties of the user account.
4. Change the default password to your own value. For example, change it to "1Qaz2wsx3edc":

   idmTransportUser=**1Qaz2wsx3edc**,ROLE_ADMIN,PERM_IMPERSONATE,enabled

   > **Note:** In a later task, you will run the IdM encryption tool to encrypt all IdM passwords and keys, including the entire IdM user account property string. You will need to copy the encrypted string back to this file. For more information, see the "Encrypt IdM passwords and keys" task.
5. Save the file.

> **Note:** You will also need to specify the same user account on the Service Manager side. For details, search for the *SAML Single Sign-On setup* in the Service Manager Help Center.

Task 12. Replace JRE policy files for the IdM server

By default, Microsoft ADFS uses the SHA-256 secure hash algorithm, which requires you to replace the default JRE policy files used by the IdM web application server.

To do this, follow these steps:

1. Download the unlimited strength JCE policy files for your JRE:
   - local_policy.jar
   - US_export_policy.jar

   For example, for Tomcat 8.0, visit the Oracle website to download the unlimited strength JCE policy files:

   http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html (for JRE 8)

   http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html (for JRE 7)
2. On the IdM web application server host, browse to the <JRE>\lib\security folder.
3. Replace the policy files with the unlimited strength JCE policy files that you have downloaded.

Task 13. Create a trust relationship with ADFS

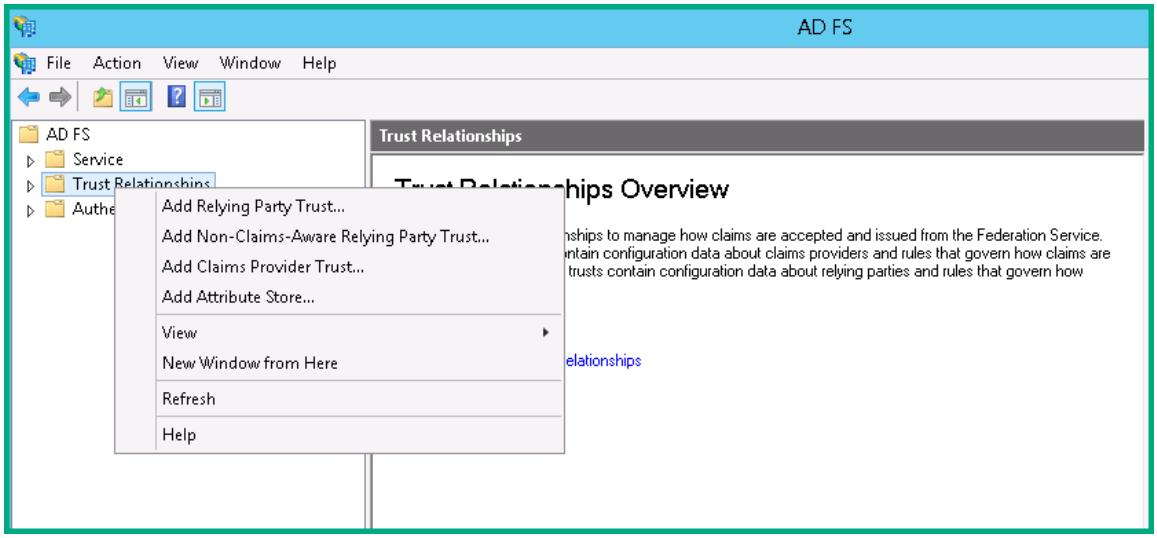
Currently, the only supported identity provider is Microsoft Active Directory Federation Service (ADFS) 2.0 or 3.0. ADFS helps you use single sign-on (SSO) to authenticate users to multiple, related web applications over the life of a single online session.

Once ADFS is installed and configured to authenticate users from an LDAP directory, you are ready to add the IdM metadata to ADFS to add the IdM service as a trusted relying party.

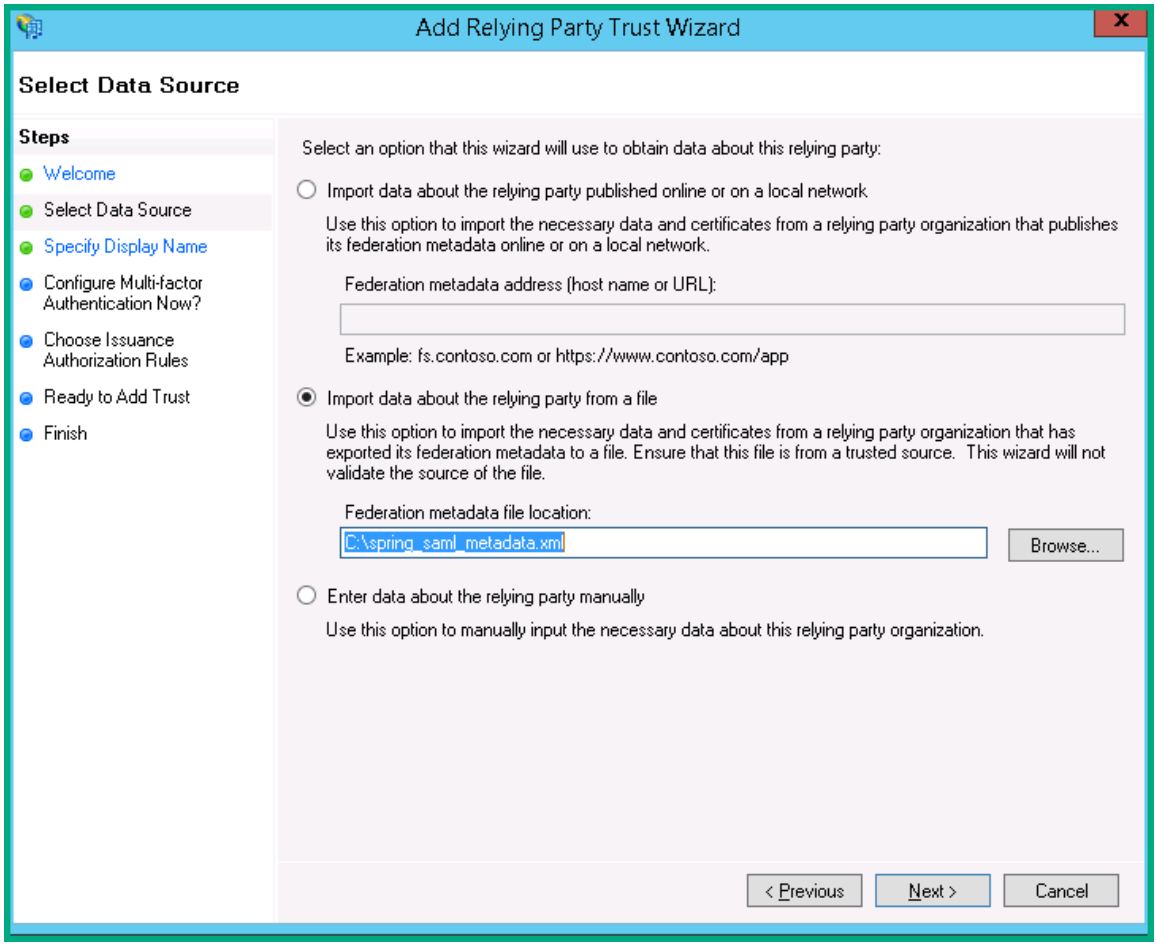
> **Note:** The screenshots in this section are from ADFS 3.0, and may slightly differ from those in ADFS 2.0.

To add the IdM service as a trusted relying party to ADFS, follow these steps:

1. In the ADFS 3.0 Management Console, right-click **Trust Relationships** and then select **Add Relying Party Trust**.

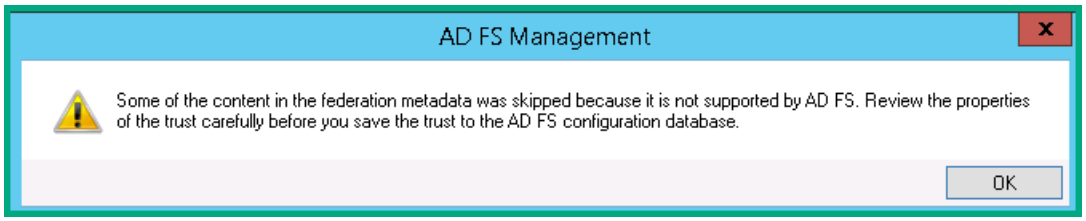


2. Select **Import data about the relying party from a file**, and then select the IdM metadata file (metadata.xml) that you created previously. Click **Next**.

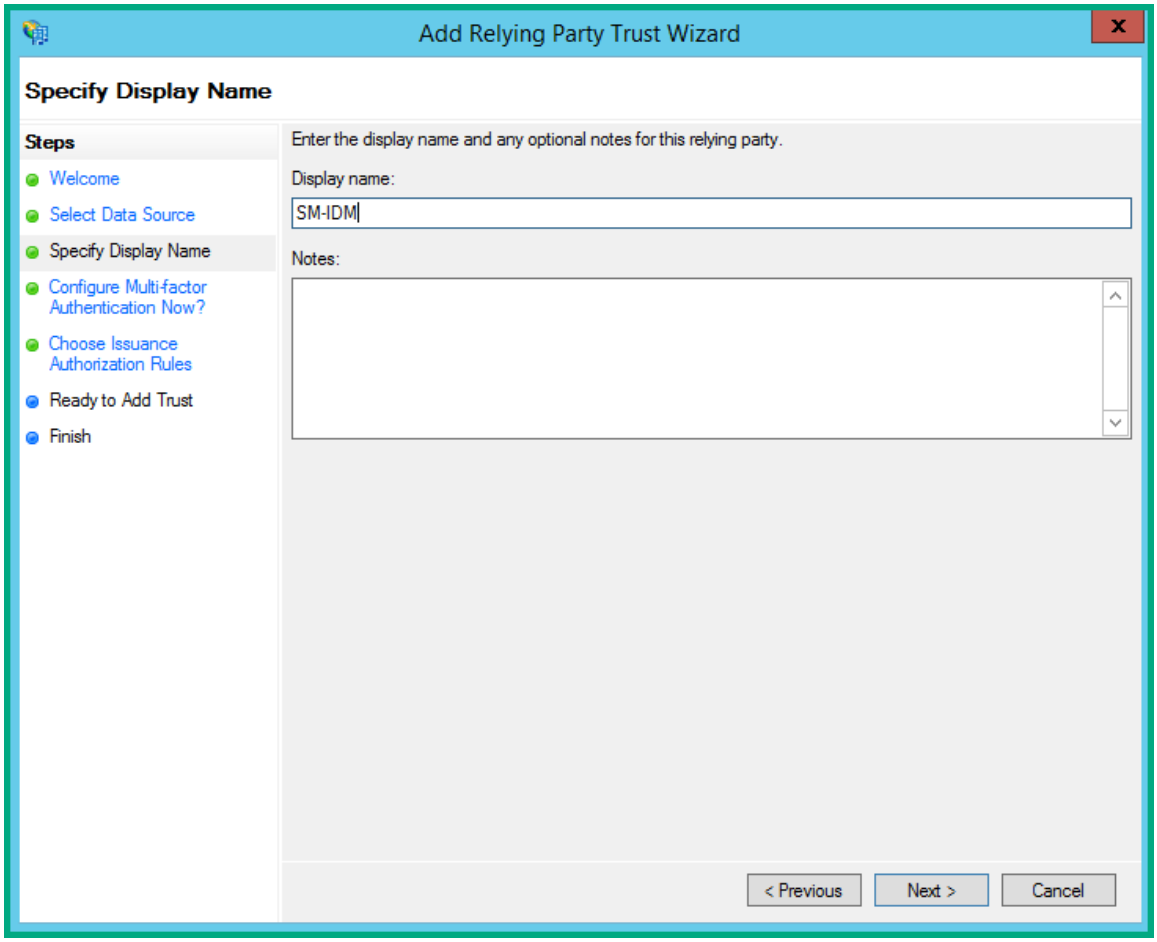


3. The wizard may display a warning, indicating that some content of the metadata is not supported. You can safely ignore this warning.

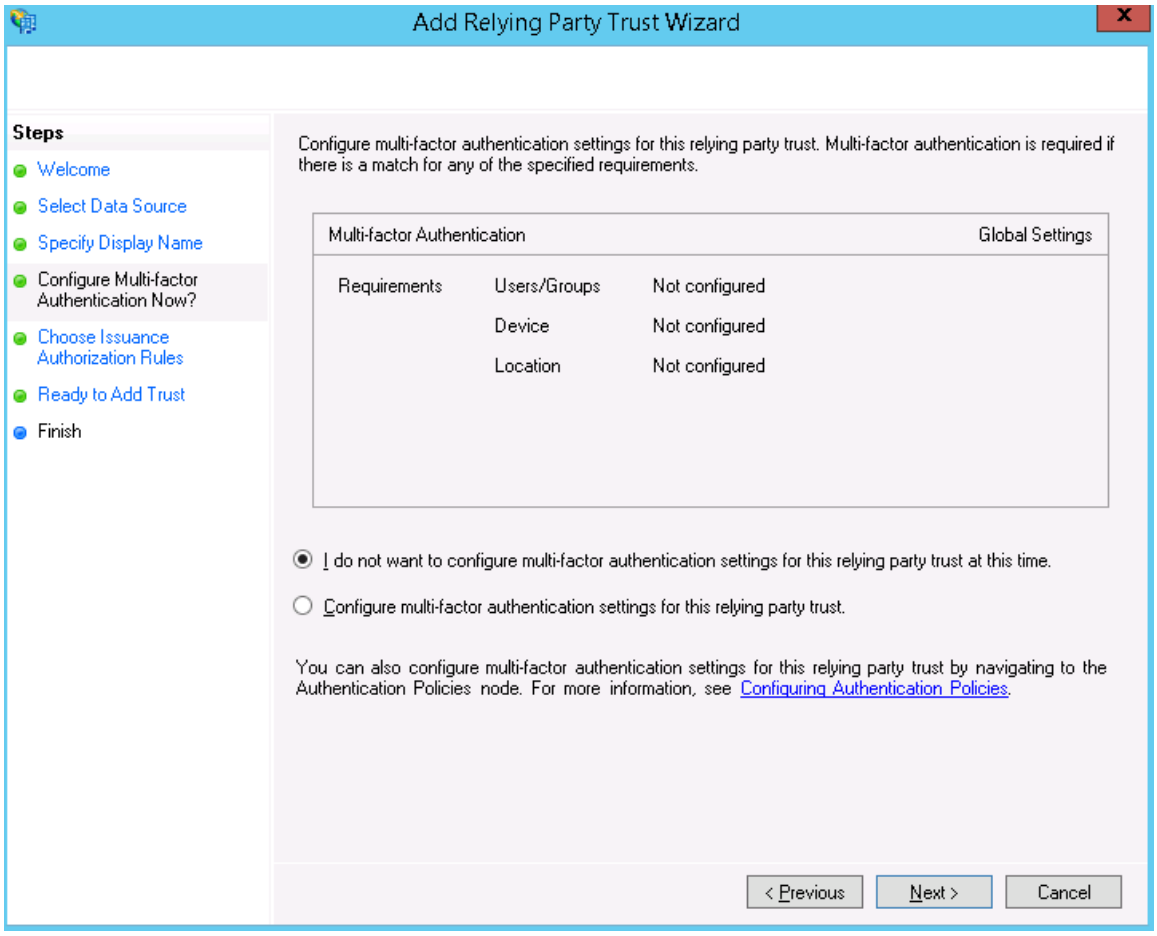
   Click **OK** to ignore the warning.



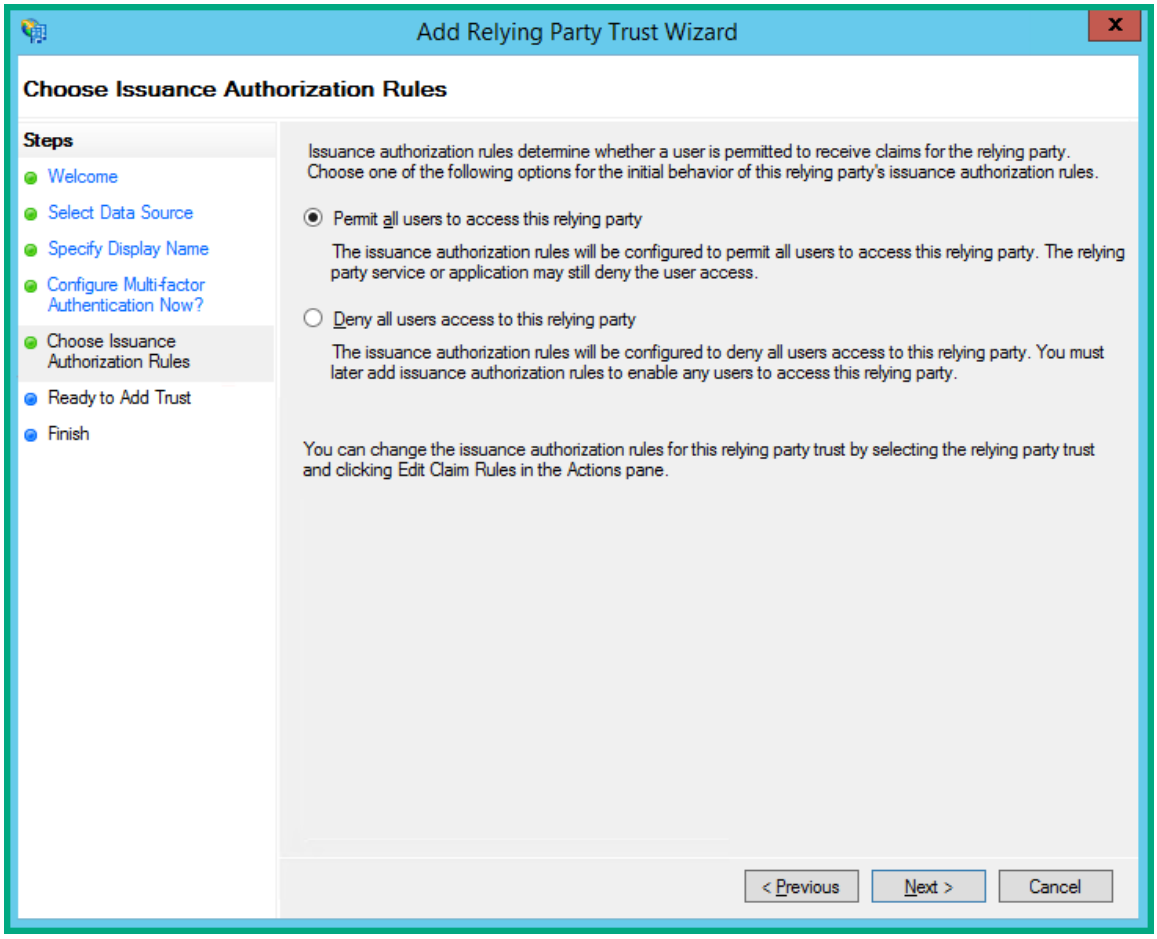
4. Specify a display name for the IdM service, and add optional notes. Click **Next**.



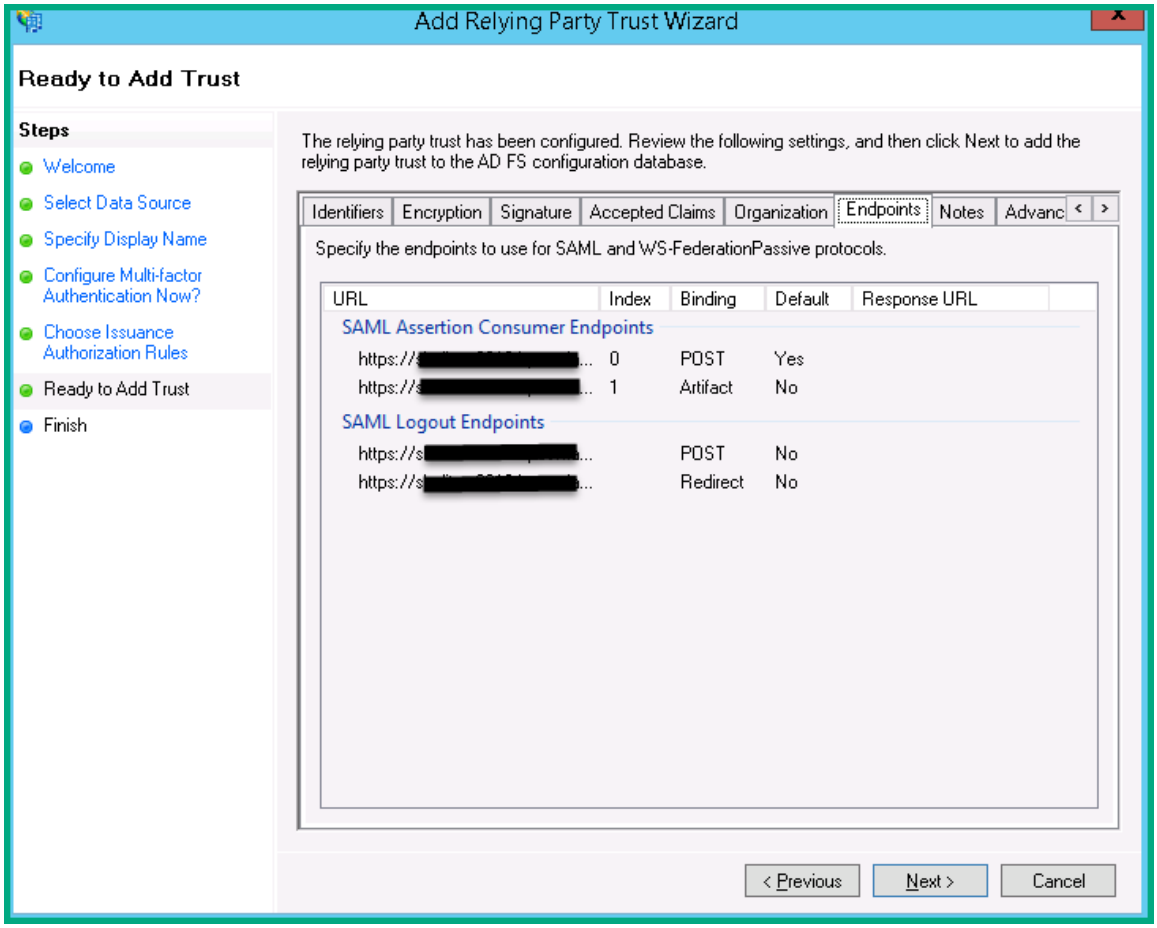
5. Make sure the **I do not want to configure multi-factor authentication setting for this relying party trust at this time** option is selected, and then click **Next**.



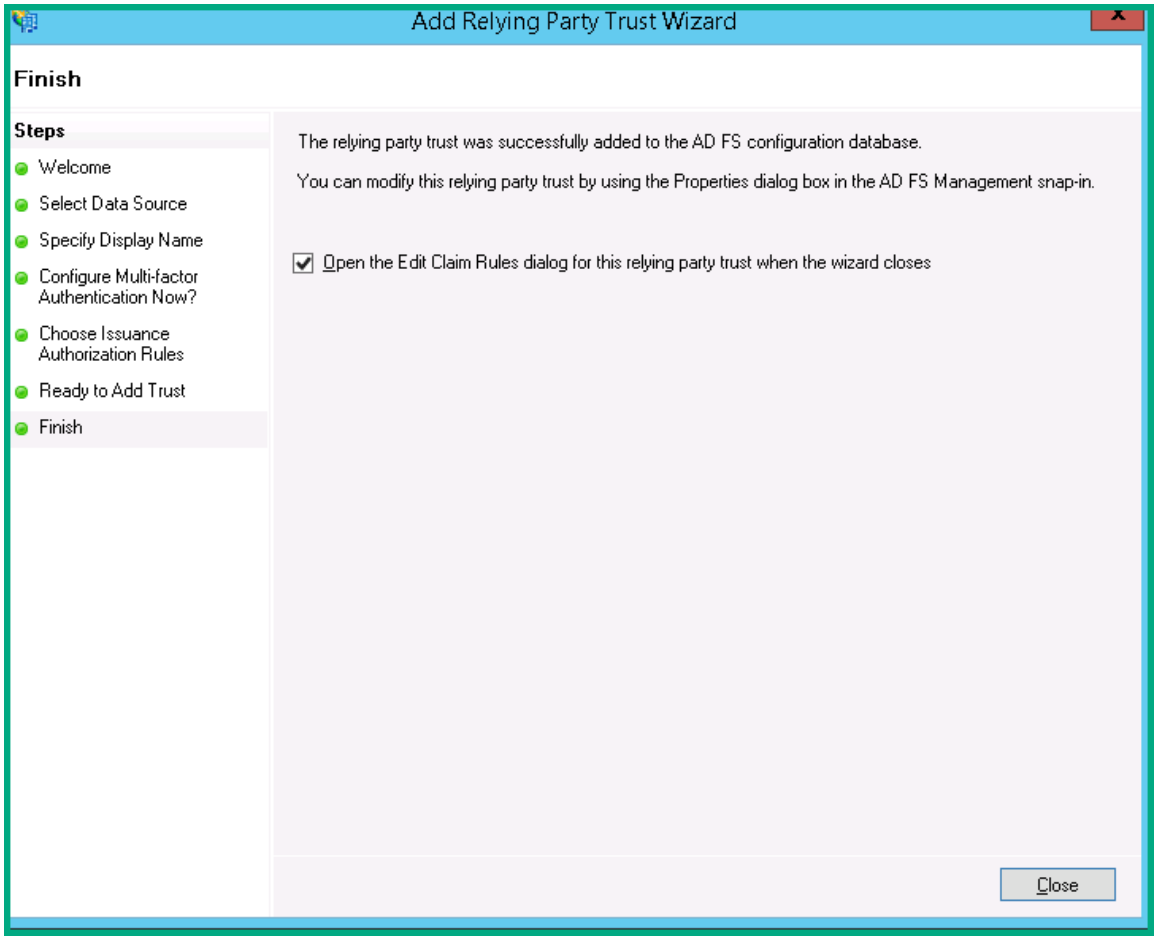
6. Select the **Permit all users to access this replying party** issuance authorization rule.



7. You are now in the Ready to Add Trust step. Check that the **Endpoints** tab contains multiple endpoint values. If not, verify that your metadata was generated with https protocol URLs.

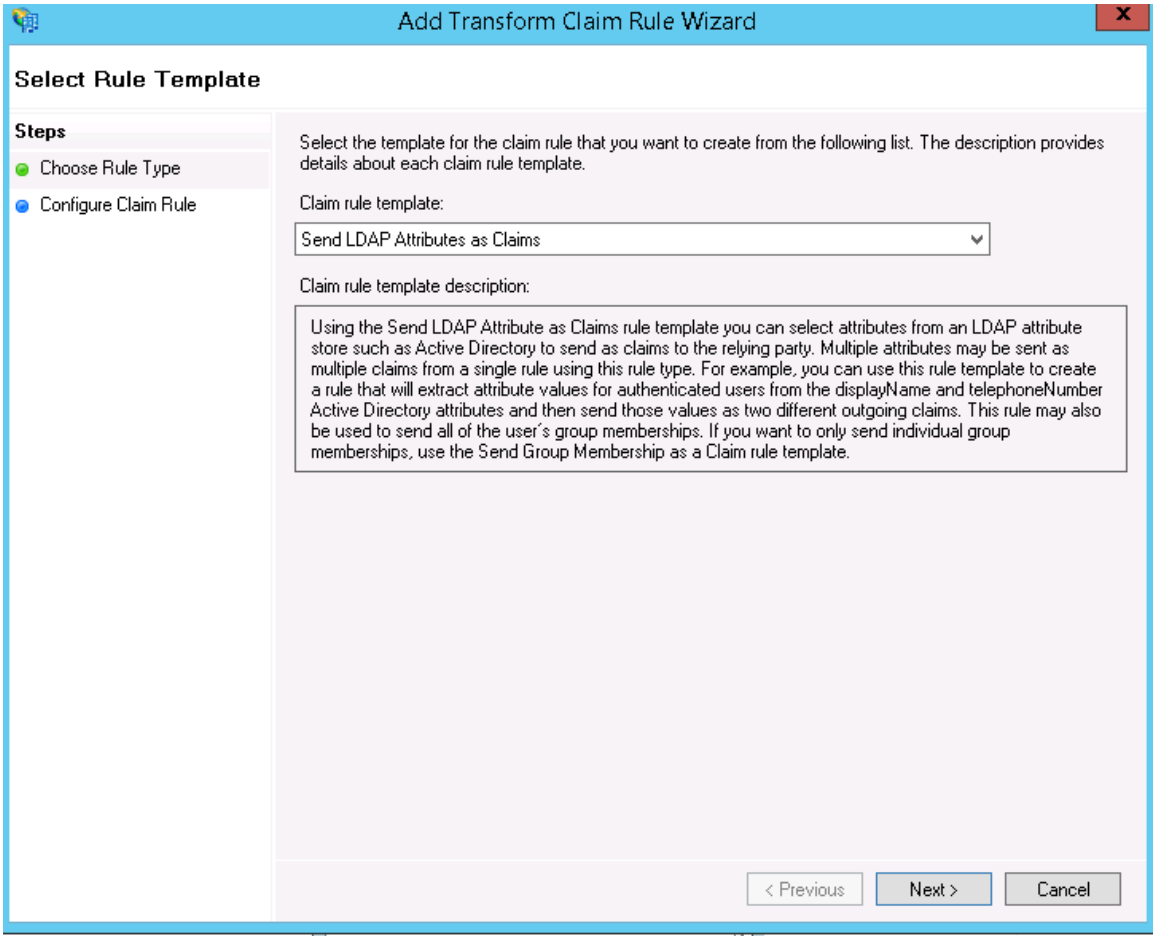


8. Leave the **Open the Edit Claim Rules dialog** checkbox selected, and click **Close** to close the wizard.



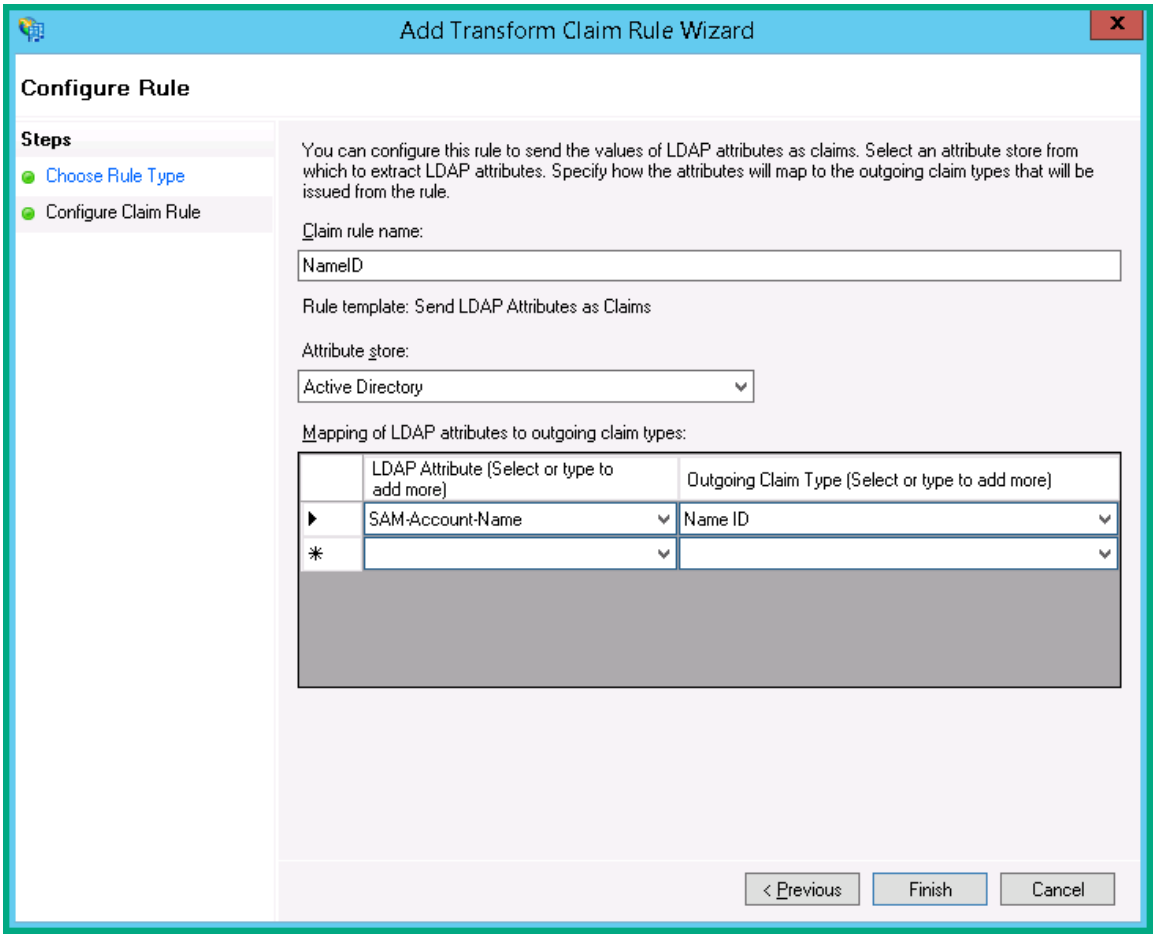
9. The Add Transform Claim Rule wizard opens. Perform the steps below to configure the NameID element as part of the Subject in the SAML Response message.

a. Select **Add Rule**, and then select **Send LDAP Attributes as Claims**. Click **Next**.



b. Specify the following fields to configure the claim rule:

- Claim rule name: enter **NameID**
- Attribute store: select **Active Directory**
- LDAP Attribute: select **SAM-Account-Name**
- Outgoing claim type: select **Name ID**



c. Close the wizard and the **Apply the claim rules** window.

> **Note:** In ADFS 3.0, you may need to configure the Name ID as a PassThrough claim.

Task 14. Import the IdP public key into the IdM SAML keystore

In this task, you will export the public key from the ADFS certificate and then import the key into the SAML keystore file of IdM. This task is required for IdM to decrypt SAML responses from ADFS.

Step 1. Export the public key portion of the ADFS federation service certificate

1. From your operating system, start Active Directory Federation Services.
2. Right-click **Federation Service**, and then click **Properties**.
3. On the **General** tab, under **Communicating certificate**, click **View**.
4. In the **Certificate** dialog box, select the **Details** tab.
5. On the **Details** tab, click **Copy to File**.

6. Click **Next**.
7. On the **Export Private Key** page, make sure that **No, do not export the private key** is selected, and then click **Next**.
8. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
9. On the **File to Export** page, specify the certificate file in **File name**, and then click **Next**.

   > **Note:** In this example, we use **Per_ADFS.cer** as the file name.

10. Click **Finish**.
11. Validate success by checking to see that the file you specified was created at the specified location.

Step 2. Import the ADFS public key into the IdM keystore

The IdM SAML keystore file is: <idm-service>\WEB-INF\classes\security\samlKeystore.jks.

To do this, run the following command:

```
keytool -importcert -alias some-alias -file Per_ADFS.cer -keystore samlKeystore.jks
```

> **Note:** When prompted for the password of samlKeystore.jks, enter `nalle123`.

If you want to use your own keystore file instead of the out-of-box one, you need to do the following:

1. Replace the out-of-box keystore file with your own one.
2. If your keystore file uses a different name, specify your file in the <idm-service>\WEB-INF\spring\applicationContext.properties file:

   idm.saml.keystore=classpath:security/samlKeystore.jks

   Replace samlKeystore.jks with your own file name.
3. Specify the following parameters accordingly in the <idm-service>\WEB-INF\spring\applicationContext.properties file:
   - idm.saml.keystore.password=ENC(xxx)
   - idm.saml.keystore.defaultKey.name=ENC(xxx)
   - idm.saml.keystore.defaultKey.password=ENC(xxx)

   > **Note:** Replace the **ENC(xxx)** parts with your own values.

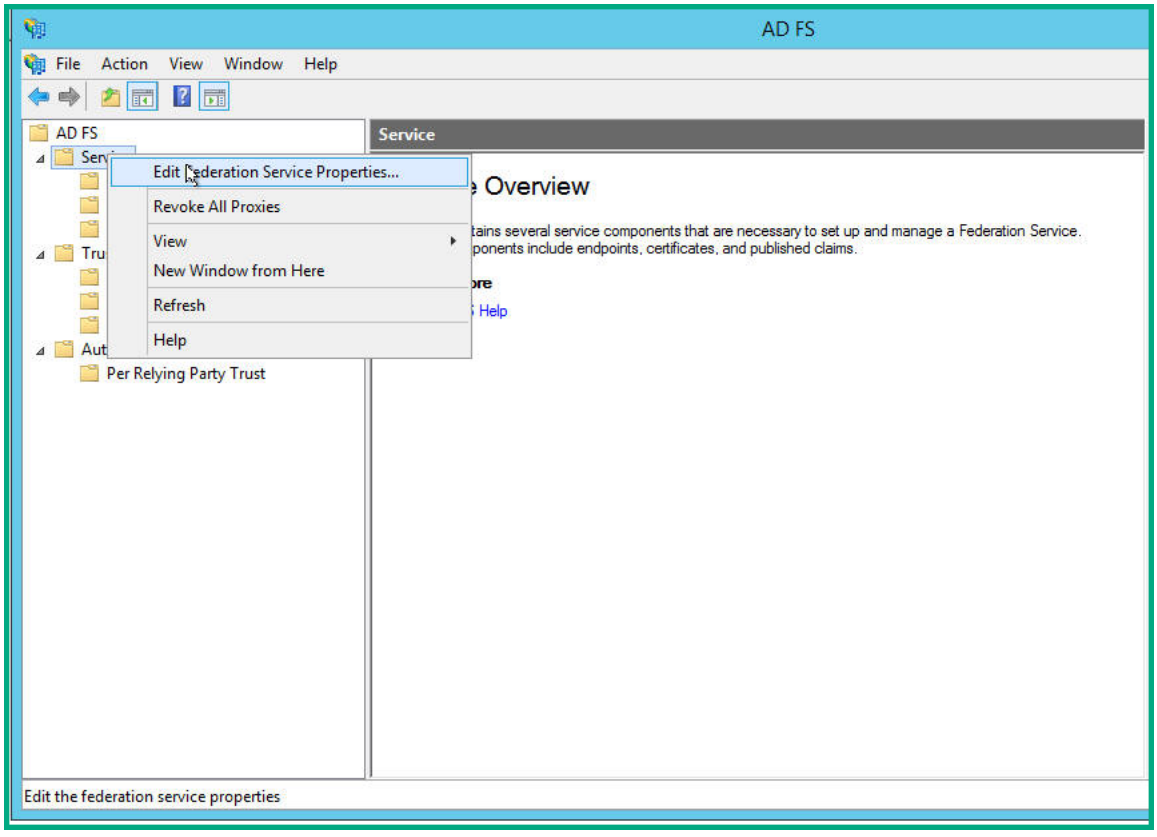
Task 15. Adjust the max authentication age setting in the IdM service

The IdP (Microsoft ADFS) uses a parameter named **Web SSO lifetime** to determine whether a user login request is sent within a valid time period of the user's last login. If yes, the user is automatically logged in without the need to enter a user name and password. Similarly, the IdM service uses a parameter named **maxAuthenticationAge** for the same purpose.

To enable SAML SSO for Service Manager, the **maxAuthenticationAge** value defined in the IdM service must be no less than the **Web SSO lifetime** value defined in the IdP. By default, the IdM service setting is 7200 seconds (2 hours), and the ADFS setting is 480 minutes (8 hours). Since this IdP setting is usually a global setting for your organization, you may want to change the IdM setting according to your IdP setting. To do this, perform the following steps.

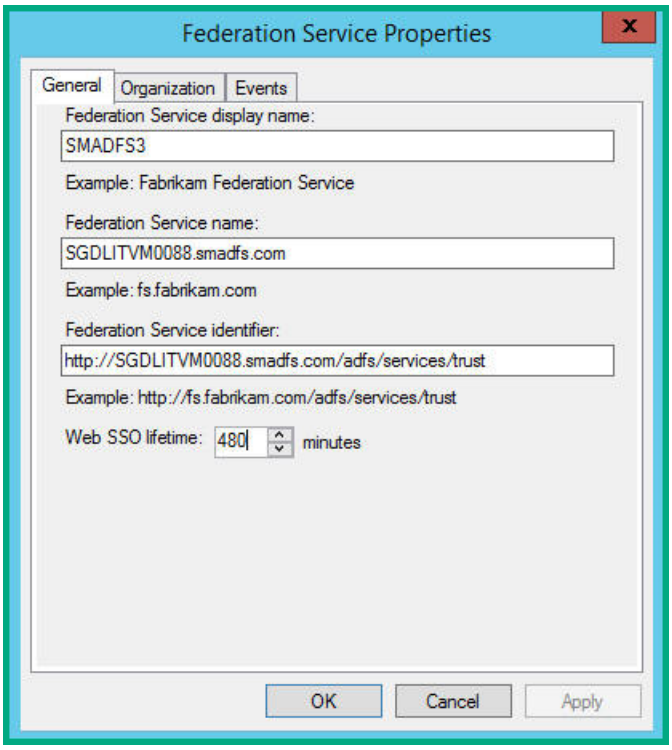
Step 1. Check the web SSO lifetime value in the IdP

1. Open Microsoft ADFS.
2. Click **Service** and then select **Edit Federation Service Properties**.



3. On the **General** tab, check the **Web SSO lifetime** value.

Note: The default value is 480 minutes (8 hours).



Step 2. Adjust the web SSO lifetime setting in the IdM service

To check the value in the IdM service, follow these steps:

1. Open the <idm-service>\WEB-INF\spring\applicationContext-saml.xml file in a text editor.
2. Search for the following line:

   ```
   <bean id="webSSOprofileConsumer"
   class="org.springframework.security.saml.websso.WebSSOProfileConsumerImpl"/>
   ```

3. Change this line to the following:

   ```
   <bean id="webSSOprofileConsumer"
   class="org.springframework.security.saml.websso.WebSSOProfileConsumerImpl">
       <property name="maxAuthenticationAge" value="xxxx"/>
   </bean>
   ```

   Where: xxxx represents a value (in seconds) that is no less than your ADFS Web SSO lifetime. For example, if your ADFS setting is 120 (minutes), XXXX should 7200 or greater.

(Optional) Task 16. Encrypt IdM passwords and keys

In this task, you will run the IdM encryption tool to encrypt all IdM passwords and keys. This task is

optional but highly recommended for the best security in production environments.

To do this, follow these steps:

1. Update the second column of the following table with the passwords and keys that you have configured for IdM.

Location	Password/Key	Description
<idm-service>\WEB-INF\classes\integrationusers.properties	idmTransportUser=xxxxxx	This is the IdM password that Service Manager uses to access the IdM service. ◦ XXXXXX is a string that defines the password and other properties of the IdM user account. For example: idmTransportUser=**1Qaz2wsx3edc**,ROLE_ADMIN,PERM_IMPERSONATE,enabled ◦ You must encrypt the entire string on the right side of the equals sign.
<idm-service>\WEB-INF\spring\applicationContext.properties	idm.encryptedSigningKey=xxxxxx	This is the signing key used to sign IdM tokens.
<idm-service>\WEB-INF\spring\applicationContext.properties	idm.persistence.connection.password = xxxxxx	This is the password of the IdM database connection account.
<idm-service>\WEB-INF\spring\applicationContext.properties	idm.saml.keystore.password=xxxxxx idm.saml.keystore.defaultKey.name=xxxxxx idm.saml.keystore.defaultKey.password=xxxxxx	This is the password, default key name and passwords of the IdM SAML keystore file: <idm-service>\WEB-INF\classes\security\samlKeystore.jks.

Location	Password/Key	Description
		If you use the out-of-box keystore file, these parameter values are already encrypted and you must not change them.

2. Change to the <idm-service>/web-inf/lib directory.
3. For each parameter value in the previous table, run the following command:

   ```
   java -cp "cryptoUtil-1.0.3.jar;jasypt-1.9.1.jar;commons-codec-1.7.jar;slf4j-log4j12-1.7.5.jar;slf4j-api-1.7.5.jar;log4j-1.2.17.jar" com.hp.ccue.crypto.util.App encrypt xxxxxx
   ```

   Where: xxxxxx represents the value that you want to encrypt.

   When the encryption is complete, the original value and encrypted value are returned. The following is an example:

   ```
   original:1Qazwsx3edc
   encrypted:0bEhLG0zDOdYBLf013p3Qfn66kNTMYvh
   ```

4. Copy the encrypted value back to the IdM configuration file to overwrite the original parameter value by using the following format:

   Parameter=ENC(encrypted value)

   Here are examples:

   idmTransportUser=ENC(0bEhLG0zDOdYBLf013p3Qfn66kNTMYvh)

   idm.encryptedSigningKey=ENC(0bEhLG0zDOdYBLf013p3Qfn66kNTMYvh)

Next steps

Next, you need to configure SAML authentication in the Service Manager Server, Web Tier, SRC, and Mobility Client and verify that your SAML SSO setup is successful. For details, see the "SAML Single Sign-On setup" help topic in the Service Manager Help Center.

Install the Service Manager Help Center

The Service Manager help center provides a centralized location to access and store all online help files. You can install the online help on a local file system, a network share, or on a web server. If you want end users to access documentation from the Windows or web clients or directly from a web browser, you must install the help on a web server.

You cannot upgrade previous Help Servers to the Service Manager9.50 Help Center. You must install the Service Manager9.50 Help Center in a new folder or on a different system than your previous Help Server. HPE recommends that you remove previous Help Servers, but it is not required.

Follow these instructions to install the Help Center.

Meet the Service Manager online help requirements

Important: You cannot upgrade previous Help Servers to the Service Manager9.50 help. You must install the Service Manager9.50 help in a new folder or on a different system than your previous Help Server. HPE recommends that you remove previous Help Servers, but it is not required.

Caution: Make a backup of any customized Help files that you have created for your Service Manager clients.

Make sure that you meet the following requirements so that you can install the online help:

1. Have 500 MB disk space.
2. Have a minimum of 256 MB RAM
   - For testing purposes, 128 MB RAM is sufficient.
   - For production purposes, RAM is based on the expected user load.
3. If you plan on installing the help on a web server:
   - Have a web server (for example, Apache) installed on the system
   - Have a free communications port to listen for HTTP connections requests. For most web servers, the default communications port is 80.

Install the Service Manager online help on a web server

Service Manager9.50 provides two sets of online help:

- **sm_help_codeless.zip**: This version if intended for customers who are running Service Manager Codeless, in which all business modules (Service Desk, Incident Management, and so on) are implemented on Process Designer.
- **sm_help_hybrid.zip**: This version is intended for customers who are running Service Manager Hybrid.

To install the online help, follow these steps:

1. Log in to the system on which you want to install help as a user with local administrator privileges.
2. Extract the online help into your web server's document root. For example, to install the online help on an Apache web server on a Windows system, extract the online help into the folder `C:\Program Files\Apache Software Foundation\Apache2.2\htdocs`.
3. Configure a virtual directory and set any access permissions you want for the online help (optional). For example, an Apache web server does not require any virtual directory configuration if you want to use the default folder **sm_help_codeless**.
4. Start your web server.

Next, you need to set up access to the online help from the Windows client and web client to test the help installation.

Set up access to the online help from the Windows Client

To configure the Windows Client to display the online Help from a web server, set the Windows Client preferences and define the help server's host name and communications port.

1. Log in to the Windows Client.
2. Click **Window** > **Preferences**. The Preferences window opens.
3. Click the **Help** node to expand it.
4. Click **Help Server**.

5. Enable the **Use a Help server to access documentation** option.
6. Type the following information:
   - **Help Server host name**: Fully qualified domain name or IP address of the help server host
   - **Help Server port number**: The communications port of the help server host
   - **Help Server context**: The virtual directory, if any, of the web server hosting your help.
7. Click **OK**. The Windows Client now displays the online help from the web server hosting help when the user clicks on the Help icon or selects **Help** > **Help Contents**.

This setting is saved with your client preferences and is captured by the Client Configuration utility so that you can deploy it to your Windows Client users.

The Window client launches the help using this URL:
http://<helpserverhost>:<helpserverport>/<helpServerContext>/

Set up access to the online help from the web client

To set up web clients to display online help from a web server, configure the web client web.xml file to define the help server's host name and communications port, as well as the virtual directory in which the online help is deployed.

1. Log in to the server where you installed the web tier.
2. In a text editor, open the `web.xml` file from the `<web tier>/WEB-INF` folder of your application server installation.
3. Set the showHelp parameter to true (default: false).

```
<context-param>
    <param-name>showHelp</param-name>
    <param-value>true</param-value>
</context-param>
```

4. In the helpServerHost entry, type the fully qualified domain name or IP address of the help server host of the web server hosting your help. For example, type `helpserver.domain.com`.

```
<init-param>
    <param-name>helpServerHost</param-name>
    <param-value>helpserver.domain.com</param-value>
</init-param>
```

5. In the helpServerPort entry, type the communication port of the help server. For example, type

`8080` or leave the communications port empty to use the default communications port of 80.

```
<init-param>
      <param-name>helpServerPort</param-name>
      <param-value>8080</param-value>
</init-param>
```

6. Insert a helpServerContext entry below the helpServerPort entry, and set the parameter to the name of the virtual directory where you publish the online help.

   ```
   <init-param>
         <param-name>helpServerContext</param-name>
         <param-value>sm_help</param-value>
   </init-param>
   ```

   > **Note:** It excludes the web server's document directory path. For example, if the help is deployed in C:/Apache/2.2/htdocs/sm_help, the document directory path is C:/Apache/2.2/htdocs/ and the virtual directory name is sm_help. Therefore, the helpServerContext parameter should be set to sm_help. The virtual directory path can contain subdirectories, such as **sm_help/codeless**.

7. Save and close the `web.xml` file.

The web client launches the online help using the following URL:

http://<*helpServerHost*>:<*helpServerPort*>/<*helpServerContext*>

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation Guide (Service Manager 9.50)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-ITSM@hpe.com.

We appreciate your feedback!

Hewlett Packard
Enterprise