



Installing the Smart+Connected PS on WebLogic

This chapter describes how to install and deploy the Cisco Smart+Connected Personalized Spaces (Smart+Connected PS) application by using the Oracle database and WebLogic application server.

- [Prerequisites, page 2-1](#)
- [Installing on a Colocated or Non-Cluster Server Setup, page 2-2](#)
- [Installing on a Cluster Server Setup, page 2-28](#)

The Smart+Connected PS installation can be initiated only after the Cisco Service Delivery Platform (SDP) is set up and database scripts for the SDP have been executed.

Prerequisites

- [Gathering Additional Information, page 2-1](#)
- [Verifying the Network Configurations, page 2-2](#)

Gathering Additional Information

Prior to beginning the installation procedure, you must gather the following information:

- Database details
 - Database SID
 - Database IP address or the DNS hostname
 - Database Port number
 - Database schema username
 - Database schema password
 - SSH credentials

These credentials are required to access the machine. This account needs to be able to run SQLPlus.
- Application Server details
 - Location of the WebLogic directory, if the WebLogic server has been pre-installed. If not, then you require the preferred path to setup the WebLogic server.
 - SSH credentials

Send documentation comments to scc-docfeedback@cisco.com

These credentials are required to access the machine. This account needs to be able to run SQLPlus.

Verifying the Network Configurations

Verify the following network configuration:

- All machines are in the same LAN.
- All machines are configured to be on the same locale.
- System time is synchronized on all the machines using NTP.
- All dependent components for the Smart+Connected PS solution must be accessible over the network.

Installing on a Colocated or Non-Cluster Server Setup

To install the Smart+Connected PS application on a colocated or non-cluster server setup, perform the following steps:

1. [Installing the Application, page 2-3](#)
2. [Configuring Audio Notification to the Cisco IP Phone, page 2-4](#)
3. [Configuring the Database, page 2-4](#)
4. [Creating the WebLogic Domain, page 2-5](#)
5. [Extending the WebLogic Domain, page 2-7](#)
6. [Starting the WebLogic Server, page 2-8](#)
7. [Configuring the Java Message Service \(JMS\), page 2-8](#)
8. [Setting Up the BIRT Engine, page 2-9](#)
9. [Configuring Logging, page 2-10](#)
10. [About Properties Files, page 2-10](#)
11. [Updating the Properties Files, page 2-15](#)
12. [Updating the WebLogic Configuration, page 2-16](#)
13. [Configuring the LDAP Authentication, page 2-18](#)
14. [Setting Up the Push-to-Phone Feature, page 2-20](#)
15. [Configuring the Secured URL, page 2-20](#)
16. [Configuring Installer for the Mobile Devices, page 2-21](#)
17. [Deploying Apache Jackrabbit, page 2-25](#)
18. [Deploying the Smart+Connected PS Application, page 2-26](#)
19. [Importing SSL Certificates, page 2-26](#)
20. [Accessing the Application and Verifying the Installation, page 2-27](#)

Send documentation comments to scc-docfeedback@cisco.com

Installing the Application

The Smart+Connected PS installation package consists of an executable file `install.bin` located on the product DVD or obtained through e-delivery.

Before you begin the installation process, do the following:

- Copy the installer file (`install.bin`) to a local directory.
- Ensure that the `JAVA_HOME` environment variable is set to the location where the JDK is installed and the `PATH` environment variable should include the `JAVA_HOME/bin` directory.

To install the Smart+Connected PS application, perform the following steps:

-
- Step 1** Open a terminal and navigate to the local directory that includes the installer and enter the `chmod u+x install.bin` command to grant permissions to execute the installer file.
 - Step 2** Enter the `./install.bin` command.
 - Step 3** Press the **Enter** key.
The Smart Plus Connected Communities —Introduction screen appears.
 - Step 4** Click **Next**.
The License Agreement screen appears.
 - Step 5** Select **I accept the terms of the License Agreement**, and click **Next**.
The Choose Install Folder screen appears.
 - Step 6** Click **Choose** to select the directory where you want the application to be installed. Alternatively, you can enter the path manually.
 - Step 7** (Optional) Click **Restore Default Folder** if you want to revert to the default directory.
 - Step 8** Click **Next**.
 - Step 9** The Pre-Installation Summary screen appears.
 - Step 10** Click **Install**.
After the installation is complete, the Install Complete screen appears.
 - Step 11** Click **Done** to complete the installation task.
Navigate to directory that you selected during the installation, and verify that the Smart+Connected PS(scps) directory has been created.
The parent directory that contains this scps directory will be referred to as `<PS_INSTALL_DIRECTORY>` in the subsequent sections of this document.
-

Send documentation comments to scc-docfeedback@cisco.com

Configuring Audio Notification to the Cisco IP Phone

The audio notification is configured to unicast an audio message to the Cisco IP phone, five minutes before the scheduled check out time. This message reminds an end-user that an automatic check out would be done in five minutes.

To configure the audio notification to the Cisco IP phone, you have to make a change in the application server on which PS is deployed. Change the `/etc/hosts` file by moving the assigned IP address of the machine before the local loopback address.

For example,

```
10.255.255.254      SCC-BGL04-DV-123
127.0.0.1          SCC-BGL04-DV-123 localhost.localdomain localhost
::1               localhost6.localdomain6 localhost6
```

Configuring the Database

- [Requirements, page 2-4](#)
- [About the Database Scripts, page 2-5](#)
- [Executing the Database Scripts, page 2-5](#)

Requirements

You must configure a database for the Smart+Connected PS environment. To configure the Smart+Connected PS database, verify the following requirements:

- Ensure that the Oracle Database 11g Release 2 (11.2.0.2) is installed on your database server, and is ready for use.

This document does not include information on how to set up the Oracle database. For more information, see the Oracle documentation.

- The required grants for a database schema user are as follows:
 - connect
 - create table
 - create procedure
 - create sequence
 - create trigger
 - create view
 - create job
- Ensure that the following SDP database SQL scripts are already executed:
 - `setup-sdp-base.sql`
 - `setup-sdp-types.sql`

Send documentation comments to scc-docfeedback@cisco.com

About the Database Scripts

A few database scripts are created after you install the Smart+Connected PS application. These database scripts are used to create the tables/objects that are necessary for the successful operation of the Smart+Connected PS application. Before you execute the database scripts, ensure that you are connected to the database schema, on which the database scripts are to be executed.

Executing the Database Scripts

In order to execute the SQL scripts locally, you need to have all the scripts and script related files stored on your local system.

You must execute the Smart+Connected PS database script `setup-pvo-base.sql` from the `<PS_INSTALL_DIRECTORY>/scps/scripts/oracle` directory in the system where you want to set up the database. This script creates the appropriate Smart+Connected PS database objects in the database.

Ensure that you have the 'read' permission to run the scripts. You can execute the SQL scripts using SQL*Plus, Toad, or SQL Developer.

Once the database scripts have been executed, the necessary objects are created in the database schema. The log file is also generated in the same directory that includes the script.



Note

After you execute the database scripts, you must check the log files to ensure that there are no errors logged. If the log file shows errors, then these errors must be corrected before you proceed with the installation procedure.

Creating the WebLogic Domain

After you have configured the database, you need to create a domain in the WebLogic 11g server.

To create a WebLogic domain, perform the following steps:

-
- Step 1** From the file browser, navigate to the `<WLS_INSTALL_DIRECTORY>/wlserver_10.3/common/bin` directory, and run the 'config.sh' file.
The Oracle WebLogic Configuration Wizard Welcome screen appears.
 - Step 2** Choose **Create a New WebLogic Domain**, and click **Next**.
The Select Domain Source screen appears.
 - Step 3** Choose **Generate a domain configured automatically to support the following products**, and click **Next**.
The Specify Domain Name and Location screen appears.
 - Step 4** Enter the domain name in the Domain Name field. For example, `scps`.
 - Step 5** (Optional) If you want to change the default domain location, click **Browse**, and choose a directory.
 - Step 6** Click **Next**.
The Configure Administrator Username and Password screen appears.
 - Step 7** Enter the administrator username, password, confirm password, and description. For example, `weblogic/weblogic123`.

Send documentation comments to scc-docfeedback@cisco.com

Note The password must include minimum eight characters.

Step 8 Click **Next**.

The Configure Server Start Mode and JDK screen appears. In the Configure Server Start Mode and JDK screen, do the following:

- a. Under WebLogic Domain Startup Mode, choose **Production Mode**.
- b. Under Available JDKs, choose Sun SDK 1.6.0_24.



Note Ensure that the JDK version 1.6.0_24 is set.

Step 9 Click **Next**.

The Select Optional Configuration screen appears.

Step 10 Select the Administration Server check box and click **Next**.

The Configure the Administration Server screen appears.

Step 11 Enter the port number (for example, 8001) in the Listen port field.

Note The Listen Port value is the port number specified when you launch the Smart+Connected PS application. This port number should not be identical to that specified for SDP in an environment, where both the SDP and the Smart+Connected PS applications are installed on the same server.

Step 12 (Optional) If you want to configure the secured URL, select the **SSL enabled** check box, and provide a unique port number (for example, 9001) in the SSL listen port field.

Note You can also configure the secured URL later. For more information, see the [“Configuring the Secured URL” section on page 2-20](#).

Step 13 Click **Next**.

The Configuration Summary screen appears.

Step 14 Review the details and then click **Create**.

A new WebLogic domain is created according to the specified specifications.

Step 15 Click **Done** to complete the installation.

Note You can navigate to `<WLS_INSTALL_DIRECTORY>/user_projects/domains` and verify that the domain has been successfully created.

Send documentation comments to scc-docfeedback@cisco.com

Extending the WebLogic Domain

After you have created the WebLogic domain, you must extend the existing WebLogic domain for the Smart+Connected PS application server in your configuration. You can use the SDP domain template that is available at `<PS_INSTALL_DIRECTORY>/scps/template/11g` to extend the WebLogic.

Ensure that you have the database connection SID, username and password before you proceed with this procedure.

To extend the WebLogic domain for the Smart+Connected PS, perform the following steps:

-
- Step 1** From the file browser, navigate to the `<WLS_INSTALL_DIRECTORY>/wlserver_10.3/common/bin` directory, and run the 'config.sh' file.
- The Oracle WebLogic Configuration Wizard Welcome screen appears.
- Step 2** Choose **Extend an Existing WebLogic Domain**, and click **Next**.
- The Select a WebLogic Domain Directory screen appears.
- Step 3** Navigate to the WebLogic domain directory that you had created for Smart+Connected PS (for example, `scps` as per the example in this document) and click **Next**.
- The Select Extension Source screen appears.
- Step 4** Choose **Extend my domain using an existing extension template**, enter the path or navigate to the domain template through `<PS_INSTALL_DIRECTORY>/scps/template/11g`, and select the `sdp11gdomain.jar` file.
- Step 5** Click **OK**, and click **Next**.
- The Configure JDBC Components Schema screen appears.
- Step 6** Select the **SDP Datasource** check box to enable the fields in the upper pane.
- From the Vendor drop-down list, choose **Oracle**.
 - From the **Driver** drop-down list, choose ***Oracle's Driver (Thin) for Instant Connections: Versions: 9.0.1 and later**.
 - In the Schema Owner field, enter the schema username.
 - In the Schema Password field, enter the schema password.
 - In the DBMS/Service field, enter the SID of the database.
 - In the Host Name field, enter the database IP address or the DNS hostname of the database server.
 - In the Port field, enter the database port number. The default port number is 1521. Enter the appropriate port number if it is not the default port number.
- Step 7** Click **Next**.
- The Test JDBC Component Schema screen appears.
- Step 8** The Data Source Connection should be tested to confirm whether the values that has been specified in the JDBC Component Schema screen are accurate.
- Step 9** Select the **SDP Datasource component schema** check box, and click **Test Connections**.
- The test results appear in the Connection Result log.
- Step 10** If the test is successful, click **Next**.

Send documentation comments to scc-docfeedback@cisco.com



Note If the test is unsuccessful, then click Previous to navigate to the Configure JDBC Component Schema screen and verify the configuration information, and ensure that the data is accurate. If not, then enter the accurate data and repeat from Step 6 to step 10.

The Select Optional Configuration screen appears.

Step 11 Click **Next**.

The configuration Summary screen appears.

Step 12 Ensure that **Deployment** is chosen from the Summary View drop-down list and verify the specified values in the Details pane.

Step 13 Click **Extend**.

The Extending Domain screen appears.

Step 14 Click **Done** to complete the WebLogic domain extension.

Starting the WebLogic Server

To start the WebLogic server, perform the following steps:

-
- Step 1** Open a terminal and navigate to `<WLS_INSTALL_DIRECTORY>/user_projects/domains/<your domain>/bin/`.
 - Step 2** Enter the `./startWebLogic.sh` command.
 - Step 3** If prompted, enter the username and password that you specified when you created the WebLogic domain. For example, `weblogic/weblogic`
 - Step 4** Verify that the WebLogic Server has started.
-

Configuring the Java Message Service (JMS)

Ensure that the WebLogic Administration server is up and running prior to configuring the JMS.

To configure the JMS, perform the following steps:

-
- Step 1** In the Address field of the Web browser, enter `http://host:port/console`.
Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic application server has been set up and 'port' is the WebLogic server port configured during the creation of the domain.
The WebLogic Administration Console login page appears.
 - Step 2** Enter the WebLogic console username and password, and click **Login**.
The WebLogic home page appears.
 - Step 3** Under Domain Structure, click **JMS Modules**, and click **SDPSystemModule-0**.
The SDPSystemModule-0 settings appear.

Send documentation comments to scc-docfeedback@cisco.com

- Step 4** Click **Lock & Edit**.
- Step 5** Click **New** and select the **Connection Factory** option. Click **Next**.
- Step 6** Enter the Connection Factory name as **ipsConnectionFactory** and the JNDI name as **jms/ipsConnectionFactory** in the corresponding fields, click **Next**, and then click **Finish**.
The Connection Factory is created.
- Step 7** Click **New**, select **Queue**, and then click **Next**.
- Step 8** Enter the Queue name as **ipsQueue** and the JNDI name as **jms/ipsQueue** in the corresponding fields, and then click **Next**.
- Step 9** Click **Create a new Subdeployment**, enter the Subdeployment name as **ipsQueueSubdeployment**, and then click **OK**.
The subdeployment is created.
- Step 10** In the Targets field, select the SDPJMS Server, and click **Finish**.
- Step 11** Click **Activate Changes** to activate the changes.
-

Setting Up the BIRT Engine

The Smart+Connected PS application uses the BIRT runtime reporting engine to generate reports and charts. Therefore, you must set up the BIRT engine after installing the Smart+Connected PS installation. The BIRT runtime reporting engine is automatically installed while installing the Smart+Connected PS.

To set up the BIRT engine, perform the following steps:

- Step 1** From the `<PS_INSTALL_DIRECTORY>/scps/resources/` directory, copy the BIRT runtime directory 'birt-runtime-2_5_2' to a home directory or any other location.



Note If you copy the directory to a location other than the home directory, you must update the path in the BirtConfig.properties file available in the scps.war file.

- Step 2** In a file browser, navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/scps.war` file and double-click this file to open the Archive Manager screen.
- Step 3** Navigate to `/WEB-INF/classes`.
- Step 4** Select 'BirtConfig.properties' and click **Extract**.
You can extract it to a suitable location, such as Desktop.
- Step 5** Open the BirtConfig.properties file from the extracted location, in an edit mode and update the directory path as follows:
`EngineHome=/path where the BIRT runtime directory is copied/birt-runtime-2_5_2/birt-runtime-2_5_2/ReportEngine`
- Step 6** Save and close the file.
- Step 7** Navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/scps.war` file and open the Archive Manager screen.

Send documentation comments to scc-docfeedback@cisco.com

Step 8 Navigate to /WEB-INF/classes and Click **Add**. Browse and select the updated ‘BirtConfig.properties’ file, and click OK.

This replaces the updated file in the scps.war file. Verify that the date and time for the ‘BirtConfig.properties’ file is updated to the current date and time.

Configuring Logging

To configure the logging, perform the following steps:

Step 1 Create the ‘SCPS_Log’ directory in the `<PS_INSTALL_DIRECTORY>` and provide the read and write access to the user, who will run the WLS domain.

Step 2 Navigate to the `<PS_INSTALL_DIRECTORY>/scps/resources` directory and open the logging.properties file in a Text Editor.

Step 3 Search for the line starting with the following text:

```
java.util.logging.FileHandler.pattern.
```

Step 4 Replace this text with the following text:

```
java.util.logging.FileHandler.pattern =
/<PS_INSTALL_DIRECTORY>/SCPS_Log/SCPS_LogInfo-%u.log
```



Note By default, the logging level is set to SEVERE for the modules and can be customized as per your requirements.

Step 5 Save the ‘logging.properties’ file.

About Properties Files

- [About the LDAP Properties File, page 2-10](#)
- [About the JMS Properties File, page 2-12](#)
- [About the Reservation Properties File, page 2-13](#)
- [About the Notificationservice Properties File, page 2-15](#)

About the LDAP Properties File

The SDP and Smart+Connected PS applications features an external properties file ‘LDAP.properties’ to support LDAP. This file is available at: `<PS_INSTALL_DIRECTORY>/scps/resources`. Based on your existing LDAP setup, you can define the values for the various properties in this properties file. The list of properties is predefined and these properties are utilized for user authentication and user information search.

Send documentation comments to scc-docfeedback@cisco.com

Table 2-1 displays the predefined properties and the descriptions for each of the properties. These values must be applied in the properties file and these values should match those of the LDAP.

Table 2-1 LDAP Properties

Property Name	Description	Value
ldap.host.name	The hostname of the LDAP server.	IP address or DNS name of the LDAP server
ldap.host.port	The port number of the LDAP server.	389
ldap.users.DN	The base DN to be used for doing a LDAP search.	–
ldap.user.fullname	The attribute to identify the full name of the user.	displayName
ldap.user.firstname	The attribute to identify the first name of the user.	givenName
ldap.user.firstname.defaultvalue	The default value to be used if the attribute for first name is invalid.	–
ldap.user.lastname	The attribute to identify the last name of the user.	sn
ldap.user.lastname.defaultvalue	The default value to be used if the attribute for the last name is invalid.	–
ldap.user.id	The attribute to identify a user. For Active Directory, the value is cn. For the Open LDAP directory, the value is uid.	<ul style="list-style-type: none"> • For the Active Directory—cn • For the Open LDAP directory—uid
ldap.user.designation	The attribute to identify the title of the user.	title
ldap.user.businessUnit	The attribute to identify the business unit.	description
ldap.user.email	The attribute to identify the e-mail ID of the user.	mail
ldap.user.email.defaultvalue	The default value to be used if the attribute for the e-mail ID is invalid.	–
ldap.user.mobile	The attribute to identify the mobile number of the user.	mobile
ldap.user.telephoneNumber	The attribute to identify the telephone number of the user, such as office phone number, and so on.	telephoneNumber
ldap.user.companyname	The attribute to identify the company name of the user.	companyName
ldap.user.companyname.defaultvalue	The default value to be used if the attribute for the company name is invalid.	–
ldap.user.photo	The attribute to identify the image of the user.	<ul style="list-style-type: none"> • For the Active Directory—thumbnailPhoto • For the Open LDAP directory—jpegPhoto
ldapUrl	The attribute to provide the LDAP URL.	http://<IP Address of the LDAP host>:389
ldapBase	The attribute to provide the LDAP user base.	–

Send documentation comments to scc-docfeedback@cisco.com

Table 2-1 LDAP Properties (continued)

Property Name	Description	Value
ldapUserName	The attribute to provide the connection name.	–
ldapPassword	The attribute to provide the password for the LDAP authentication.	–

About the JMS Properties File

Table 2-2 displays the predefined properties, description, and sample values for each of the properties in the pvoJms.properties file. This file is available at: `<PS_INSTALL_DIRECTORY>/scps/resources`. These values must be applied in this properties file.

Table 2-2 JMS Properties

Property Name	Description	Sample Value
ips.jms.jndi	This attribute identifies the JNDI name for the ips queue.	jms/ipsQueue ¹
ips.jms.connectionfactory	This attribute identifies the Connection factory for the ips queue.	jms/ipsConnectionFactory ¹
ips.jms.initialContext	This attribute identifies the Smart+Connected PS initial context url.	weblogic.jndi.WLInitialContextFactory ¹
URL	This attribute identifies the SDP topic URL.	t3://localhost:7001
username	The attribute identifies the SDP domain username.	weblogic
password	The attribute identifies the SDP domain password.	weblogic
providerurl	The attribute identifies the Smart+Connected PS Queue URL.	t3://localhost:8001
provideruserName	The attribute identifies the scps domain admin username.	weblogic
providerpassword	The attribute identifies the scps domain admin password.	weblogic

1. This property value should not be changed.

Send documentation comments to scc-docfeedback@cisco.com

About the Reservation Properties File

Table 2-3 describes the reservation.properties and the default value for each property.

Table 2-3 Reservation Properties

Property	Description	Default Value
triggertimeforpushtophone	The trigger time (in milliseconds) to push the audio and messages to the Cisco IP Phone.	300000
triggertimeforautocancel	The trigger time (in milliseconds) to trigger an auto cancel.	900000
autocancelflag	Determines whether the automatic cancellation should happen at the trigger time or not. If an autocancelflag is positive, then the auto cancelling occurs for the time configured in the triggertime for autocancel. If autocancelflag is negative and the booking period is for X hours, then the auto cancelling process occurs after X hours.	1
autocancel	The auto cancel time in minutes. Automatic cancellation of the reservation happens when user does not check-in before the trigger time.	15
gracetimeforcheckin	Allows you to check in to a workspace prior to the reserved time. The grace time is in minutes.	15
advancebookingstatus	Allows you to book a workspace in advance if the value is true.	true
advancebookingmaxday	Represents the maximum number of days for which a booking in advance is allowed.	10
repeatbookingstatus	Allows you to book for multiple days if the value is true. This is dependent on the advance booking status.	true
repeatbookingmaxday	Defines the maximum number of days for which you can book for multiple days. This is dependent on the advancebookingmaxday property.	10
iecDefaultURL	Defines the path for the displaying the PS application Sign Out page.	/digital-signage-end.html
signageWelcomePage	Defines the path for the displaying the PS application Welcome page.	/digital-signage-welcome.html
signageLayoutPage	Defines the path for the displaying the users layout content.	/getPage.ip?id=

Send documentation comments to scc-docfeedback@cisco.com

Table 2-3 Reservation Properties (continued)

Property	Description	Default Value
iecRefreshInterval	Defines the duration by which the content gets refreshed.	10000
minbookingduration	Defines the duration by which the workspace can be available. This duration is in minutes.	15
hostname	The value for hostname should be changed to the IP address of the Smart+Connected PS host.	localhost
port	The value for port should be changed to the value of the listen port configured while creating the Smart+Connected PS domain.	The port number that you have configured for launching the Smart+Connected PS application.
appURL	Defines the application URL for the IEC device to display the layout contents.	http://<host>:<port>/ips app Where, 'host' is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the port number that you have defined for the WebLogic administration server.



Note

If you deploy the application in a cluster setup, the hostname and the port will refer to the proxy hostname and the port or the load balancer hostname or port.

[Send documentation comments to scc-docfeedback@cisco.com](mailto:scc-docfeedback@cisco.com)

About the Notificationservice Properties File

Table 2-4 describes the notificationservice.properties and the default value of each property.

Table 2-4 Notificationservice Properties

Field	Description	Sample Value
system_admin_address	This attribute defines the e-mail address of the Smart+Connected PS system administrator, who notifies the events such as location, delete, and create to the respective administrators.	somebody@example.com
admin_address	This attribute defines the e-mail address of the Smart+Connected administrator, who is notified about the events by the super administrator.	abc@example.com
from_address	This attribute defines the e-mail address of the Smart+Connected PS administrator, who can notify the end-users on the reservation status.	zyz@example.com
reply_to_address	This attribute is the e-mail address of the Smart+Connected PS administrator to whom, an end-user can reply to.	nobody@example.com

Updating the Properties Files

- [Preparing the Properties File, page 2-15](#)
- [Setting Up Reservation and Notification Properties, page 2-16](#)

Preparing the Properties File

To prepare the LDAP.properties and pvoJms.properties files for the Smart+Connected PS, perform the following steps:

-
- Step 1** Navigate to the `<PS_INSTALL_DIRECTORY>/scps/resources` and open the LDAP.properties and pvoJms.properties files in a text editor.
 - Step 2** Edit the LDAP.properties file to provide the values for each of the property names as listed in [Table 2-1](#).
 - Step 3** Edit the pvoJms.properties file to provide the values for each of the property names as listed in [Table 2-2](#).
 - Step 4** Make a note of the location where you save the LDAP.properties and pvoJms.properties files. This location is used during the configuration of the Smart+Connected Weblogic domain startup script.
-

Send documentation comments to scd-docfeedback@cisco.com

Setting Up Reservation and Notification Properties

To update the reservation and notification properties files, perform the following steps:

-
- Step 1** In a file browser, navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/scps.war` file and double-click this file to open the Archive Manager screen.
 - Step 2** Navigate to `/WEB-INF/classes`.
 - Step 3** Select `Reservation.properties` and click **Extract**. You can extract it to a suitable location, such as the desktop.
 - Step 4** Select `notification.service.properties` and click **Extract** and extract it to a suitable location.
 - Step 5** Open the `Reservation.properties` file, which is available at the specified location, in an edit mode and update the property values as described in [Table 2-3](#).
 - Step 6** Save and close the file.
 - Step 7** Open the `notification.service.properties` file, which is available at the specified location, in an edit mode and update the property values as described in [Table 2-4](#).
 - Step 8** Save and close the file.
 - Step 9** Navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/scps.war` file and open the Archive Manager screen.
 - Step 10** Navigate to `/WEB-INF/classes` and Click **Add**.
 - Step 11** Browse and select the updated `Reservation.properties` file and click **OK**.
 - Step 12** Browse and select the updated `notification.service.properties` file and click **OK**.

This replaces the updated file in the `scps.war` file. Verify that the date and time of the `Reservation.properties` and the `notification.service.properties` files are updated to the current date and time.

Updating the WebLogic Configuration

Prior to configuring the WebLogic domain, ensure that the WebLogic domain is shut down.

To update the WebLogic domain configurations, perform the following steps:

-
- Step 1** From the file browser, navigate to the `<WLS_INSTALL_DIRECTORY>/user_projects/domains/<Your domain>/bin` directory, and open the `setDomainEnv.sh` file.
 - Step 2** In the `setDomainEnv` file, search for the following text:


```
JAVA_PROPERTIES="${JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
```
 - Step 3** Add the following text at the end of the line before the (`"`):


```
-Dcom.cisco.sdp.ldap.configfilepath=<path to ldap.properties file>/LDAP.properties
```

 For example:


```
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
```


Send documentation comments to scc-docfeedback@cisco.com

After adding the command line, the text is displayed as follows:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties"
```

Step 4 In the setDomainEnv file, search for the following text:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
```

Step 5 Add the following text at the end of the line before the ("):

```
-Dpvo_jms_props=<path to pvoJms.properties file>/pvoJms.properties
```

For example:

```
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
```

After adding the command line, the text is displayed as follows:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties/pvoJms.properties">
```

Step 6 Save the file.

Step 7 In the setDomainEnv file, search for the following text:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
```

Step 8 Add the following text at the end of the line just before ("):

```
-Djava.util.logging.config.file=<path to logging.properties>/logging.properties
```

For example:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES}-Djava.util.logging.config.file=/u01/scps/config/lo
gging.properties/logging.properties">
```

After adding the command line, the text is displayed as follows:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1-Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
-Djava.util.logging.config.file=/u01/scps/config/logging.properties"
```

Step 9 In the setDomainEnv file, search for the following text:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
```

Step 10 Append the following text at the end of the line just before ("):

```
-Dpvo_ldap_props=<path to ldap.properties file>/LDAP.properties
```

Send documentation comments to scc-docfeedback@cisco.com

For example:

```
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties
```

Step 11 After adding the text, it looks like:

```
JAVA_PROPERTIES="{JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1-Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
-Djava.util.logging.config.file=/u01/scps/config/logging.properties
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties"
```

Step 12 In the setDomainEnv file, search for the following text:

```
JAVA_OPTIONS="{JAVA_OPTIONS} {JAVA_PROPERTIES}
-Dwlv.iterativeDev=${iterativeDevFlag} -Dwlv.testConsole=${testConsoleFlag}
-Dwlv.logErrorsToConsole=${logErrorsToConsoleFlag}"
```

Step 13 Append the following text at the end of the line just before ("):

```
-Dcom.cisco.sdp.ldap.configfilepath=<path to ldap.properties file>/LDAP.properties
-Dweblogic.management.clearTextCredentialAccessEnabled=true
```

For example:

```
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dweblogic.management.clearTextCredentialAccessEnabled=true
```

Step 14 After adding the text, it looks like:

```
JAVA_OPTIONS="{JAVA_OPTIONS} {JAVA_PROPERTIES}
-Dwlv.iterativeDev=${iterativeDevFlag} -Dwlv.testConsole=${testConsoleFlag}
-Dwlv.logErrorsToConsole=${logErrorsToConsoleFlag}
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dweblogic.management.clearTextCredentialAccessEnabled=true"
```

Step 15 Save the file.

Configuring the LDAP Authentication

Ensure that the WebLogic Administration server is up and running before configuring the LDAP authentication.

To configure the LDAP authentication, perform the following steps:

Step 1 In the Address field of the Web browser, enter `http://host:port/console`.

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic application server has been set up and 'port' is the WebLogic server port configured during the creation of the domain.

The WebLogic Administration Console login page appears.

Step 2 Enter the WebLogic console username and password, and click **Login**.

The WebLogic home page appears.

Step 3 Under **Domain Structure**, click **Security Realms**.

The Summary of Security Realms page appears.

Send documentation comments to scc-docfeedback@cisco.com

- Step 4** Click **myrealm**.
The Settings for myrealm page appears.
- Step 5** Click the **Providers** tab, and click **SDP LDAP Auth Provider**.
The Settings for SDP LDAP Auth provider page appears.
- Step 6** Under **Configuration**, click **Provider Specific**.
- Step 7** Click **Lock & Edit**, and provide the following LDAP server and LDAP user details with their actual values in the corresponding text boxes:

Property	Description	Value
Configured Tenants	Defines the number of tenants you want to access. The value 0 implies multiple tenants.	0
Connection Password	The attribute to provide the password for the LDAP authentication.	<password>
Please type again To confirm	The attribute to again provide the password for confirmation.	<password>
Connection URL	The attribute to provide the LDAP URL.	http://<IP Address of the LDAP host>:389
User Base	The attribute to provide the LDAP user base.	<user base>
Authentication	Simple authentication is required.	simple
Connection Username	The attribute to provide the connection name.	<connection name>
Jndi Name	The data source jndi name. The default value is jdbc/scc.	jdbc/scc
User Search Matching	The matching search string to find the user.	<ul style="list-style-type: none"> • For the Active Directory—cn={0} • For the open LDAP directory—uid={0}

- Step 8** Click **Save**.
- Step 9** Click **Activate Changes** to activate the changes.

Send documentation comments to scc-docfeedback@cisco.com

Setting Up the Push-to-Phone Feature

To configure the IP Push-to-Phone feature for the Smart+Connected PS application, perform the following steps:

Step 1 From the file browser, navigate to the `<WLS_INSTALL_DIRECTORY>/user_projects/domains/<Your domain>/bin` directory, and open the `setDomainEnv.sh` file.

Step 2 In the `setDomainEnv` file, search for the following text:

```
JAVA_PROPERTIES="${JAVA_PROPERTIES} ${WLP_JAVA_PROPERTIES}"
```

Step 3 Add the following text at the end of the line before the (`"`):

```
-Dweblogic.net.proxyAuthenticatorClassName=java.net.Authenticator
-DUseSunHttpHandler=true
```

After adding the command line, the text is displayed as follows:

```
JAVA_PROPERTIES="${JAVA_PROPERTIES} ${WLP_JAVA_PROPERTIES}
-Dweblogic.net.proxyAuthenticatorClassName=java.net.Authenticator
-DUseSunHttpHandler=true "
```

Step 4 Save the file.

Configuring the Secured URL

To launch the Smart+Connected PS application in a secured environment, you need to configure the secured URL.

You can configure the secured URL while creating the WebLogic domain (see [“Creating the WebLogic Domain” section on page 2-5](#)). If you have not configured the secured URL while creating the WebLogic domain, perform the following steps:

Step 1 Ensure that the WebLogic Administration server is up and running.

Step 2 In the Address field of the Web browser, enter `http://host:port/console`.

Where, ‘host’ is the IP address or DNS hostname of the host on which the WebLogic application server has been set up and ‘port’ is the WebLogic server port configured during the creation of the domain.

The WebLogic Administration Console login page appears.

Step 3 Enter the WebLogic console username and password, and click **Login**.

The WebLogic home page appears.

Step 4 Under Domain Structure, click **Environment > Servers**.

The Summary of Servers area appears.

Step 5 In the Servers table, click **AdminServer(admin)**.

The Settings for AdminServer area appears.

Step 6 Click **Lock & Edit**.

Step 7 In the Settings for AdminServer area, perform the following steps:

- a. Select the **SSL Listen Port Enabled** check box.

Send documentation comments to scc-docfeedback@cisco.com

- b. In the SSL Listen Port field, provide a unique port number to be used for launching the secured URL.
- c. Click **Save**.

Step 8 Click **Activate Changes** to activate the changes.

Configuring Installer for the Mobile Devices

The Smart+Connected PS installation package comprises the following files in the MobileApps directory:

- For the Android phones—SCPS_Mobile.apk
- For the iPhones—SCPSMobileIOSNew.ipa and SCPSMobileIOSNew.plist

These files are required for configuring installer for the mobile devices.

- [Configuring Installer for the Android Phones, page 2-21](#)
- [Configuring Installer for the iPhones, page 2-23](#)

Configuring Installer for the Android Phones

To configure installer for the Android phones, perform the following steps:

Step 1 Extract the Messages.properties file:

- a. Copy the SCPS_Mobile.apk file from the MobileApps directory to a local directory.
- b. Double-click the copied SCPS_Mobile.apk file and open the Archive Manager screen.
- c. Navigate to /assets/www/resources, select the Messages.properties file, and click **Extract**.
You can extract it to a suitable location, such as Desktop.

Step 2 Update the Messages.properties file:

- a. Open the Messages.properties file from the extracted location in an edit mode and update the following values:

- secureServerURL = https://<host>:<SSL port>

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic Administration server has been set up and 'SSL port' is the port number that you have defined as the SSL listen port in the [“Configuring the Secured URL”](#) section on page 20.



Note If you have not configured the secured URL, you must provide the 'serverURL' value in the 'secureServerURL' field so that the application can be accessed in a non-secured environment.

- serverURL = http://<host>:<port>

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the port number that you have defined for the WebLogic administration server.

- b. Save and close the file.

Send documentation comments to scs-docfeedback@cisco.com

- Step 3** Replace the Messages.properties file in the SCPS_Mobile.apk file:
- Double-click the SCPS_Mobile.apk file from the extracted location and open the Archive Manager screen.
 - Navigate to /assets/www/resources, and click **Add**.
 - Browse and select the updated Messages.properties file, and click **OK**.
 - Close the Archive Manager screen of the SCPS_Mobile.apk file.

- Step 4** Navigate to the \$JAVA_HOME/bin directory, and enter the following command to generate a key for signing the SCPS_Mobile.apk file:

```
./keytool -genkey -v -keystore my-release-key.keystore -alias <alias name> -keyalg RSA
-keysize 2048 -validity <number of days>
```

For example:

```
./keytool -genkey -v -keystore my-release-key.keystore -alias scps -keyalg RSA -keysize
2048 -validity 10000
```

You are prompted to specify the following required details:

- Enter keystore password—Specify a password for keystore. You also need to use the same keystore password for the signing the SCPS_Mobile.apk file.
- Re-enter new password—Specify the new password again.
- What is your first and last name?—Specify the host name of the machine.
- What is the name of your organizational unit?—Specify your organizational unit.
- What is the name of your organization?—Specify your organization name.
- What is the name of your City or Locality?—Specify the name of your city.
- What is the name of your State or Province?—Specify the name of your state or province.
- What is the two-letter country code for this unit?—Specify the first two letters of your country.
- Is CN=<name>, OU=<organizational unit>, O=<organization>, L=<city>, ST=<state>, C=<country> correct?—Verify the specified values, enter ‘Yes’ if the values are correct, and press **Enter**.

The RSA key and self-signed certificate with a validity of <number of days> days is generated. You are prompted for the key password of the <alias name>. Press **Enter**.

Automatically, the keystore password is retained for the <alias name> key password.

- Step 5** Enter the following command to sign the SCPS_Mobile.apk file:

```
./jarsigner -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore
my-release-key.keystore <location of SCPS_Mobile.apk>/SCPS_Mobile.apk <alias name>
```

For example:

```
./jarsigner -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore my-release-key.keystore
/home/u01/Desktop/SCPS_Mobile.apk SCPS
```

You are prompted for the keystore password. Enter the keystore password, and press **Enter**.

The SCPS_Mobile.apk file is successfully signed.

- Step 6** Replace the SCPS_Mobile.apk file in the scps.war file:
- Double-click the scps.war file from the <SCPS_INSTALL_DIRECTORY>/scps/bin/war/ directory, and open the Archive Manager screen.

Send documentation comments to scc-docfeedback@cisco.com

- b. Navigate to /mobile_download, and click **Add**.
 - c. Browse and select the signed SCPS_Mobile.apk file, and click **OK**.
 - d. Close the Archive Manager screen of the scps.war file.
-

Configuring Installer for the iPhones

While configuring installer for the iPhones, you need to sign the SCPSMobileIOSNew.ipa file using the MAC machine. Therefore, the provisioning profile must be available in your MAC machine.

To configure installer for the iPhones, perform the following steps:

-
- Step 1** Extract the download.properties file:
- a. In a file browser, navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/scps.war` file and double-click this file to open the Archive Manager screen.
 - b. Navigate to /mobile_download, select the download.properties file, and click **Extract**.
You can extract it to a suitable location, such as Desktop.
- Step 2** Update the download.properties file:
- a. In a terminal, navigate to the directory where the download.properties file is available.
 - b. Open the download.properties file in an edit mode, and update the following line:

```
ios_url=http://<host>:<port>/ipsapp/mobile_download/SCPSMobileIOSNew.plist
```

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the port number that you have defined for the WebLogic administration server.
 - c. Save and close the file.
- Step 3** Copy the SCPSMobileIOSNew.ipa and SCPSMobileIOSNew.plist files from the MobileApps directory to your MAC machine.
- Step 4** In the MAC machine, update the SCPSMobileIOSNew.plist file:
- a. In a terminal, navigate to the directory where the SCPSMobileIOSNew.plist file is available.
 - b. Open the SCPSMobileIOSNew.plist file in an edit mode, and update the following string:

```
<string>http://<host>:<port>/ipsapp/mobile_download/SCPSMobileIOSNew.ipa</string>
```

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the port number that you have defined for the WebLogic administration server.
 - c. Save and close the file.
- Step 5** In the MAC machine, sign the SCPSMobileIOSNew.ipa file:
- a. In a terminal, navigate to the directory where the SCPSMobileIOSNew.ipa file is available.
 - b. Unzip the SCPSMobileIOSNew.ipa file by entering the following command:

```
unzip SCPSMobileIOSNew.ipa
```
 - c. Remove the existing signature by entering the following command:

Send documentation comments to scc-docfeedback@cisco.com

```
rm -rf Payload/SCPSMobileIOSNew.app/_CodeSignature
```

- d. Open the Messages.properties file in an edit mode using the following command:

```
vi Payload/SCPSMobileIOSNew.app/www/resources/Messages.properties
```

- e. Update the following values:

- secureServerURL = https://<host>:<SSL port>

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic Administration server has been set up and 'SSL port' is the port number that you have defined as the SSL listen port in the "Configuring the Secured URL" section on page 20.



Note If you have not configured the secured URL, you must provide the 'serverURL' value in the 'secureServerURL' field so that the application can be accessed in a non-secured environment.

- serverURL = http://<host>:<port>

Where, 'host' is the IP address or DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the port number that you have defined for the WebLogic administration server.

- f. Save and close the file.
- g. Copy the available provisioning profile (.mobileprovision file) to Payload/SCPSMobileIOSNew.app/ directory and name it as 'embedded.mobileprovision'.
- h. Enter the following command:

```
/usr/bin/codesign -f -s "iPhone Distribution: <distribution name>" --resource-rules "Payload/SCPSMobileIOSNew.app/ResourceRules.plist" "Payload/SCPSMobileIOSNew.app"
```

Where <distribution name> is the distribution license name.

- i. Zip the SCPSMobileIOSNew.ipa file by entering the following command:

```
zip -r SCPSMobileIOSNew.ipa Payload
```

Step 6 Copy the updated SCPSMobileIOSNew.ipa and SCPSMobileIOSNew.plist files from the MAC machine to the machine where the Smart+Connected PS application is installed.

Step 7 Replace the download.properties, SCPSMobileIOSNew.ipa, and SCPSMobileIOSNew.plist files in the scps.war file:

- a. Double-click the scps.war file from the <SCPS_INSTALL_DIRECTORY>/scps/bin/war/ directory, and open the Archive Manager screen.
- b. Navigate to /mobile_download, and click **Add**.
- c. Browse and select the updated download.properties, signed SCPSMobileIOSNew.ipa, and SCPSMobileIOSNew.plist files, and click **OK**.
- d. Close the Archive Manager screen of the scps.war file.

Send documentation comments to scc-docfeedback@cisco.com

Deploying Apache Jackrabbit

The Apache Jackrabbit server is an open source content repository for the Java platform, and the Smart+Connected PS application uses the Apache Jackrabbit to store content.

To deploy the Apache Jackrabbit server, perform the following steps:

-
- Step 1** In a file browser, navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/jackrabbit.war` file, and double-click this file to open the Archive Manager screen.
 - Step 2** Navigate to `/WEB-INF/lib`, select the `jcr-2.0.jar` file, and extract the file to the following location:
`<WLS_INSTALL_DIRECTORY>/user_projects/domains/<your domain>/lib`
 - Step 3** Close the Archive Manager screen.
 - Step 4** From the file browser, navigate to the `<WLS_INSTALL_DIRECTORY>/user_projects/domains/<your domain>/bin` directory, and run the `./startWebLogic.sh` file.
The WebLogic Administration server starts.
 - Step 5** In the address field of the Web browser, enter the URL `http://host:port/console`.
Where, 'host' is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the Administration server port.
 - Step 6** In the Oracle WebLogic Server Administration Console Login page, enter the username and password, and click **Deployments**.
 - Step 7** Click **Lock & Edit**.
 - Step 8** Select the **sdpapp** and **sdpreport** check boxes from the Deployments table, and click **Delete** to delete the SDP app and report that are created when you use the SDP domain extension template.
 - Step 9** Click **Install**.
 - Step 10** Navigate to `<PS_INSTALL_DIRECTORY>/scps/bin/war/` by either selecting the current location option or by entering path in the path field and choose the 'jackrabbit.war' file.
 - Step 11** Click **Next** twice.
 - Step 12** Click **Finish**.
 - Step 13** Change the Deployment Order to **50**, and then click **Save**.
 - Step 14** Click **Activate Changes** to activate the changes.
 - Step 15** Select the check box next to the jackrabbit entry, and from the **Start** drop-down list, select **Servicing all requests**.
 - Step 16** Verify that the application is deployed and is active.
 - Step 17** In the Address field of the browser, enter the URL `http://host:port/jackrabbit`, and click **Create Content Repository**.
The `<WLS_INSTALL_DIRECTORY>/user_projects/domains/<your domain>/jackrabbit` directory repository structure is created.
-

Send documentation comments to scc-docfeedback@cisco.com

Deploying the Smart+Connected PS Application

To deploy the Smart+Connected PS application, perform the following steps:

-
- Step 1** In the address field of the Web browser, enter the URL `http://host:port/console`.
Where, 'host' is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the Administration server port.
 - Step 2** In the Oracle WebLogic Server Administration Console Login page, enter the username and password
 - Step 3** In the WebLogic Home page, under **Domain Structure**, click **Deployments**.
 - Step 4** Click **Lock and Edit**.
 - Step 5** Click **Install**.
 - Step 6** Navigate to `<PS_INSTALL_DIRECTORY>/scps/bin/war/` by either selecting the current location option or by entering path in the path field.
 - Step 7** Select the `scps.war` radio button, and click **Next**.
 - Step 8** Keep the default selection **Install this deployment as an application**, and click **Next**.
 - Step 9** Click **Finish and Save** to complete the deployment.
 - Step 10** Click **Activate Changes** to activate the changes.
 - Step 11** Select the check box next to the SCPS entry, and from the **Start** drop-down list, select **Servicing all requests**.
 - Step 12** Verify that the application is deployed and is active.
-

Importing SSL Certificates

You must import SSL certificate for the Cisco Unified Communications Manager (CUCM). You may require to import SSL certificate for the Cisco Digital Media Player (DMP) and Microsoft Exchange Server.

Before you begin importing SSL certificates, ensure that you obtain the certificates from CUCM, DMP, and Exchange Server, and store the certificates in a directory on the application server.

To import SSL certificates, perform the following steps:

-
- Step 1** Open a terminal and navigate to the `$JAVA_HOME/bin` directory.
 - Step 2** Enter the following command:


```
./keytool -import -alias <Alias Name> -file <Certificate file name with complete path>
-keystore <WLS_INSTALL_DIRECTORY>/wlserver_10.3/server/lib/DemoTrust.jks -storepass
DemoTrustKeyStorePassPhrase
```

where `<Certificate file name with complete path>` is the certificate file name with a complete directory path where you store your certificates and the `<Alias Name>` is the unique alias name provided to the certificate.

For example:

Send documentation comments to scc-docfeedback@cisco.com

```
./keytool -import -alias CUCM -file /u01/scps/config/CUCM.cer -keystore  
/u01/bea/wlserver_10.3/server/lib/DemoTrust.jks -storepass DemoTrustKeyStorePassPhrase
```

A message prompts you to trust this certificate.

Step 3 Choose **Yes**, and press **Enter**.

The certificates are imported.

Step 4 In the `setDomainEnv.sh` file in the WebLogic domain directory, append the `JAVA_PROPERTIES` line with the following line:

```
-Djavax.net.ssl.trustStore=<WLS_INSTALL_DIRECTORY>/wlserver_10.3/server/lib/DemoTrust.  
jks -Djavax.net.ssl.trustStorePassword=DemoTrustKeyStorePassPhrase
```

For example:

```
-Djavax.net.ssl.trustStore=/u01/bea/wlserver_10.3/server/lib/DemoTrust.jks  
-Djavax.net.ssl.trustStorePassword=DemoTrustKeyStorePassPhrase
```



Note You must restart the WebLogic server after importing the certificates.

Restarting the WebLogic Server

You can restart the WebLogic server after making changes through the WebLogic console or performing any configuration updates.

To restart the WebLogic server, perform the following steps:

Step 1 Open a terminal and navigate to the following directory:

```
<WLS_INSTALL_DIRECTORY>/user_projects/domains/<your_domain>/bin directory.
```

Step 2 Stop the WebLogic server using the following the command:

```
./stopWebLogic.sh
```

Step 3 When the WebLogic server is stopped and the prompt returns, start the WebLogic server using the following command:

```
./startWebLogic.sh
```

Step 4 If prompted, enter the username and password that you specified when you created the WebLogic domain. For example, `weblogic/weblogic`

The WebLogic server is restarted.

Accessing the Application and Verifying the Installation

To access the Smart+Connected PS application and to verify the installation, perform the following steps:

Send documentation comments to scc-docfeedback@cisco.com

Step 1 In the Address field of a Web browser, type one of the following application server URLs, and press **Enter**:

- <http://<host>:<port>/ipsapp>—To access the application in a non-secured environment.
Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘port’ is the port number that you have defined for the WebLogic administration server.
- <https://<host>:<SSL port>/ipsapp>—To access the application in a secured environment.
Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘SSL port’ is the port number that you have defined as the SSL listen port.

Step 2 Enter the username and password for the Smart+Connected PS application.

The Smart+Connected PS login page appears.

Step 3 Enter the username and password for the Smart+Connected PS application, and click **Login**.

Your default login credentials are:

- Username—superadmin
- Password—superadmin

You can change your password by logging in to the SDP application. You can also create additional users by using the SDP application. For more information on how to assign roles and permissions to users in the SDP application, see the *Cisco Service Delivery Platform Administrator Guide*.

For more information on how to use the Smart+Connected PS features, see the *Cisco Smart+Connected Personalized Spaces User Guide*.

Installing on a Cluster Server Setup

- [About Clustering, page 2-29](#)
- [Installing the Application, page 2-30](#)
- [Configuring Audio Notification to the Cisco IP Phone, page 2-30](#)
- [Configuring the Smart+Connected PS Database, page 2-30](#)
- [Setting Up Managed Server, page 2-31](#)
- [Configuring the Proxy/Administration Server, page 2-34](#)
- [Configuring the Secured URL, page 2-42](#)
- [Configuring Installer for the Mobile Devices, page 2-42](#)
- [Deploying Apache Jackrabbit, page 2-46](#)
- [Deploying the Smart+Connected PS Application, page 2-47](#)
- [Starting Servers, page 2-47](#)
- [Configuring Jackrabbit Repository for Clustering, page 2-49](#)
- [Accessing the Application and Verifying the Installation, page 2-51](#)

Send documentation comments to scc-docfeedback@cisco.com

About Clustering

A WebLogic server cluster consists of multiple WebLogic server instances running simultaneously and working together to provide increased scalability, reliability, and high availability. A cluster appears to clients to be a single WebLogic server instance. The server instances that constitute a cluster can run on the same machine or are usually located on different machines. You can increase a cluster's capacity by adding additional server instances to the cluster on an existing machine or on different machines. Each server instance in a cluster must run on the same WebLogic version.

An example of clustered deployment in a distributed environment is discussed in this document (see [Table 2-4](#)). In this example scenario:

- The database is non-clustered.
- The application servers are clustered.
- Three virtual machines host the application servers.
- One of the virtual machine hosts the admin server and a proxy server. This proxy server acts as a software load balancer.
- The application is deployed on two machines, Machine 1 and Machine 2, which have two managed servers.

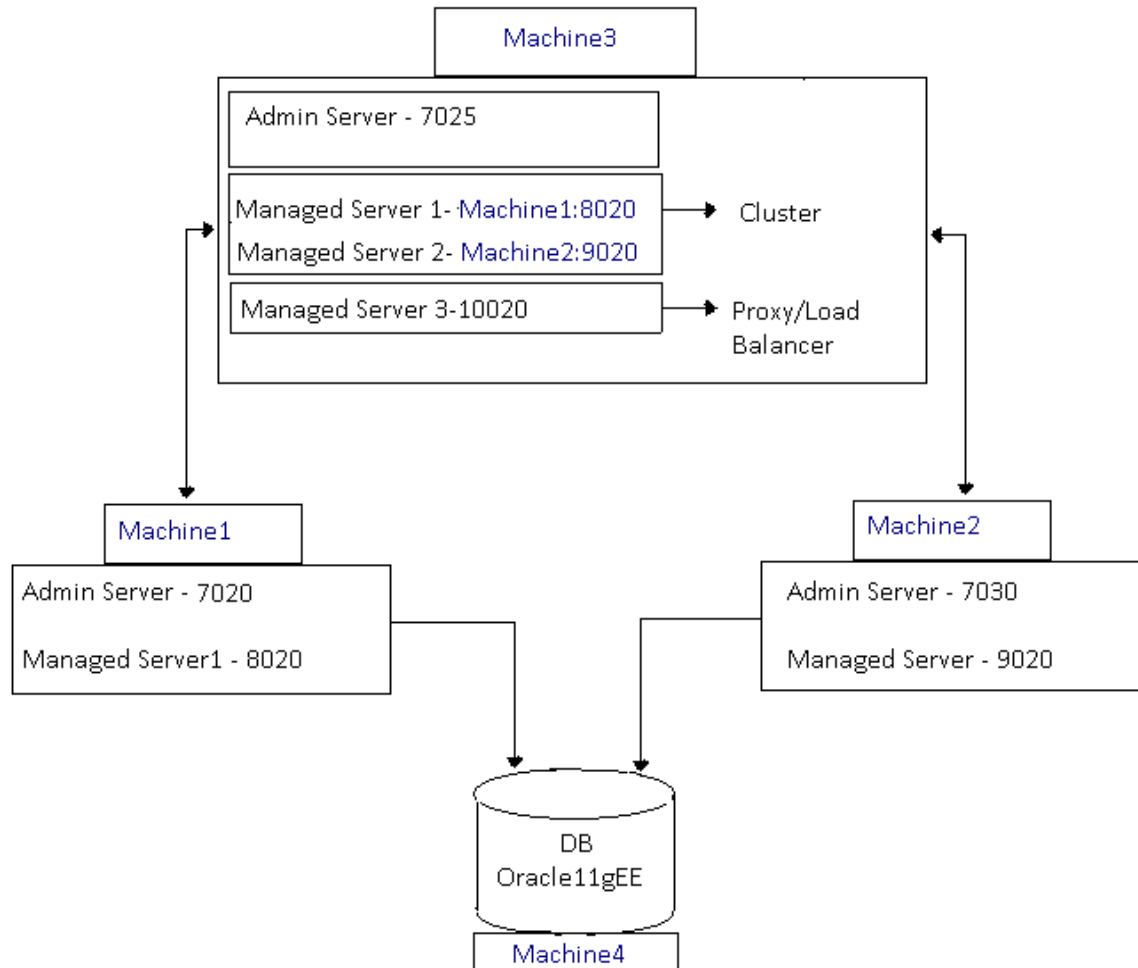
You can modify this setup based on your requirement (number of managed servers, port numbers, and so on).

The requirements for the clustered deployment in this example, includes the following:

- Machine 1: WebLogic Managed Server 1 (WebLogic 10.3.5)
- Machine 2: WebLogic Managed Server 2 (WebLogic 10.3.5)
- Machine 3: WebLogic Admin Server and HTTP Proxy Server (WebLogic 10.3.5)
- Machine 4: Database Server (Oracle Database 11g)

Send documentation comments to scc-docfeedback@cisco.com

Figure 2-1 Example of a Clustering Setup



Installing the Application

For information on how to install the Smart+Connected PS application on the admin and managed nodes, see the [“Installing the Application”](#) section on page 2-3.

Configuring Audio Notification to the Cisco IP Phone

For information on how to configure the audio notification to the Cisco IP phone, see the [“Configuring Audio Notification to the Cisco IP Phone”](#) section on page 2-4.

Configuring the Smart+Connected PS Database

For information on how to configure the Smart+Connected PS database, see the [“Configuring the Database”](#) section on page 2-4.

[Send documentation comments to scc-docfeedback@cisco.com](mailto:scc-docfeedback@cisco.com)



Setting Up Managed Server

This section explains the configurations that are required to set up one managed server. In order to complete the setup, the same configurations must be performed on all the other managed servers.

- [Creating a New WebLogic Domain for a Managed Server, page 2-31](#)
- [Extending the WebLogic Domain for a Managed Server, page 2-32](#)
- [Setting JMS Configuration, page 2-32](#)
- [Setting Up the BIRT Engine, page 2-33](#)
- [Configuring Logging, page 2-33](#)
- [Setting Up the Push-to-Phone Feature, page 2-34](#)

Creating a New WebLogic Domain for a Managed Server

To create a WebLogic domain for managed servers on a machine, perform the following steps:

-
- Step 1** Log in to the machine where you want to create a WebLogic domain.
- Step 2** Open a terminal and navigate to `<WLS_INSTALL_DIRECTORY>/wlserver_10.3/common/bin` and run the `config.sh` file.
- The Configuration Wizard screen appears.
- Step 3** Choose the **Create a new WebLogic domain** radio button, and click **Next**.
- The Select Domain Source screen appears.
- Step 4** Select the **Generate a domain configured automatically to support the following products** radio button, and click **Next**.
- The Specify Domain Name and Location screen appears.
- Step 5** Enter the domain name in the Domain Name field. For example, `scps`.
- Step 6** (Optional) If you want to change the default domain location, click **Browse**, and choose a directory.
- Step 7** Click **Next**.
- The Configure Administrator Username and Password screen appears.
- Step 8** Enter the administrator username, password, confirm password, and description. For example, `weblogic/weblogic123`.
-  **Note** The password must include minimum eight characters.
-
- Step 9** Click **Next**.
- The Configure Server Start Mode and JDK screen appears. In the Configure Server Start Mode and JDK screen, do the following:
- Under WebLogic Domain Startup Mode, choose **Production Mode**.
 - Under Available JDKs, choose `Sun SDK 1.6.0_24`.
-  **Note** Ensure that the JDK version `1.6.0_24` is set.
-

Send documentation comments to scc-docfeedback@cisco.com

Step 10 Click **Next**.

The Select Optional Configuration screen appears.

Step 11 Select the **Managed Servers, Clusters and Machines** check box, and click **Next**.

The Configure Managed Server screen appears.

Step 12 To add the managed server, do the following:

a. In the Configure Managed Servers screen, click **Add** from the top left corner of the page.

A row for the new managed server appears.

b. Enter the name of the managed server, such as MS1 in the **Name** field.



Note When you configure managed server names for Machine 1 and 2, make sure that the managed server names are unique. For example, MS1 for Machine 1 and MS2 for Machine 2.

c. Enter the IP address of the Managed Server (MS1) in the Listen address field.

d. Enter the port number in the **Listen Port** field.



Note You can use Listen Port 8020 for Machine 1 and 9020 for Machine 2.

Step 13 Click **Next**.

The Configure Clusters screen appears.

Step 14 Click **Next**.

The Configure Machines screen appears.

Step 15 Click **Next**.

The Configuration Summary screen appears.

Step 16 Review the summary, and click **Create**.

A new WebLogic domain is created according to your specifications.

Step 17 Click **Done** to complete the installation.

After creating the WebLogic domain, you can navigate to `<WLS_INSTALL_DIRECTORY>/user_projects/domains`, and verify that the domain has been created successfully. If you have specified a different location for the domain, navigate to that location to verify that the domain has been created successfully.

Extending the WebLogic Domain for a Managed Server

For information on how to extend the WebLogic Domain for a managed server, see the [Extending the WebLogic Domain, page 2-7](#).

Setting JMS Configuration

- [Updating the JMS Properties File, page 2-33](#)
- [Updating the WebLogic Configuration, page 2-33](#)

Send documentation comments to scc-docfeedback@cisco.com

Updating the JMS Properties File

To update the properties file, perform the following steps:

-
- Step 1** In a file browser, navigate to the `<PS_INSTALL_DIRECTORY>/scps/resorces` directory, and open the 'pvoJms.properties' file.
- Step 2** Edit the 'pvoJms.properties' file as follows:
- Update **URL** to **t3://<SDP Appserver IP Address or Hostname>:<SDP Appserver port number>**
 - Update **userName** to **<SDP weblogic console user name>**
 - Update **password** to **<SDP weblogic console password>**
 - Update **providerurl** to **t3://<Admin server IP Address or Hostname>:<Admin server port number>**
 - Update **provideruserName** to **<Admin server weblogic console user name>**
 - Update **providerpassword** to **<Admin server weblogic console password>**
- For example:
- URL=t3://SDPServer1:7001
 - userName=weblogic
 - password=weblogic
 - providerurl=t3://AdminServer1:8001
 - provideruserName=weblogic
 - providerpassword=weblogic123
- Step 3** Save and close the file.
- Make a note of the location where you save the 'pvoJms.properties' file. This location is used for setting up the run parameters in the WebLogic startup script.
-

Updating the WebLogic Configuration

For information on how to add configurations to the WebLogic server, please see the [“Updating the WebLogic Configuration”](#) section on page 2-16.

Setting Up the BIRT Engine

For information on how to configure the BIRT engine, see the [“Setting Up the BIRT Engine”](#) section on page 2-9.

Configuring Logging

For information on how to configure the log file, see the [“Configuring Logging”](#) section on page 2-10.

Send documentation comments to scc-docfeedback@cisco.com

Setting Up the Push-to-Phone Feature

For information on how to set up the Push-to-Phone feature, see the “Setting Up the Push-to-Phone Feature” section on page 2-20.

Configuring the Proxy/Administration Server

- [Setting Up the Proxy/Administration Server, page 2-34](#)
- [Starting the WebLogic Server, page 2-36](#)
- [Configuring the Cluster, page 2-36](#)

Setting Up the Proxy/Administration Server

You need to set up the proxy/administration server, so that the application can be accessed from other machines.

To set up the proxy/administration server, perform the following steps:

-
- Step 1** Log in to Machine 3 where you want to create admin/proxy server.
- Step 2** Navigate to `<WLS_INSTALL_DIRECTORY>/wlserver_10.3/common/bin` and run the `config.sh` file. The Configuration Wizard screen appears.
- Step 3** Choose **Create a new WebLogic domain** and click **Next**. The Select Domain Source screen appears.
- Step 4** Select **Generate a domain configured automatically to support the following products** and click **Next**. The Specify Domain Name and Location screen appears.
- Step 5** Enter the domain name in the Domain Name field. For example, `scps`.
- Step 6** (Optional) If you want to change the default domain location, click **Browse**, and choose a directory.
- Step 7** Click **Next**. The Configure Administrator Username and Password screen appears.
- Step 8** Enter the administrator username, password, confirm password, and description. For example, `weblogic/weblogic123`.



Note The password must include minimum eight characters.

- Step 9** Click **Next**. The Configure Server Start Mode and JDK screen appears. In the Configure Server Start Mode and JDK screen, do the following:
- Under WebLogic Domain Startup Mode, choose **Production Mode**.
 - Under Available JDKs, choose Sun SDK 1.6.0_24.



Note Ensure that the JDK version 1.6.0_24 is set.

Send documentation comments to scc-docfeedback@cisco.com

Step 10 Click **Next**.

The Select Optional Configuration screen appears.

Step 11 Select the following check boxes, and click **Next**:

- **Administration Server**
- **Managed Servers, Clusters and Machines**

The Configure the Administration Server screen appears.

Step 12 Enter the port number (for example, 8001) in the Listen port field.



Note The Listen Port value is the port number specified when you launch the WebLogic console URL.

Step 13 Enter the administrator username, password, confirm password, and description in the corresponding fields and click **Next**.

The Configure Managed Server screen appears.

Step 14 To add the managed server, perform the following steps:

- a. On the Configure Managed Servers screen, click **Add**.

A row for the new managed server appears.

- b. Enter the name of the managed server in the Name field. For example, MS1.

- c. Enter the host IP address of the managed server 1 in the Listen address field.

- d. Enter the port number as 8020 in the Listen port field. This port number is the listen port of the managed server 1.

- e. On the Configure Managed Servers page, click **Add**.

A row for the new managed server appears.

- f. Enter the name of the managed server in the Name field. For example, MS2.

- g. Enter the host IP address of the managed server 2 in the Listen address field.

- h. Enter the port number as 9020 in the Listen port field. This port number is the listen port of the managed server 2.

- i. On the Configure Managed Servers page, click **Add**.

A row for the new managed server appears to add the proxy server.

- j. Enter the name of the managed server in the Name field. For example, MS3.

- k. Enter the host IP address of the admin/proxy server in the Listen address field.

- l. Enter the port number as 10020 in the Listen port field. This port number is the listen port of the proxy server.

Step 15 Click **Next**.

The Configure Clusters screen appears.

Step 16 Click **Add**, and do the following:

- Enter a name for the cluster (for example, scpsCluster)
- From the **Cluster messaging mode** drop-down list, select **multicast**.
- Change the multicast port (for example, 11020).

Step 17 Click **Next**.

Send documentation comments to scc-docfeedback@cisco.com

The Assign Servers to the Clusters screen appears.

Step 18 Move all the managed servers under Servers to the clusters pane. Do not move the proxy server.

Step 19 Click **Next**.

The Create HTTP Proxy Applications screen appears.

Step 20 Select the **Create HTTP Proxy** check box next to the cluster name that you had created in [Step 16](#) and ensure that MS3 is selected from the **Proxy Server** drop-down list.

Step 21 Click **Next**.

The Configure Machines screen appears.

Step 22 Click **Next**.

The Configuration Summary screen appears.

Step 23 Review the summary, and click **Create**.

A new WebLogic domain is created according to your specifications.

**Note**

After creating the WebLogic domain, you can navigate to `<WLS_INSTALL_DIRECTORY>/user_projects/domains` and verify that the domain has been successfully created. If you have specified a different location for the domain, navigate to the specified location to verify that the domain has been successfully created.

Step 24 Extend the admin server domain by performing the steps in the [Extending the WebLogic Domain for a Managed Server, page 2-32](#) section.

Starting the WebLogic Server

For information on how to start the admin server, see the “Starting the WebLogic Server” section on [page 2-8](#).


Configuring the Cluster

- [Configuring a Replication Group, page 2-36](#)
- [Setting Up the Message Types, page 2-37](#)
- [Enabling the WebLogic Plug-in, page 2-38](#)
- [Configuring the LDAP Authentication, page 2-38](#)
- [Configuring the DataSource, page 2-40](#)
- [Configuring Distributed JMS Configuration, page 2-40](#)
- [Restarting the WebLogic Server, page 2-41](#)
- [Updating the Properties Files, page 2-41](#)
- [Configuring LDAP Settings, page 2-41](#)

Configuring a Replication Group

To configure a replication group, perform the following steps:

Send documentation comments to scc-docfeedback@cisco.com

-
- Step 1** Ensure that the administration server is up and running.
- Step 2** Log in to the WebLogic Server Administration Console by typing the URL `http://<host>:<port>/console`.
Where, 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.
The WebLogic Server Administration Login screen appears.
- Step 3** Enter the user details that you have specified during the WebLogic domain creation and click **Login**.
The WebLogic Server Administration Console home page appears.
- Step 4** Click **Lock & Edit**.
- Step 5** In the Domain Structure pane, expand the 'Environment' node and click **Servers**.
The Summary of Servers screen appears. Ensure that all the servers are listed with the appropriate port numbers.
- Step 6** Under the **Name** column, select **MS1**.
The Settings for Managed Server 1 page appears.
- Step 7** Click **Cluster**. Enter the replication group name in the **Replication Group** field. For example, rep1.
- Step 8** Click **Save**.
- Step 9** Repeat [Step 5](#) through [Step 8](#) for all the other managed servers. For example, MS2.
-  **Note** You must enter the same replication group name in both, Managed Server 1 and Managed Server 2. If you change the name, the clustering setup will not work.
-
- Step 10** Click **Activate Changes**.
-

Setting Up the Message Types

For a cluster setup, you must change the message settings from multicast to unicast.

To change the message settings, perform the following steps:

-
- Step 1** Log in to the WebLogic Server Administration Console by typing the URL `http://<host>:<port>/console`.
Where, 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.
The WebLogic Server Administration Login screen appears.
- Step 2** Enter the user details that you specified during the WebLogic domain creation, and click **Login**.
The WebLogic Server Administration Console home page appears.
- Step 3** In the Domain Structure pane, expand the 'Environment' node and click **Clusters**.
The Summary of Clusters page appears.
- Step 4** Under the Name column, select **Cluster**.
The Settings for Cluster page appears.

Send documentation comments to scc-docfeedback@cisco.com

- Step 5** Under the **Configuration** tab, click the **Messaging** tab.
 - Step 6** Click **Lock and Edit**.
 - Step 7** From the **Messaging Mode** drop-down list, choose **Unicast**, and click **Save**.
 - Step 8** Click **Activate Changes**.
- The message settings are now changed to unicast successfully.
-

Enabling the WebLogic Plug-in

To enable the WebLogic plug-in for a cluster setup, perform the following steps:

- Step 1** Log in to the WebLogic Server Administration Console by typing the URL `http://<host>:<port>/console`. Where, 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.
The WebLogic Server Administration Login screen appears.
 - Step 2** Enter the user details that you had specified while creating the WebLogic domain, and click **Login**.
The WebLogic Server Administration Console home page appears.
 - Step 3** In the Domain Structure pane, expand the Environment node, and click **Clusters**.
The Summary of Clusters page appears.
 - Step 4** In the Name column, select **Cluster**.
The Settings for Cluster page appears.
 - Step 5** Click **Lock & Edit**. Scroll down the page, and click **Advanced**.
 - Step 6** Select the **WebLogic Plug-In Enabled** check box, and click **Save**.
 - Step 7** In the Domain Structure pane, click the domain name.
The settings for domain page appears.
 - Step 8** Click the **Web Applications** tab.
 - Step 9** Select the **Client Cert Proxy Enabled** and **WebLogic Plug-In Enabled** check boxes, and click **Save**.
 - Step 10** Click **Activate Changes**.
The WebLogic plug-in is successfully enabled.
-

Configuring the LDAP Authentication

Ensure that the WebLogic Administration server is up and running before configuring the LDAP authentication.

To configure the LDAP authentication, perform the following steps:

- Step 1** Open the weblogic console using the Admin port. In the Address field of the Web browser, enter `http://host:port/console`.

Send documentation comments to scc-docfeedback@cisco.com

Where 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.

The WebLogic Administration Console login page appears.

Step 2 Enter the WebLogic console username and password, and click **Login**.

The WebLogic home page appears.

Step 3 Under **Domain Structure**, click **Security Realms**.

The Summary of Security Realms page appears.

Step 4 Click **myrealm**.

The Settings for myrealm page appears.

Step 5 Click the **Providers** tab, and click **SDP LDAP Auth Provider**.

The Settings for SDP LDAP Auth provider page appears.

Step 6 Under **Configuration**, click **Provider Specific**.

Step 7 Click **Lock & Edit**, and provide the following LDAP server and LDAP user details with their actual values in the corresponding textboxes:

Property	Description	Value
Configured Tenants	Defines the number of tenants you want to access. The value 0 implies multiple tenants.	0
Connection Password	The attribute to provide the password for the LDAP authentication.	<password>
Please type again To confirm	The attribute to again provide the password for confirmation.	<password>
Connection URL	The attribute to provide the LDAP URL.	http://<IP Address of the LDAP host>:389
User Base	The attribute to provide the LDAP user base.	<user base>
Authentication	Simple authentication is required.	simple
Connection Username	The attribute to provide the connection name.	<connection name>
Jndi Name	The datasource jndi name. The default value is jdbc/scc.	jdbc/scc
User Search Matching	The matching search string to find the user.	<ul style="list-style-type: none"> • For the Active Directory—cn={0} • For the open LDAP directory—uid={0}

Step 8 Click **Save**.

Step 9 Click **Activate Changes** to activate the changes.

Send documentation comments to scc-docfeedback@cisco.com

Configuring the DataSource

In a cluster setup, all the managed nodes need to be pointed to a common data source.

To configure the data source, perform the following steps:

-
- Step 1** Log in to the WebLogic Server Administration Console by typing the URL `http://<host>:<port>/console`. Where, 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.
- The WebLogic Server Administration Login screen appears.
- Step 2** Enter the user details that you have specified during the WebLogic domain creation, and click **Login**. The WebLogic Server Administration Console home page appears.
- Step 3** Under **Domain Structure**, click **Services > Data Sources**. The Summary of JDBC Data Sources page appears.
- Step 4** Click **sdpDatasource**. The Settings for sdpDatasource page appears.
- Step 5** Click the **Targets** tab. The Servers and Clusters areas appear.
- Step 6** Do the following:
- Click **Lock & Edit**.
 - In the Clusters area, select the check box next to the cluster that you had created for the WebLogic cluster setup, and click the **All servers in the cluster** radio button.
 - Click **Save**.
- Step 7** Click **Activate Changes** to activate the changes.
-

Configuring Distributed JMS Configuration

For a cluster setup, a connection Factory and a distributed Queue need to be created.

To create the connection factory and the distributed queue, perform the following steps:

-
- Step 1** Log in to the WebLogic Server Administration Console by typing the URL `http://<host>:<port>/console`. Where, 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.
- The WebLogic Server Administration Login screen appears.
- Step 2** Enter the user details that you have specified during the WebLogic domain creation, and click **Login**. The WebLogic Server Administration Console home page appears.
- Step 3** Under **Domain Structure**, click **Services > Messaging > JMS Modules**.
- Step 4** Click **SDPSystemModule-0**. The SDPSystemModule-0 settings appear.

Send documentation comments to scc-docfeedback@cisco.com

- Step 5** Click **Lock & Edit**.
- Step 6** Click **New** and select the **Connection Factory** option.
- Step 7** Click **Next**.
- Step 8** Retain the default Connection Factory name that appears in the Name field. For example, ConnectionFactory-0.
- Step 9** Enter the JNDI name as 'jms/ipsConnectionFactory' in the JNDI Name field.
- Step 10** Click **Next**.
- Step 11** Ensure that the target selected is selected as 'AdminServer', and click **Finish**.
The Connection Factory is created.
- Step 12** In the Settings for the SDPSystem Module-0 screen, click **New**, and select **Distributed Queue**.
- Step 13** Click **Next**.
- Step 14** Retain the default Queue name that appears in the Name field. For example, DistributedQueue-0.
- Step 15** Enter the JNDI name as 'jms/ipsQueue' in the JNDI Name field.
- Step 16** Click **Next**.
- Step 17** Click **Advanced Targeting**.
- Step 18** Click **Create a New Subdeployment**.
- Step 19** Enter a name in the Subdeployment Name field. For example, DistributedQueueSubDeployment.
- Step 20** Click **OK**.
The subdeployment is created.
- Step 21** In the Targets area, select 'AdminServer', and click **Finish**.
The distributed queue is created.
- Step 22** Click **Activate Changes**.
-

Restarting the WebLogic Server

For information on how to restart the WebLogic Server, see the [“Restarting the WebLogic Server” section on page 2-27](#).

About Properties Files

For information on the properties files, see the [“About Properties Files” section on page 2-10](#).

Updating the Properties Files

For information on updating the properties files, see the [“Updating the Properties Files” section on page 2-15](#).

Configuring LDAP Settings

For information on how to configure the LDAP settings, see the [“Updating the WebLogic Configuration” section on page 2-16](#).

Send documentation comments to scc-docfeedback@cisco.com

Configuring the Secured URL

To launch the Smart+Connected PS application in a secured environment, you need to configure the secured URL.

To configure the secured URL, perform the following steps:

-
- Step 1** Ensure that the WebLogic Administration server is up and running.
- Step 2** Log in to the WebLogic Server Administration console by typing the URL `http://<host>:<port>/console`. Where, 'host' is the IP address or the DNS hostname of the admin server on which the WebLogic Administration server has been set up and 'port' is the Admin port number that you have defined for the WebLogic administration server.
- The WebLogic Server Administration Login screen appears.
- Step 3** Enter the WebLogic console username and password, and click **Login**.
- The WebLogic home page appears.
- Step 4** Under Domain Structure, click **Environment > Servers**.
- The Summary of Servers area appears.
- Step 5** In the Servers table, click the proxy server. For example, MS3.
- The Settings for the proxy server (MS3) area appears.
- Step 6** Click **Lock & Edit**.
- Step 7** In the Settings for AdminServer area, perform the following steps:
- Select the **SSL Listen Port Enabled** check box.
 - In the SSL Listen Port field, provide a unique port number to be used for launching the secured URL.
 - Click **Save**.
- Step 8** Click **Activate Changes** to activate the changes.

Configuring Installer for the Mobile Devices

The Smart+Connected PS installation package comprises the following files in the MobileApps directory:

- For the Android phones—SCPS_Mobile.apk
- For the iPhones—SCPSMobileIOSNew.ipa and SCPSMobileIOSNew.plist

These files are required for configuring installer for the mobile devices.

- [Configuring Installer for the Android Phones, page 2-42](#)
- [Configuring Installer for the iPhones, page 2-44](#)

Configuring Installer for the Android Phones

To configure installer for the Android phones, perform the following steps:

-
- Step 1** Extract the Messages.properties file:
- Copy the SCPS_Mobile.apk file from the MobileApps directory to a local directory.

Send documentation comments to scc-docfeedback@cisco.com

- b. Double-click the copied SCPS_Mobile.apk file and open the Archive Manager screen.
- c. Navigate to /assets/www/resources, select the Messages.properties file, and click **Extract**.
You can extract it to a suitable location, such as Desktop.

Step 2 Update the Messages.properties file:

- a. Open the Messages.properties file from the extracted location in an edit mode and update the following values:
 - secureServerURL = https://<host>:<SSL port>

Where, 'host' is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and 'SSL port' is the port number that you have defined as the SSL listen port for the proxy server in the [“Configuring the Secured URL” section on page 42](#).



Note If you have not configured the secured URL, you must provide the 'serverURL' value in the 'secureServerURL' field so that the application can be accessed in a non-secured environment.

- serverURL = http://<host>:<port>

Where, 'host' is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and 'port' is the port number that you have defined for the WebLogic proxy server.

- b. Save and close the file.

Step 3 Replace the Messages.properties file in the SCPS_Mobile.apk file:

- a. Double-click the SCPS_Mobile.apk file from the extracted location and open the Archive Manager screen.
- b. Navigate to /assets/www/resources, and click **Add**.
- c. Browse and select the updated Messages.properties file, and click **OK**.
- d. Close the Archive Manager screen of the SCPS_Mobile.apk file.

Step 4 Navigate to the \$JAVA_HOME/bin directory, and enter the following command to generate a key for signing the SCPS_Mobile.apk file:

```
./keytool -genkey -v -keystore my-release-key.keystore -alias <alias name> -keyalg RSA -keysize 2048 -validity <number of days>
```

For example:

```
./keytool -genkey -v -keystore my-release-key.keystore -alias scps -keyalg RSA -keysize 2048 -validity 10000
```

You are prompted to specify the following required details:

- Enter keystore password—Specify a password for keystore. You also need to use the same keystore password for the signing the SCPS_Mobile.apk file.
- Re-enter new password—Specify the new password again.
- What is your first and last name?—Specify the host name of the machine.
- What is the name of your organizational unit?—Specify your organizational unit.
- What is the name of your organization?—Specify your organization name.

Send documentation comments to scc-docfeedback@cisco.com

- What is the name of your City or Locality?—Specify the name of your city.
- What is the name of your State or Province?—Specify the name of your state or province.
- What is the two-letter country code for this unit?—Specify the first two letters of your country.
- Is CN=<name>, OU=<organizational unit>, O=<organization>, L=<city>, ST=<state>, C=<country> correct?—Verify the specified values, enter ‘Yes’ if the values are correct, and press **Enter**.

The RSA key and self-signed certificate with a validity of <number of days> days is generated. You are prompted for the key password of the <alias name>. Press **Enter**.

Automatically, the keystore password is retained for the <alias name> key password.

Step 5 Enter the following command to sign the SCPS_Mobile.apk file:

```
./jarsigner -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore
my-release-key.keystore <location of SCPS_Mobile.apk>/SCPS_Mobile.apk <alias name>
```

For example:

```
./jarsigner -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore my-release-key.keystore
/home/u01/Desktop/SCPS_Mobile.apk SCPS
```

You are prompted for the keystore password. Enter the keystore password, and press **Enter**.

The SCPS_Mobile.apk file is successfully signed.

Step 6 Replace the SCPS_Mobile.apk file in the scps.war file:

- Double-click the scps.war file from the <SCPS_INSTALL_DIRECTORY>/scps/bin/war/ directory, and open the Archive Manager screen.
- Navigate to /mobile_download, and click **Add**.
- Browse and select the signed SCPS_Mobile.apk file, and click **OK**.
- Close the Archive Manager screen of the scps.war file.

Configuring Installer for the iPhones

While configuring installer for the iPhones, you need to sign the SCPSMobileIOSNew.ipa file using the MAC machine. Therefore, the provisioning profile must be available in your MAC machine.

To configure installer for the iPhones, perform the following steps:

Step 1 Extract the download.properties file:

- In a file browser, navigate to the directory containing the <PS_INSTALL_DIRECTORY>/scps/bin/war/scps.war file and double-click this file to open the Archive Manager screen.
- Navigate to /mobile_download, select the download.properties file, and click **Extract**.
You can extract it to a suitable location, such as Desktop.

Step 2 Update the download.properties file:

- In a terminal, navigate to the directory where the download.properties file is available.
- Open the download.properties file in an edit mode, and update the following line:
ios_url=http://<host>:<port>/ipsapp/mobile_download/SCPSMobileIOSNew.plist

Send documentation comments to scc-docfeedback@cisco.com

Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘port’ is the port number that you have defined for the WebLogic proxy server.

- c. Save and close the file.

Step 3 Copy the SCPSMobileIOSNew.ipa and SCPSMobileIOSNew.plist files from the MobileApps directory to your MAC machine.

Step 4 In the MAC machine, update the SCPSMobileIOSNew.plist file:

- a. In a terminal, navigate to the directory where the SCPSMobileIOSNew.plist file is available.
- b. Open the SCPSMobileIOSNew.plist file in an edit mode, and update the following string:

```
<string>http://<host>:<port>/ipsapp/mobile_download/SCPSMobileIOSNew.ipa</string>
```

Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘port’ is the port number that you have defined for the WebLogic proxy server.

- c. Save and close the file.

Step 5 In the MAC machine, sign the SCPSMobileIOSNew.ipa file:

- a. In a terminal, navigate to the directory where the SCPSMobileIOSNew.ipa file is available.
- b. Unzip the SCPSMobileIOSNew.ipa file by entering the following command:

```
unzip SCPSMobileIOSNew.ipa
```

- c. Remove the existing signature by entering the following command:

```
rm -rf Payload/SCPSMobileIOSNew.app/_CodeSignature
```

- d. Open the Messages.properties file in an edit mode using the following command:

```
vi Payload/SCPSMobileIOSNew.app/www/resources/Messages.properties
```

- e. Update the following values:

- secureServerURL = https://<host>:<SSL port>

Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘SSL port’ is the port number that you have defined as the SSL listen port for the proxy server in the [“Configuring the Secured URL” section on page 42](#).



Note If you have not configured the secured URL, you must provide the ‘serverURL’ value in the ‘secureServerURL’ field so that the application can be accessed in a non-secured environment.

- serverURL = http://<host>:<port>

Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘port’ is the port number that you have defined for the WebLogic proxy server.

- f. Save and close the file.
- g. Copy the available provisioning profile (.mobileprovision file) to Payload/SCPSMobileIOSNew.app/ directory and name it as ‘embedded.mobileprovision’.

Send documentation comments to scc-docfeedback@cisco.com

- h. Enter the following command:

```
/usr/bin/codesign -f -s "iPhone Distribution: <distribution name>" --resource-rules
"Payload/SCPSMobileIOSNew.app/ResourceRules.plist" "Payload/SCPSMobileIOSNew.app"
```

Where *<distribution name>* is the distribution license name.

- i. Zip the SCPSMobileIOSNew.ipa file by entering the following command:

```
zip -r SCPSMobileIOSNew.ipa Payload
```

- Step 6** Copy the updated SCPSMobileIOSNew.ipa and SCPSMobileIOSNew.plist files from the MAC machine to the machine where the Smart+Connected PS application is installed.
- Step 7** Replace the download.properties, SCPSMobileIOSNew.ipa, and SCPSMobileIOSNew.plist files in the scps.war file:
- Double-click the scps.war file from the *<SCPS_INSTALL_DIRECTORY>/scps/bin/war/* directory, and open the Archive Manager screen.
 - Navigate to */mobile_download*, and click **Add**.
 - Browse and select the updated download.properties, signed SCPSMobileIOSNew.ipa, and SCPSMobileIOSNew.plist files, and click **OK**.
 - Close the Archive Manager screen of the scps.war file.
 -
-

Deploying Apache Jackrabbit

To deploy the Apache Jackrabbit, perform the following steps:

-
- Step 1** Log in to the WebLogic Server Administration Console.
The WebLogic Home Page appears.
- Step 2** In the WebLogic Home Page, under the **Domain Structure**, click **Deployments**.
The Summary of Deployments screen appears.
- Step 3** Click **Lock & Edit**.
- Step 4** Delete the SDP app and the SDP report created when you use the SDP domain extension template.
- Step 5** Click **Install**.
- Step 6** Navigate to *<PS_INSTALL_DIRECTORY>/scps/bin/war/* by either selecting the current location option or by entering path in the path field and select the **jackrabbit.war** file.
- Step 7** Click **Next**.
- Step 8** Install this deployment as an application and click **Next**.
Select the configured cluster as Target and click **Next**.
- Step 9** Click **Yes, take me to the deployment's configuration screen** and click **Finish**.
The Configuration screen appears.
- Step 10** Change the Deployment Order to **50**, and then click **Save**.

Send documentation comments to scc-docfeedback@cisco.com

- Step 11** Click **Save**.
- Step 12** Click **Activate Changes**.
- Step 13** Stop Managed Server2 on Machine2. Ensure that the Managed Server1 is running at this point of time.
- Step 14** In the Address field of the browser, enter `http://adminserverhostname:proxy port/jackrabbit`, and then click **Create Content Repository**.
The `<WLS_INSTALL_DIRECTORY>/<user_projects>/domains/<Your domain>/jackrabbit/` directory repository structure is created in the Managed Server1.
- Step 15** Start Managed Server2 on Machine2.
- Step 16** Stop the managed Server1 on Machine 1. Ensure that the Managed Server2 is running at this point of time.
- Step 17** In the Address field of the browser, enter `http://adminserverhostname:proxy port/jackrabbit`, and click **Create Content Repository**.
The `<WLS_INSTALL_DIRECTORY>/<user_projects>/domains/<Your domain>/jackrabbit/` directory repository structure is created in the Managed Server2.
-

Deploying the Smart+Connected PS Application

To deploy the Smart+Connected PS application, perform the following steps:

-
- Step 1** In the address field of the Web browser, enter `http://host:port/console`.
Where, 'host' is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been setup and 'port' is the Administration server port.
- Step 2** In the Oracle WebLogic Server Administration Console Login page, enter the username and password
- Step 3** In the WebLogic Home page, under **Domain Structure**, click **Deployments**.
- Step 4** Click **Lock and Edit**.
- Step 5** Click **Install**.
- Step 6** Navigate to `<PS_INSTALL_DIRECTORY>/scps/bin/war/` by either selecting the current location option or by entering path in the path field.
- Step 7** Select the **scps.war** radio button, and click **Next**.
- Step 8** Choose **cluster** as the target.
- Step 9** Keep the default selection **Install this deployment as an application**, and click **Next**.
- Step 10** Click **Finish and Save** to complete the deployment.
- Step 11** Click **Activate Changes** to activate the changes.
- Step 12** Verify that the application is deployed and is active.
-

Starting Servers

- [Starting the Admin Server, page 2-48](#)

Send documentation comments to scc-docfeedback@cisco.com

- [Starting the Proxy Server, page 2-48](#)
- [Starting the Managed Server, page 2-48](#)

Starting the Admin Server

To start the admin server, perform the following steps:

-
- Step 1** Log in to the machine that hosts the WebLogic admin server.
- Step 2** Open a terminal and navigate to the `<WLS_INSTALL_DIRECTORY>/<user_projects>/domains/<Your domain>/bin` directory.
- Step 3** Enter the following command:
- ```
./startWebLogic.sh
```
- Provide the domain username and password, if prompted. For example, weblogic/weblogic123.
- The admin server is started.
- 

### Starting the Proxy Server

To start the proxy server, perform the following steps:

- 
- Step 1** Ensure that the admin server is running.
- Step 2** Log in to the machine that hosts the WebLogic proxy server.
- Step 3** Open a terminal and navigate to the `<WLS_INSTALL_DIRECTORY>/<user_projects>/domains/<Your domain>/bin` directory.
- Step 4** Enter the following command:
- ```
./startManagedWebLogic.sh <name of Managed Server> t3://<IP address of admin server>:<listen Port of admin server>
```

For example:

```
./startManagedWebLogic.sh MS3 t3://10.65.111.54:7025
```

Provide the domain username and password, if prompted. For example, weblogic/weblogic123.

The proxy server is started.

Starting the Managed Server

To start the managed server, perform the following steps:

-
- Step 1** Login to the server that hosts the WebLogic managed server.
- Step 2** Open a terminal and navigate to the `<WLS_INSTALL_DIRECTORY>/<user_projects>/domains/<Your domain>/bin` directory.
- Step 3** Enter the following command to start a managed server:

Send documentation comments to scc-docfeedback@cisco.com

```
./startManagedWebLogic.sh <name of Managed Server> t3://<IP address of admin
server>:<listen Port of admin server>
```

For example:

```
./startManagedWebLogic.sh MS1 t3://10.65.111.54:7025 (on machine1)
./startManagedWebLogic.sh MS2 t3://10.65.111.54:7025 (on machine2)
```

Provide the domain user name and password, if prompted. For example: weblogic/weblogic123

- Step 4** Repeat [Step 1](#) through [Step 3](#) to start all the managed servers in the cluster.
- Step 5** Login to the WebLogic administration console using the WebLogic console username and password. The WebLogic Home Page appears.
- Step 6** In the WebLogic Home Page, under the Domain Structure, click **Deployments**.
- Step 7** Select the check box for all deployments and choose **Start > Start Servicing all requests**.



Note Make sure that the administrator server of the cluster is in the running mode.

- Step 8** Log in to the WebLogic Administration Console. The WebLogic home page appears.
 - Step 9** In the WebLogic home page, under the **Domain Structure**, click **Servers**. The Summary of Servers screen appears. All the servers must display a RUNNING status.
-

Configuring Jackrabbit Repository for Clustering

To configure the Jackrabbit repository for clustering, perform the following steps:

- Step 1** In a file browser, navigate to the directory containing the `<PS_INSTALL_DIRECTORY>/scps/bin/war/jackrabbit.war` file, and double-click this file to open the Archive Manager screen.
- Step 2** Navigate to `/WEB-INF/lib`, select the `jcr-2.0.jar` file, and extract the file to the following location: `<WLS_INSTALL_DIRECTORY>/user_projects/domains/<your domain>/lib`.
- Step 3** Close the Archive Manager Screen.
- Step 4** Navigate to the `<WLS_INSTALL_DIRECTORY>/<user_projects>/domains/<your domain>/jackrabbit/` directory on the managed server which is running, and open the `repository.xml` file for editing.



Note Get the DB host IP address, DB port number (default 1521 if changed), DB SID, PS schema username and PS schema Password.

- Step 5** Search for the below text:

```
<FileSystem class="org.apache.jackrabbit.core.fs.local.LocalFileSystem">
<param name="path" value="{rep.home}/repository"/>
</FileSystem>
```

Replace with:

Send documentation comments to scc-docfeedback@cisco.com

```
<FileSystem class="org.apache.jackrabbit.core.fs.db.OracleFileSystem">
<param name="driver" value="oracle.jdbc.driver.OracleDriver"/>
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>:<SID
of the db>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="schemaObjectPrefix" value="F_1_"/>
</FileSystem>
```

Step 6 Search for the below text:

```
<DataStore class="org.apache.jackrabbit.core.data.FileDataStore"/>
```

Replace with:

```
<DataStore class="org.apache.jackrabbit.core.data.db.DbDataStore">
<param name="driver" value="oracle.jdbc.driver.OracleDriver"/>
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>:<SID
of the db>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="schemaObjectPrefix" value="D_1_"/>
</DataStore>
```

Step 7 Search for the below text:

```
<PersistenceManager
class="org.apache.jackrabbit.core.persistence.pool.DerbyPersistenceManager">
<param name="url" value="jdbc:derby:${wsp.home}/db;create=true"/>
<param name="schemaObjectPrefix" value="${wsp.name}_"/>
</PersistenceManager>
```

Replace with:

```
<PersistenceManager
class="org.apache.jackrabbit.core.persistence.pool.OraclePersistenceManager">
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>:<SID
of the db>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="schemaObjectPrefix" value="W_1_"/>
</PersistenceManager>
```

Step 8 Search for the below text:

```
<PersistenceManager
class="org.apache.jackrabbit.core.persistence.pool.DerbyPersistenceManager">
<param name="url" value="jdbc:derby:${rep.home}/version/db;create=true"/>
<param name="schemaObjectPrefix" value="version_"/>
</PersistenceManager>
```

Replace with:

```
<PersistenceManager
class="org.apache.jackrabbit.core.persistence.pool.OraclePersistenceManager">
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>:<SID
of the db>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="schemaObjectPrefix" value="V_1_"/>
</PersistenceManager>
```

Step 9 Add the following text at the end of the preceding text:

```
<Cluster id="node1" syncDelay="1000">
<Journal class="org.apache.jackrabbit.core.journal.OracleDatabaseJournal">
```

Send documentation comments to scc-docfeedback@cisco.com

```
<param name="driver" value="oracle.jdbc.driver.OracleDriver"/>
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>:<SID
of the db>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="schemaObjectPrefix" value="C_1_"/>
</Journal>
</Cluster>
```



Note Change the cluster ID accordingly for each managed server. Example: node1 for MS1, node2 for MS2 and so on.

- Step 10** In the preceding steps, replace the following strings with their actual values:
- Replace *<db host IP address>* with the database server IP address
 - Replace *<db port number>* with the database port number
 - Replace *<SID of the db>* with the SID of the database
 - Replace *<schema username>* with the database user name
 - Replace *<schema password>* with the database user password
- Step 11** Navigate to *<WLS_INSTALL_DIRECTORY>/user_projects/domains/<Your domain>/jackrabbit/workspaces/* directory and delete the available default and security directories.
- Step 12** Repeat [Step 1](#) through [Step 11](#) on all the managed servers in the cluster.
- Step 13** Start all the managed servers and verify that the 13 new tables and the two new sequences have been created in the database. These tables and sequences have names starting with *c_1_*, *d_1_*, *f_1_*, *v_1_*, *w_1_*, and so on.

Accessing the Application and Verifying the Installation

To access the Smart+Connected PS application and to verify the installation, perform the following steps:

- Step 1** In the Address field of a Web browser, type one of the following application server URLs, and press **Enter**:
- `http://<host>:<port>/ipsapp`—To access the application in a non-secured environment.
Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘port’ is the port number that you have defined for the WebLogic proxy server.
 - `https://<host>:<SSL port>/ipsapp`—To access the application in a secured environment.
Where, ‘host’ is the IP address or the DNS hostname of the host on which the WebLogic Administration server has been set up and ‘SSL port’ is the port number that you have defined as the SSL listen port for the proxy server in the [“Configuring the Secured URL”](#) section on page 42.
- Step 2** Enter the username and password for the Smart+Connected PS application.
The Smart+Connected PS login page appears.
- Step 3** Enter the username and password for the Smart+Connected PS application, and click **Login**.

Send documentation comments to scc-docfeedback@cisco.com

Your default login credentials are:

- Username—superadmin
- Password—superadmin

You can change your password by logging in to the SDP application. You can also create additional users by using the SDP application. For more information on how to assign roles and permissions to users in the SDP application, see the *Cisco Service Delivery Platform Administrator Guide*.

For more information on how to use the Smart+Connected PS features, see the *Cisco Smart+Connected Personalized Spaces User Guide*.
