



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



## **Cisco Smart+Connected Personalized Spaces Installation Guide**

Release 2.1.1  
November 2013

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Text Part Number: OL-30285-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

*Cisco Smart+Connected Personalized Spaces Installation Guide*  
© 2013 Cisco Systems, Inc. All rights reserved.



## **Preface ix**

Audience ix

Organization ix

Conventions x

Related Documentation x

Obtaining Documentation and Submitting a Service Request x

---

## **CHAPTER 1**

### **Introduction 1-1**

About Cisco Smart+Connected Personalized Spaces 1-1

System Architecture 1-1

List of Acronyms and Abbreviations 1-3

System Requirements 1-4

Types of Server Setup 1-5

Non-Cluster Server Setup 1-6

Cluster Server Setup 1-7

---

## **CHAPTER 2**

### **Installing the Smart+Connected PS on JBoss and Oracle 2-9**

Prerequisites 2-9

Gathering Required Information 2-9

Verifying Network Configurations 2-10

Installing on a Non-Cluster Server Setup 2-10

Configuring the Database 2-11

Requirements 2-11

About Database Scripts 2-11

Executing the Database Scripts 2-13

Installing the Application 2-13

Configuring Audio Notification to the Cisco IP Phone 2-15

Creating JBoss Profile 2-15

Setting Up Port 2-17

Setting Up Security Configuration 2-18

Setting Up Java Messaging Service (JMS) 2-19

Creating a Connection Factory 2-19

Creating an Event Topic 2-21

Configuring an Event Topic 2-22

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

Creating a Queue	2-23
Setting Up Library	2-23
Setting Up the BIRT Engine	2-24
Configuring Logging	2-24
Configuring the Properties Files	2-26
About the Properties Files	2-26
Updating the Properties Files	2-33
Setting Up Run Parameters	2-34
Setting Up the Push-to-Phone Feature	2-35
Configuring the Secured URL	2-36
Configuring Installer for the Mobile Devices	2-37
Configuring Installer for the Android Phones	2-37
Configuring Installer for the iPhones	2-39
Setting Up Apache Jackrabbit	2-41
Importing SSL Certificates	2-42
Starting the JBoss Server	2-43
Accessing the Application and Verifying the Installation	2-43
Smart+Connected PS Web Application	2-43
Smart+Connected PS Mobile Application	2-44
Installing on a Cluster Server Setup	2-44
About Clustering	2-46
Installing the Application	2-47
Configuring Audio Notification to the Cisco IP Phone	2-47
Configuring the Database	2-47
Configuring the JBoss Profile	2-48
Setting Up Port	2-49
Setting Up Security Configuration	2-49
Setting Up Java Messaging Service (JMS)	2-50
Setting Up Library	2-50
Setting Up the BIRT Engine	2-50
Configuring Logging	2-50
Configuring the Cluster Server Setup	2-50
Installing mod_cluster on the Proxy Node	2-51
Configuring Cluster on Nodes	2-53
Configuring the Properties Files	2-54
Setting Up Run Parameters	2-54
Setting Up the Push-to-Phone Feature	2-54
Configuring Installer for the Mobile Devices	2-54
Configuring Installer for the Android Phones	2-54
Configuring Installer for the iPhones	2-56

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

Setting Up Apache Jackrabbit	2-58
Configuring the Jackrabbit Repository	2-59
Importing SSL Certificates	2-60
Starting the Cluster and Proxy	2-61
Accessing the Application and Verifying the Installation	2-62
Smart+Connected PS Web Application	2-62
Smart+Connected PS Mobile Application	2-62

## CHAPTER 3

### **Installing the Smart+Connected PS on JBoss and Postgres** 3-63

Prerequisites	3-63
Gathering Required Information	3-63
Verifying Network Configurations	3-64
Installing on a Colocated or Non-Cluster Server Setup	3-64
Installing the Application	3-65
Configuring Audio Notification to the Cisco IP Phone	3-65
Configuring the Database	3-65
Requirements	3-65
About Database Scripts	3-65
Executing Database Scripts	3-68
Creating JBoss Profile	3-69
Setting Up Port	3-71
Setting Up Security Configuration	3-72
Setting Up Java Messaging Service (JMS)	3-73
Creating a Connection Factory	3-73
Creating an Event Topic	3-75
Configuring an Event Topic	3-76
Creating a Queue	3-77
Setting Up Library	3-77
Setting Up the BIRT Engine	3-78
Configuring Logging	3-78
Configuring the Properties Files	3-80
About the Properties Files	3-80
Updating the Properties Files	3-81
Setting Up Run Parameters	3-82
Setting Up the Push-to-Phone Feature	3-83
Configuring the Secured URL	3-84
Configuring Installer for the Mobile Devices	3-85
Configuring Installer for the Android Phones	3-85
Configuring Installer for the iPhones	3-87

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

Setting Up Apache Jackrabbit	3-89
Importing SSL Certificates	3-90
Starting the JBoss Server	3-91
Accessing the Application and Verifying the Installation	3-91
Smart+Connected PS Web Application	3-91
Smart+Connected PS Mobile Application	3-92
Installing on a Cluster Server Setup	3-92
About Clustering	3-94
Installing the Application	3-95
Configuring Audio Notification to the Cisco IP Phone	3-95
Configuring the Database	3-95
Configuring the JBoss Profile	3-96
Setting Up Port	3-97
Setting Up Security Configuration	3-97
Setting Up Java Messaging Service (JMS)	3-98
Setting Up Library	3-98
Setting Up the BIRT Engine	3-98
Configuring Logging	3-98
Configuring the Cluster Server Setup	3-98
Installing mod_cluster on the Proxy Node	3-99
Configuring Cluster on Nodes	3-101
Configuring the Properties Files	3-102
Setting Up Run Parameters	3-102
Setting Up the Push-to-Phone Feature	3-102
Configuring Installer for the Mobile Devices	3-102
Configuring Installer for the Android Phones	3-102
Configuring Installer for the iPhones	3-104
Setting Up Apache Jackrabbit	3-106
Configuring the Jackrabbit Repository	3-107
Importing SSL Certificates	3-109
Starting the Cluster and Proxy	3-109
Accessing the Application and Verifying the Installation	3-110
Smart+Connected PS Web Application	3-110
Smart+Connected PS Mobile Application	3-110

## CHAPTER 4

### **Configuring the Smart+Connected PS** 4-111

Configuring Locations	4-111
Adding Locations	4-111
Editing a Location	4-113

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

Deleting a Location	4-113
Configuring Devices	4-114
Adding Device Types	4-114
Adding Device Types in the Oracle Database	4-114
Adding Device Types in the PostgreSQL Database	4-116
Adding a Device	4-118
Deleting a Devices	4-123
Configuring Room Types	4-123
Configuring Adapters	4-123
Adapter Description	4-124
Configuring Adapter Properties	4-124
Configuring the Adapters to a Location	4-127
Sample Adapter Configurations	4-128
Configuring Services in CUCM	4-129
Assigning Roles (groups) to the Application User	4-130
Customizing the Branding Images	4-131

---

**INDEX**

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





## Preface

---

This preface describes the audience, organization, and conventions of the *Cisco Smart+Connected Personalized Spaces Installation Guide*, and provides information on the related documentation.

- [Audience, page ix](#)
- [Organization, page ix](#)
- [Conventions, page x](#)
- [Related Documentation, page x](#)
- [Obtaining Documentation and Submitting a Service Request, page x](#)

## Audience

This guide is intended for system administrators who install, configure, and maintain the Cisco Smart+Connected Personalized Spaces (Smart+Connected PS) application.

## Organization

This guide includes the following sections:

Chapter Number and Title	Description
<a href="#">Chapter 1, “Introduction”</a>	Provides an overview of the Smart+Connected PS application, describes the architecture, lists out the prerequisites, and the deployment models of this application.
<a href="#">Chapter 2, “Installing the Smart+Connected PS on JBoss and Oracle”</a>	Describes out to install and deploy the Smart+Connected PS application by using the Oracle database and the JBoss application server.
<a href="#">Chapter 3, “Installing the Smart+Connected PS on JBoss and Postgres”</a>	Describes how to install and deploy the Smart+Connected PS application by using the PostgreSQL database and JBoss application server.
<a href="#">Chapter 4, “Configuring the Smart+Connected PS”</a>	Describes how to configure the Smart+Connected PS application, post the installation.

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

## Conventions

This document uses the following conventions:

Convention	Indication
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Required alternative keywords are grouped in braces and separated by vertical bars.
courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

## Related Documentation

- *Cisco Smart+Connected Personalized Spaces User Guide*
- *Cisco Smart+Connected Personalized Spaces Mobile Application User Guide*
- *Cisco Smart+Connected Personalized Spaces Administrator Guide*
- *Release Notes for the Cisco Smart+Connected Personalized Spaces*
- *Cisco Service Delivery Platform Installation Guide*

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



# Introduction

---

This chapter provides information on the architecture, system requirements, and deployment models of the Cisco Smart+Connected Personalized Spaces (Smart+Connected PS) application.

- [About Cisco Smart+Connected Personalized Spaces, page 1-1](#)
- [System Architecture, page 1-1](#)
- [List of Acronyms and Abbreviations, page 1-3](#)
- [System Requirements, page 1-4](#)
- [Types of Server Setup, page 1-5](#)

## About Cisco Smart+Connected Personalized Spaces

The Smart+Connected PS application is a part of the Smart+Connected Communities (S+CC) solutions, and it leverages the platform capabilities of the Cisco Service Delivery Platform (SDP).

The Smart+Connected PS solution enables you to plan utilization of resources at your workspace by maximizing office usage and minimizing energy consumption. You can search for and book available workspaces and set your preferences for the light settings, blinds, air conditioning, and so on.

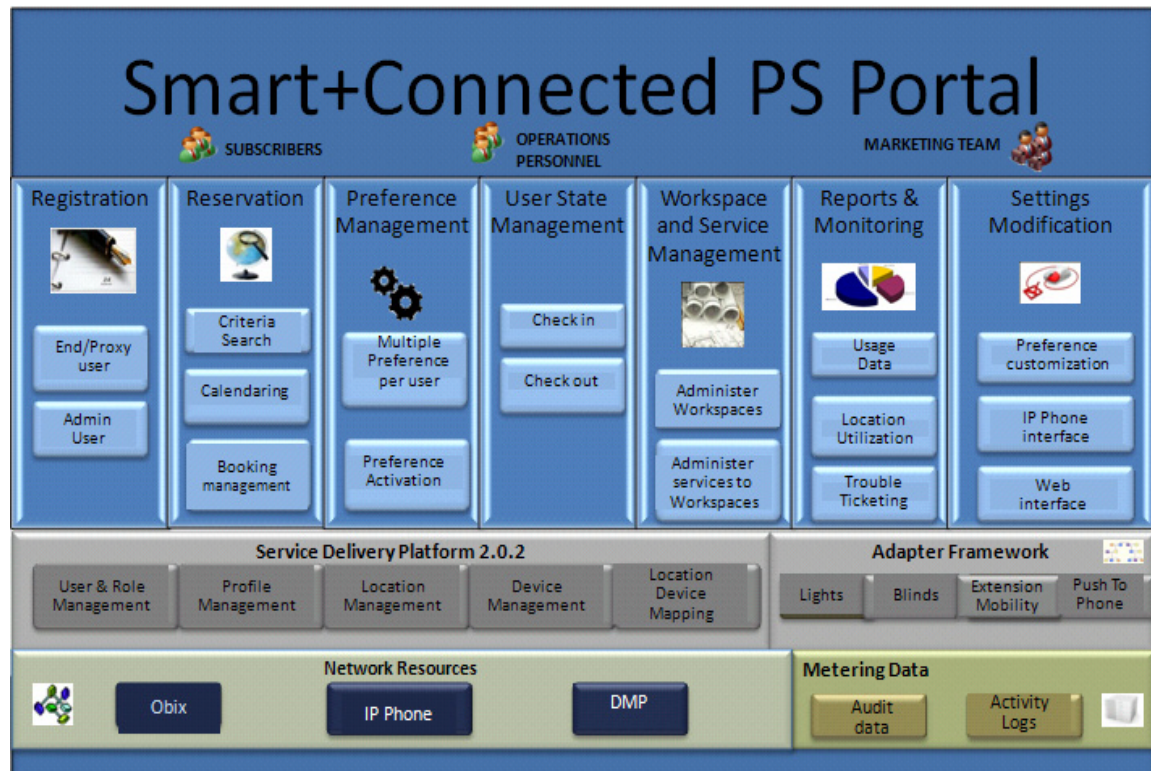
## System Architecture

The Smart+Connected PS solution is a holistic solution with an end-to-end integration for simple, flexible, and dynamic workspaces. It combines the following technologies to achieve a personalized user experience:

- Cisco Unified Communications Manager (CUCM)—For Cisco IP Phone interface integration with the Smart+Connected PS
- Building Automation—For workspace services, such as light setting controls, blinds, and air conditioners
- Digital Signage—To display personalized content, such as images and messages at your workspace

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

**Figure 1-1 Smart+Connected PS - System Architecture**



The Smart+Connected PS solution offers the following features:

- **Workspace Search**—Allows an end-user to search for an available workspace.
- **Workspace Booking with Preference Setting**—Allows an end-user to book a workspace for either themselves or for another user and preset preferences such as light setting control, blinds, dimmer, air conditioning, and digital signages.
- **Checking in and out**—Allows an end-user to check-in to the booked workspace at the scheduled time using either the web portal or a Cisco IP Phone available at the workspace. After using the workspace, the end-user is checked out of the workspace.

The Smart+Connected PS Mobile Application allows you to access the Smart+Connected PS application on your mobile devices, such as Android and iPhones. The Smart+Connected PS Mobile Application offers the following features:

- Viewing your upcoming meeting and workspace reservation details.
- Checking in and out of a reserved workspace.
- Ad-hoc checking in from the list of available workspaces.
- Checking in and out using the QR code scanning feature.
- Marking workspaces and people within an enterprise as favorites.
- Setting your preferences for a building and floor.
- Searching for people in an enterprise.
- Calling contacts or sending e-mails to them.
- Importing multiple contacts from the LDAP directory.

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

The Smart+Connected PS application provides the multi-language support configuration. Although English is the language that is supported out-of-the-box, other languages can be supported by doing necessary configurations.

## List of Acronyms and Abbreviations

**Table 1-1** *List of Acronyms and Abbreviations*

Acronym	Expansion
BIRT	Business Intelligence and Reporting Tools
BMS	Building Management Systems
CPU	Central Processing Unit
CUCM	Cisco Unified Communications Manager
DB	Database
DMP	Cisco Digital Media Player
DBMS	Database Management System
DNS	Domain Name System
EM	Extension Mobility
HTTP	Hypertext Transfer Protocol
JDBC	Java Database Connectivity
JDK	Java Development Kit
JMS	Java Message Service
JNDI	Java Naming and Directory Interface
JVM	Java Virtual Machine
LAN	Local Area Network
LDAP	Light Weight Directory Access Protocol
NTP	Network Time Protocol
RAM	Random-access Memory
RAC	Real Application Cluster
RDBMS	Relational Database Management Systems
RPM	Redhat Package Manager
RHEL	Red Hat Enterprise Linux
S+CC	Smart+Connected Communities
SDP	Cisco Service Delivery Platform
Smart+Connected PS	Smart+Connected Personalized Spaces
SQL	Structured Query Language
vCPU	Virtual CPU
VM	Virtual Machine

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

# System Requirements

Before installing the applications, ensure that your system meets all the necessary requirements.

**Table 1-2**      **System Requirements**

Software/Hardware	Supported Requirements
Operating System	Red Hat Linux (RHEL) 6.3 (64-bit)
Hardware	Minimum requirements are:
Note:	<ul style="list-style-type: none"> <li>• Hard Disk Space—200 GB</li> <li>• RAM—Minimum configuration of 4 GB or above</li> <li>• Processor <ul style="list-style-type: none"> <li>– 2 vCPU dual core for Virtual Machine (VM)</li> <li>– Intel x86/I386 Architecture for physical machines</li> <li>– Certified on Cisco UCS B-Series and C-Series with Intel CPUs.</li> </ul> </li> </ul>
<p>This requirement is for one VM (for example, colocated) or one physical machine.</p> <p>For a non-cluster setup, you need two VMs, with the listed minimum specifications. In this case, one VM is for the application server, while the second one is for the database.</p> <p>For a cluster setup, the hardware requirements are based on the deployment scenario and the user requirements.</p>	
Database	<ul style="list-style-type: none"> <li>• Oracle Enterprise Edition 11g R2 (11.2.0.2) with character set configured to UTF8</li> </ul> <p>For more information on how to install the Oracle database, see the Oracle documentation.</p> <ul style="list-style-type: none"> <li>• PostgreSQL 9.0 with character set configured to UTF8</li> </ul> <p>For more information on how to install the PostgreSQL database, see the PostgreSQL documentation.</p>
Application Server	JBoss 6.0
Java Development Kit (JDK)	JDK version 1.6.0_24
Cisco Service Delivery Platform (SDP)	SDP Version 2.0.2.0
Exchange Server	<ul style="list-style-type: none"> <li>• Microsoft Exchange Server 2007 SP3</li> <li>• Microsoft Exchange Server 2010 SP1, SP2</li> <li>• Microsoft Exchange Server 2013 V2.0</li> </ul>
Directory Services	<ul style="list-style-type: none"> <li>• Active Directory <ul style="list-style-type: none"> <li>– Windows 2008 Version 6.0</li> <li>– Windows 2003 Version 5.2 R2</li> </ul> </li> <li>• OpenLDAP - 2.3.43.12</li> </ul>

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

**Table 1-2 System Requirements (continued)**

Software/Hardware	Supported Requirements
Cisco Digital Media Player (DMP)	DMP 4400: <ul style="list-style-type: none"> <li>Firmware 5.1</li> <li>Firmware 5.2.3</li> <li>Firmware 5.3.5</li> </ul>
Cisco Interactive Experience Client (IEC)	IEP-4632-HW-K9: <ul style="list-style-type: none"> <li>Firmware 4.155.393</li> </ul>
Cisco IP Phone	<ul style="list-style-type: none"> <li>Touchscreen: 7975 and 9971</li> <li>Non-Touchscreen: 7962 and 9951</li> </ul>
Cisco Unified Communications Manager (CUCM)	<ul style="list-style-type: none"> <li>Cisco Call Manager Version 8.x</li> <li>Cisco Call Manager Version 9.x</li> </ul>
Browser	<ul style="list-style-type: none"> <li>Mozilla Firefox Versions 6.0, 14.0, and 15.0</li> <li>Microsoft Internet Explorer Versions 8.0 and 9.0</li> <li>Google Chrome Version 23.0</li> </ul>
Digital Signage	Resolutions: <ul style="list-style-type: none"> <li>1920 x 1080</li> <li>1366 x 768</li> </ul>
Mediation Gateway	Tridium with Obix Versions 3.5.34 and 3.7.x
Remedy	BMC Remedy Version 7.5
Mobile Operating System	<ul style="list-style-type: none"> <li>iOS Version 6.x</li> <li>Android               <ul style="list-style-type: none"> <li>Gingerbread 2.3.x</li> <li>Ice Cream Sandwich 4.0.x</li> <li>Jelly Bean 4.1.x</li> </ul> </li> </ul>

## Types of Server Setup

You can install and deploy the Smart+Connected PS application by using one of the following methods:

- **Non-Cluster Setup**—The database and the application server are installed on two different hosts.
- **Cluster Setup**—In this type of deployment, the database is installed on a server and the application server is installed on a cluster of servers. This setup provides high availability.



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

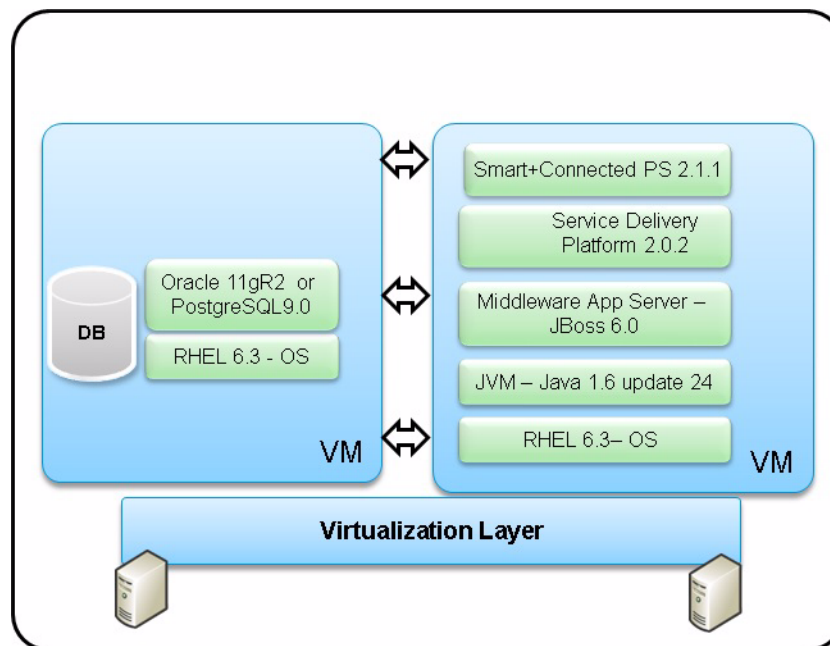
This guide describes the installation process in a colocated, non-cluster, and cluster server setups.

- [Non-Cluster Server Setup, page 1-6](#)
- [Cluster Server Setup, page 1-7](#)

## Non-Cluster Server Setup

In this setup, the database and the application server are installed on two different instances: either a physical or a virtual machine. This is a common server setup method for the Smart+Connected PS enterprise installations. The database is set up on one instance, and the application server, SDP, and the S+CC application are installed and set up on a second instance.

**Figure 1-2 Non-Cluster Server Setup**



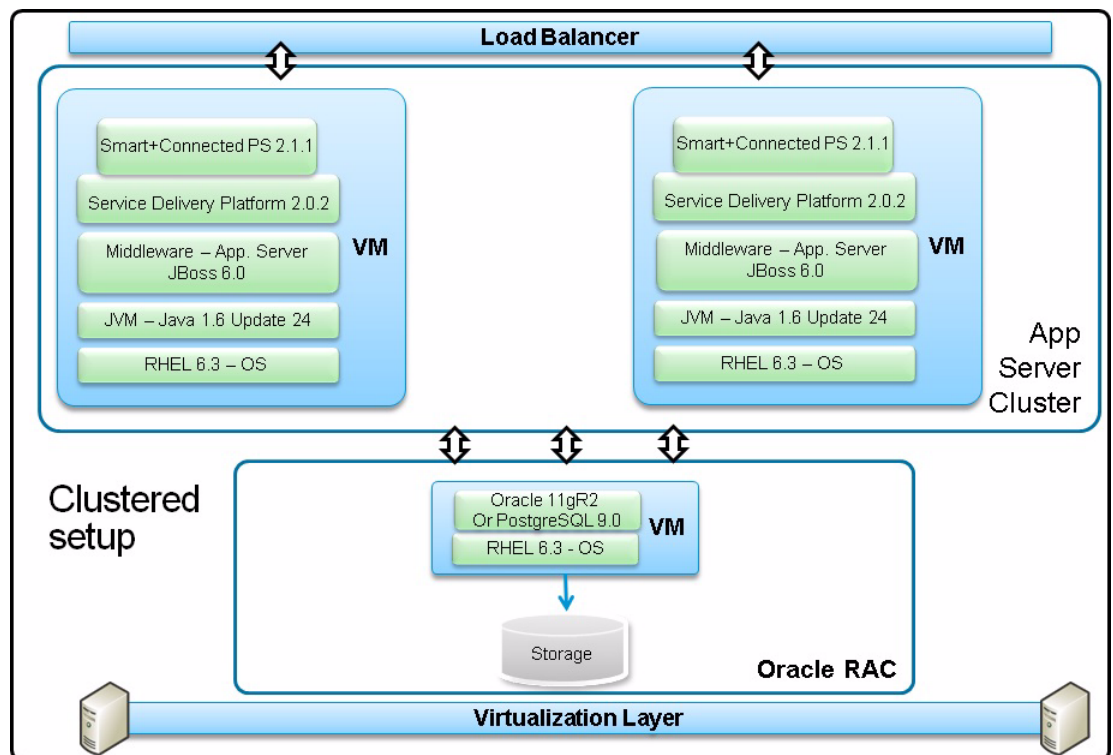


***Send documentation comments to [scc-docfeedback@cisco.com](mailto:scc-docfeedback@cisco.com)***

## Cluster Server Setup

A cluster setup consists of multiple servers that run an application simultaneously and work together to provide increased scalability, reliability, and high availability. In a distributed cluster setup, the solution is deployed on the multiple servers. Cluster setup acts as a single server instance with increased scalability, load balancing, and high availability.

**Figure 1-3 Cluster Setup**



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



## Installing the Smart+Connected PS on JBoss and Oracle

---

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

- [Prerequisites, page 2-9](#)
- [Installing on a Non-Cluster Server Setup, page 2-10](#)
- [Installing on a Cluster Server Setup, page 2-44](#)

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

### Prerequisites

- [Gathering Required Information, page 2-9](#)
- [Verifying Network Configurations, page 2-10](#)

### Gathering Required Information

You need to provide the following information during installation:

- Database Details:
  - Database server IP address.
  - Database name.
  - Port number on which PostgreSQL is to run. The default port number is 5432.
  - Database schema username.
  - Database schema password.
  - SSH credentials.
- Application Server Details:
  - Location of the `<JBoss_INSTALL_LOCATION>` directory if the JBoss server has been pre-installed. The `<JBoss_INSTALL_LOCATION>` directory is the complete path where the jboss files are available. Ensure that the `$JBoss_HOME` environment variable is set to the `<JBoss_INSTALL_LOCATION>` directory.

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

- Location of the `<JDK_INSTALL_LOCATION>` directory if the JDK has been pre-installed. The `<JDK_INSTALL_LOCATION>` directory is the complete path where you have installed JDK. Ensure that the `$JAVA_HOME` environment variable is set to the `<JDK_INSTALL_LOCATION>` directory and the `PATH` environment variable includes the `$JAVA_HOME/bin` directory.
- SSH credentials.

## Verifying Network Configurations

Verify the following network configurations:

- All machines in the setup are in the same network domain.
- All machines are in the same LAN.
- All machines are configured to be on the same locale.
- System time is synchronized on all machines by using the Network Time Protocol (NTP).
- All dependent components for the Smart+Connected PS application must be accessible over the network.

## Installing on a Non-Cluster Server Setup

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

1. [Configuring the Database, page 2-11](#)
2. [Installing the Application, page 2-13](#)
3. [Configuring Audio Notification to the Cisco IP Phone, page 2-15](#)
4. [Creating JBoss Profile, page 2-15](#)
5. [Setting Up Port, page 2-17](#)
6. [Setting Up Security Configuration, page 2-18](#)
7. [Setting Up Java Messaging Service \(JMS\), page 2-19](#)
8. [Setting Up Library, page 2-23](#)
9. [Setting Up the BIRT Engine, page 2-24](#)
10. [Configuring Logging, page 2-24](#)
11. [Configuring the Properties Files, page 2-26](#)
12. [Setting Up Run Parameters, page 2-34](#)
13. [Setting Up the Push-to-Phone Feature, page 2-35](#)
14. [Configuring the Secured URL, page 2-36](#)
15. [Configuring Installer for the Mobile Devices, page 2-37](#)
16. [Setting Up Apache Jackrabbit, page 2-41](#)
17. [Importing SSL Certificates, page 2-42](#)
18. [Starting the JBoss Server, page 2-43](#)
19. [Accessing the Application and Verifying the Installation, page 2-43](#)

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

## Configuring the Database

- [Requirements, page 2-11](#)
- [About Database Scripts, page 2-11](#)
- [Executing the Database Scripts, page 2-13](#)

### Requirements

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

- 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.

- Ensure that the following rights are granted to the database schema user:
  - 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

### About 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 or 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.

- [SDP Database Scripts, page 2-12](#)
- [PS Application Database Scripts, page 2-12](#)

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

## SDP Database Scripts

The SDP database scripts are available at the following directory on the server where you have installed the SDP application:

`<SDP_INSTALL_DIRECTORY>/sdp/`

**Table 2-1 SDP Database Script - Details**

Script	Description
<code>clean-sdp-objects.sql</code>	Cleans all SDP-related objects from the user schema if an instance of SDP was running earlier. Executing this script is not necessary if you are installing the SDP for the first time.
<code>setup-sdp-base.sql</code>	<ul style="list-style-type: none"> <li>Creates the tables, constraints, sequences, and indexes.</li> <li>Loads only the basic data that is required to bootstrap the application.</li> <li>Enables the local database authentication.</li> <li>Creates a user with the default username/password as superadmin/superadmin.</li> <li>Adds the locations that are defined in the seed data.</li> <li>Grants access rights to the locations to SuperAdmin (super administrator).</li> </ul>
<code>setup-sdp-types.sql</code>	Loads the device types and device properties data.

## PS Application Database Scripts

The Smart+Connected PS database scripts are available at the following directory in the system where you have installed the application:

`<PS_INSTALL_DIRECTORY>/scps/scripts/oracle`

These scripts create the appropriate Smart+Connected PS database objects in the database.

**Table 2-2 Smart+Connected PS Database Script - Details**

Script	Description
<code>clean-pvo-objects.sql</code>	Cleans all the Smart+Connected PS-related objects from the user schema. Executing this script is not necessary if you are installing the application for the first time.

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

**Table 2-2 Smart+Connected PS Database Script - Details**

Script	Description
<code>insert-seed-data.sql</code>	Inserts the required basic seed data into the tables. This is available in the directory: <PS_INSTALL_DIRECTORY>/scps/scripts/oracle/commonscript
<code>setup-pvo-base.sql</code>	<ul style="list-style-type: none"> <li>Creates the tables, constraints, sequences, and indexes.</li> <li>Loads the basic data that is required to bootstrap the application.</li> </ul>

## Executing the Database Scripts

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

Execute the following Smart+Connected PS database scripts in the system where you want to set up the database:

1. `insert-seed-data.sql` from the <PS\_INSTALL\_DIRECTORY>/scps/scripts/oracle/commonscript directory.
2. `setup-pvo-base.sql` from the <PS\_INSTALL\_DIRECTORY>/scps/scripts/oracle directory.

The above scripts creates the appropriate Smart+Connected PS database objects in the database.

Ensure that you have the 'read' permission to run the scripts and they are executed in the same order as listed here. 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.

## 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.

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

**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 the directory that you selected during the installation, and verify that the Smart+Connected PS directory has been created.



**Note**

The parent directory that contains this Smart+Connected PS directory will be referred to as <PS\_INSTALL\_DIRECTORY> in the subsequent sections of this document.



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

## Creating JBoss Profile

After configuring the database, you need to create a profile in the JBoss server for running the Smart+Connected PS application.

To create a profile in the JBoss server, perform the following steps:

**Step 1** Download `jboss-6.0.0.Final.zip`.

JBoss is open source, and you can download it from the Internet. For example:

<http://sourceforge.net/projects/jboss/files/JBoss/JBoss-6.0.0.Final/jboss-as-distribution-6.0.0.Final.zip/download>

**Step 2** Create a directory named ‘jboss’, and unzip the `jboss-6.0.0.Final.zip` file into that directory.

**Step 3** Set the `$JBOSS_HOME` and `$JAVA_HOME` environment variables by entering the following commands:

```
$ export JAVA_HOME=<JDK_INSTALL_LOCATION>
$ export JBOSS_HOME=<JBOSS_INSTALL_LOCATION>
```

Where, `<JBOSS_INSTALL_LOCATION>` is the complete path where the unzipped `jboss-6.0.0` files are available and `<JDK_INSTALL_LOCATION>` is the complete path where you have installed `jdk1.6.0_24`.



**Note** You can also add the preceding commands to the user’s profile script so that the `$JBOSS_HOME` and `$JAVA_HOME` environment variables are automatically set up during login.

**Step 4** Navigate to the server directory in `$JBOSS_HOME` by entering the following command:

```
cd $JBOSS_HOME/server
```

**Step 5** Copy the ‘default’ directory with the name ‘scps’ by entering the following command:

```
cp -R default scps
```

The ‘scps’ directory is created under the `$JBOSS_HOME/server` directory. The ‘scps’ directory is used as the Smart+Connected PS application profile.

**Step 6** Copy the `ipsapp.war` file, which is available in `<PS_INSTALL_DIRECTORY>/scps/bin/war`, to the `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:

```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/ipsapp.war $JBOSS_HOME/server/scps/deploy
```

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

**Step 7** Create a datasource file so that the Smart+Connected PS application communicates with the database machine:

a. Create the oracle-ds.xml file under the 'scps/deploy' directory with the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<local-tx-datasource>
<jndi-name>jdbc/scc</jndi-name>
<connection-url>jdbc:oracle:thin:@IPaddress:DBport:SID</connection-url>
<driver-class>oracle.jdbc.OracleDriver</driver-class>
<user-name>DBusername</user-name>
<password>DBpassword</password>
<exception-sorter-class-name>
org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter
</exception-sorter-class-name>
</local-tx-datasource>
</datasources>
```

b. Replace the following text with their actual values in the code that you had added in [Step 7 a.](#):

- 'IPaddress' with the database server IP address or DNS hostname
- 'SID' with the oracle SID
- 'DBport' with the database port number (default is 1521, if not changed)
- 'DBusername' with the database schema username
- 'DBpassword' with the database schema password

c. Save the file.

d. Provide the executable permissions to the newly created oracle-ds.xml file by entering the following command:

```
chmod 755 oracle-ds.xml
```

**Step 8** Add an entry for scanning deployers:

a. Navigate to the `$JBoss_HOME/server/scps/deployers` directory, and open the `scanning-deployers-jboss-beans.xml` file.

b. Search for the following text:

```
<install method="addIgnored">
<parameter>java.lang.LinkageError</parameter>
</install>
```

c. Add the following code after the searched text:

```
<install method="addIgnored">
<parameter>java.lang.reflect.MalformedParameterizedTypeException</parameter>
</install>
```

d. Save the file.

**Step 9** Update the `run.conf` file to increase the memory:

a. Open the `run.conf` file available in `$JBoss_HOME/bin` and search for the following text:

```
JAVA_OPTS="-Xms128m -Xmx512m -XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

Replace with the following text:

```
JAVA_OPTS="-Xms256m -Xmx1024m -XX:MaxPermSize=512m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

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

- b. Save the file.

## Setting Up Port

You need to set up a port for the Smart+Connected PS application by changing the following default port values:

- JBoss web HTTP connector socket value. By default, the 'HttpConnector' value is 8080.
- Listening socket for the naming service. By default, the 'Port' value is 1099.



### Note

While changing the default port values, ensure that you do not change any other port number apart from the 'HttpConnector' and 'Port' values for the property name 'bindingName'.

To set up a port for the Smart+Connected PS application, perform the following steps:

- Step 1** Open the following file:  
`$JBOSS_HOME/server/scps/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml`
- Step 2** Search for the port number 8080 that has the 'bindingName' value as 'HttpConnector' and replace with a port number that is not in use, for example 7001.

After changing the value, the text is displayed as follows:

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">
  <property name="serviceName">jboss.web:service=WebServer</property>
  <property name="bindingName">HttpConnector</property>
  <property name="port">7001</property>
  <property name="description">JBoss Web HTTP connector socket; also drives the values
for the HTTPS and AJP sockets</property>
</bean>
```

- Step 3** Search for the port number 1099 that has the 'bindingName' value as 'Port' and replace with a port number 11099.

After changing the value, the text is displayed as follows:

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">
  <property name="serviceName">jboss.service=Naming</property>
  <property name="bindingName">Port</property>
  <property name="port">11099</property>
  <property name="description">The listening socket for the Naming service</property>
</bean>
```

- Step 4** Save the file.
- Step 5** Repeat [Step 1](#) through [Step 4](#) in the bindings-jboss-beans.xml file for the SDP profile.

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

## Setting Up Security Configuration

You need to set up security configuration in the Smart+Connected PS application for the following:

- Disabling the JMS message security, its value is set to 'true' by default.
- Authenticating LDAP users of the Smart+Connected PS application.

To set up security configuration, perform the following steps:

**Step 1** To disable the JMS message security:

- In the `$JBOSS_HOME/server/scps/deploy/hornetq/hornetq-configuration.xml` file, add the tag `<security-enabled>>false</security-enabled>` after the `</security-settings>` end tag.
- Save the file.

The JMS message security is now set to false.

**Step 2** To enable the LDAP authentication for application users:

- In the `$JBOSS_HOME/server/scps/conf/login-config.xml` file, search for the following text:

```
<application-policy name="JBossWS">
  <authentication>
    <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule"
      flag="required">
      <module-option
name="usersProperties">props/jbossws-users.properties</module-option>
      <module-option
name="rolesProperties">props/jbossws-roles.properties</module-option>
      <module-option name="unauthenticatedIdentity">anonymous</module-option>
    </login-module>
  </authentication>
</application-policy>
```

- Add the following code after the preceding text:

```
<application-policy name="SDP">
  <authentication>
    <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
      flag="sufficient">
      <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.SDPDataSourceLoginMod
ule</module-option>
      <module-option name="jndiName">java:jdbc/scc</module-option>
      <module-option name="debug">true</module-option>
    </login-module>
    <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
      flag="sufficient">
      <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.ldap.SDPLdapLoginModu
le</module-option>
      <module-option name="jndiName">java:jdbc/scc</module-option>
      <module-option
name="initialContextFactory">com.sun.jndi.ldap.LdapCtxFactory</module-option>
      <module-option
name="connectionURL">ldap://ldap.example.com:389</module-option>
      <module-option
name="connectionUsername">uid=name1,ou=people,ou=com</module-option>
      <module-option name="connectionPassword">password123</module-option>
      <module-option name="authentication">simple</module-option>
      <module-option
name="userBase">ou=active,ou=employees,ou=people,o=example.com</module-option>
      <module-option name="userSearchMatching">uid={0}</module-option>
```

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

```
<module-option name="userSearchSubtree">true</module-option>
<module-option name="debug">true</module-option>
</login-module>
</authentication>
</application-policy>
```

- c. Replace the following LDAP server and LDAP user details with their actual values in the code that you added in [Step 2 b.](#):

- connectionURL
- connectionUsername
- connectionPassword
- authentication
- userBase
- userSearchMatching
- userSearchSubtree



**Note** If LDAP does not require authentication or uses anonymous bind, the connectionUsername and connectionPassword values can be left blank.

- d. Save the file.  
The LDAP configuration is complete.

## Setting Up Java Messaging Service (JMS)

- [Creating a Connection Factory, page 2-19](#)
- [Creating an Event Topic, page 2-21](#)
- [Configuring an Event Topic, page 2-22](#)
- [Creating a Queue, page 2-23](#)

### Creating a Connection Factory

You need to create a connection factory in the SDP and Smart+Connected PS application.

- [Creating a Connection Factory in the SDP, page 2-19](#)
- [Creating a Connection Factory in the Smart+Connected PS, page 2-21](#)

#### Creating a Connection Factory in the SDP

You need to create a connection factory in the SDP for the Smart+Connected PS application to work properly.

To create a connection factory in the SDP, perform the following steps:

- Step 1** Navigate to the `$JBOSS_HOME/server/<SDP_PROFILE_DIR>/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.

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

Where, `<SDP_PROFILE_DIR>` is the SDP JBoss profile directory.

**Step 2** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="NettyConnectionFactory">
  <connectors>
    <connector-ref connector-name="netty" />
  </connectors>
  <entries>
    <entry name="/ConnectionFactory" />
    <entry name="/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 3** Replace `'/ConnectionFactory'` with `'/SDPXConnectionFactory'` as follows:

```
<entries>
  <entry name="/SDPXConnectionFactory" />
  <entry name="/XAConnectionFactory" />
</entries>
```

**Step 4** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="InVMConnectionFactory">
  <connectors>
    <connector-ref connector-name="in-vm" />
  </connectors>
  <entries>
    <entry name="/ConnectionFactory" />
    <entry name="/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 5** Replace `'/ConnectionFactory'` with `'/SDPXConnectionFactory'` as follows:

```
<entries>
  <entry name="/SDPXConnectionFactory" />
  <entry name="/XAConnectionFactory" />
</entries>
```

**Step 6** Save the file.

The connection factory is created in the SDP.

---

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

## Creating a Connection Factory in the Smart+Connected PS

To create a connection factory in the Smart+Connected PS, perform the following steps:

**Step 1** Navigate to the `$JBOSS_HOME/server/scps/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.

**Step 2** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="NettyConnectionFactory">
  <connectors>
    <connector-ref connector-name="netty" />
  </connectors>
  <entries>
    <entry name="/ConnectionFactory" />
    <entry name="/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 3** Replace `'/ConnectionFactory'` with `'/jms/ipsConnectionFactory'` as follows:

```
<entries>
  <entry name="/jms/ipsConnectionFactory" />
  <entry name="/XAConnectionFactory" />
</entries>
```

**Step 4** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="InVMConnectionFactory">
  <connectors>
    <connector-ref connector-name="in-vm" />
  </connectors>
  <entries>
    <entry name="java:/ConnectionFactory" />
    <entry name="java:/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 5** Replace `'/ConnectionFactory'` with `'/jms/ipsConnectionFactory'` as follows:

```
<entries>
  <entry name="java:/jms/ipsConnectionFactory" />
  <entry name="java:/XAConnectionFactory" />
</entries>
```

**Step 6** Save the file.

The connection factory for the Smart+Connected PS is created.

## Creating an Event Topic

You need to create an event topic in the SDP server.

To create an event topic, perform the following steps in the SDP server:

**Step 1** Navigate to the `$JBOSS_HOME/server/<SDP_PROFILE_DIR>/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.

Where, `<SDP_PROFILE_DIR>` is the SDP JBoss profile directory.

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

**Step 2** In the hornetq-jms.xml file, search for the following text:

```
<queue name="ExpiryQueue">
  <entry name="/queue/ExpiryQueue"/>
</queue>
```

**Step 3** At the end of the preceding text, add an entry for “/jms/sdp.event.Topic” as follows:

```
<topic name="sdp.event.Topic">
<entry name="/jms/sdp.event.Topic"/>
</topic>
```

**Step 4** Save the file.

An event topic is created in the SDP server.

---

## Configuring an Event Topic

After creating an event topic in the SDP, perform the following steps to configure events in the SDP server:

**Step 1** In a file browser, navigate to the `$JBOSS_HOME/server/<SDP_PROFILE_DIR>/deploy/hornetq` directory, and open the `hornetq-configuration.xml` file.

Where, `<SDP_PROFILE_DIR>` is the SDP JBoss profile directory.

**Step 2** In the `hornetq-configuration.xml` file, add the following to disable the JMS message security:

```
<security-enabled>>false</security-enabled>
```



**Note** The value of the JMS message security is set to ‘true’ by default.

---

**Step 3** Navigate to `$JBOSS_HOME/bin`, and open the `run.sh` file for the SDP profile.

**Step 4** In the `run.sh` file, search for the following text:

```
JAVA_OPTS="$ {JAVA_OPTS:--Dprogram.name=$PROGNAME}
-DANTLR_USE_DIRECT_CLASS_LOADING=true -Dshared.dir=$JBOSS_HOME/shared
-Dcom.sun.xml.bind.v2.bytecode.ClassTailor.noOptimize=true
-Dsdp.af.cache.root=$JBOSS_HOME/server/default/tmp"
```

**Step 5** Add the following command line to the text that you have searched for:

```
"-Dsdp.event.config.mode=global"
```

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

```
JAVA_OPTS="$ {JAVA_OPTS:--Dprogram.name=$PROGNAME}
-DANTLR_USE_DIRECT_CLASS_LOADING=true -Dsdp.event.config.mode=global
-Dshared.dir=$JBOSS_HOME/shared
-Dcom.sun.xml.bind.v2.bytecode.ClassTailor.noOptimize=true
-Dsdp.af.cache.root=$JBOSS_HOME/server/default/tmp"
```

**Step 6** Save the file.

---



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

## Creating a Queue

You need to create a queue in the Smart+Connected PS application server.

To create a queue, perform the following steps in the Smart+Connected PS application server:

- 
- Step 1** Navigate to the `$JBOSS_HOME/server/scps/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.
- Step 2** In the `hornetq-jms.xml` file, search for the following text:
- ```
<queue name="ExpiryQueue">
  <entry name="/queue/ExpiryQueue"/>
</queue>
```
- Step 3** After the preceding text, add an entry for “/jms/ipsQueue” as follows:
- ```
<queue name="ipsQueue">
  <entry name="/jms/ipsQueue"/>
</queue>
```
- Step 4** Save the file.
- A queue for the Smart+Connected PS application is created.
- 

## Setting Up Library

To set up the library, perform the following steps in the Smart+Connected PS application server:


- 
- Step 1** Copy the following jar files to the `$JBOSS_HOME/server/scps/lib` directory:
- `ojdbc14.jar`
  - `sdp-authmodules.jar`—Available at the `<SDP_INSTALL_DIRECTORY>/sdp/bin/jars` location on the server where the SDP has been installed.
- Step 2** Navigate to the `$JBOSS_HOME/server/scps/lib` directory, and provide the required permissions to the saved files (`ojdbc14.jar` and `sdp-authmodules.jar`) by entering the following command:
- ```
chmod 755 *
```
-

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

## 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 application. The BIRT runtime reporting engine is automatically installed while installing the Smart+Connected PS application.

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

- 
- Step 1** Create the 'SCPS\_Log' directory in the `<PS_INSTALL_DIRECTORY>`, and provide the read and write permissions to the users who run the JBoss profile for the Smart+Connected PS application.
- Step 2** Navigate to the `$JBOSS_HOME/server/scps/deploy/` directory, and open the 'jboss-logging.xml' file in a text editor.
- Step 3** Below the existing 'periodic-rotating-file-handler' tag, add the following text:
- ```
<periodic-rotating-file-handler
```

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

```

        file-name="<PS_INSTALL_DIRECTORY>/SCPS_Log/PS_Server.log"
        name="SDPFILEHANDLER"
        autoflush="true"
        append="true"
        suffix=".yyyy-MM-dd">
    <error-manager>
        <only-once/>
    </error-manager>
    <formatter>
        <pattern-formatter pattern="%d %-5p [%c] (%t) %s%E%n"/>
    </formatter>
</periodic-rotating-file-handler>

```

For example:

```

<periodic-rotating-file-handler
    file-name="/home/scc-qa/scps/SCPS_Log/PS_Server.log"
    name="SDPFILEHANDLER"
    autoflush="true"
    append="true"
    suffix=".yyyy-MM-dd">
    <error-manager>
        <only-once/>
    </error-manager>
    <formatter>
        <pattern-formatter pattern="%d %-5p [%c] (%t) %s%E%n"/>
    </formatter>
</periodic-rotating-file-handler>

```

The logs are created after the application is up and running at the location that you had specified in the 'file-name' attribute.

**Step 4** Search for the following text:

```

<root-logger>
    <!-- Set the root logger priority via a system property, with a default value. -->
    <level name="${jboss.server.log.threshold:INFO}"/>
    <handlers>
        <handler-ref name="CONSOLE"/>
        <handler-ref name="FILE"/>
    </handlers>
</root-logger>

```

Replace the text as follows:

```

<root-logger>
    <!-- Set the root logger priority via a system property, with a default value. -->
    <level name="${jboss.server.log.threshold:INFO}"/>
    <handlers>
        <handler-ref name="CONSOLE"/>
        <handler-ref name="FILE"/>
        <handler-ref name="SDPFILEHANDLER"/>
    </handlers>
</root-logger>

```

**Step 5** Save the 'jboss-logging.xml' file.

Logging is configured for the Smart+Connected PS application.

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

## Configuring the Properties Files

- [About the Properties Files, page 2-26](#)
- [Updating the Properties Files, page 2-33](#)

### About the Properties Files

- [About the LDAP Properties File, page 2-26](#)
- [About the JMS Properties File, page 2-29](#)
- [About the Reservation Properties File, page 2-30](#)
- [About the Notificationservice Properties File, page 2-32](#)

### 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.

[Table 2-3](#) 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 2-3**      **LDAP Properties**

Property Name	Description
ldap.host.name (Mandatory)	The hostname of the LDAP server.
ldap.host.port (Mandatory)	The port number of the LDAP server.
ldap.users.DN (Mandatory)	The base DN to be used for doing a LDAP search.
ldap.user.id (Mandatory)	The attribute to identify a user.
ldap.user.fullname	The attribute to identify the full name of the user.
ldap.user.firstname	The attribute to identify the first name of the user.
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.
ldap.user.lastname.defaultvalue	The default value to be used if the attribute for the last name is invalid.
ldap.user.title	The attribute to identify the title of the user.
ldap.user.email	The attribute to identify the e-mail ID of the user.
ldap.user.mobile	The attribute to identify the mobile number of the user.
ldap.user.telephonenumber	The attribute to identify the telephone number of the user.
ldap.user.email.defaultValue	The default value to be used if the attribute for the e-mail ID is invalid.

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

**Table 2-3 LDAP Properties (continued)**

Property Name	Description
ldap.user.companyname	The attribute to identify the name of the company in which the user is employed.
ldap.bind.pwd (Mandatory	The bind password in case of a non-anonymous bind.
ldap.bind.username (Mandatory	The bind username in case of a non-anonymous bind.
ldap.user.companyname.defaultValue	The default value to be used if the attribute for the company name is invalid.
ldap.ssl.enabled	This attribute indicates if a connection is to be made over SSL (such as, ldap) or not. The value should be set to true, in case access is over SSL.
ldap.common.name	The attribute to identify the common name of the user (first name+last name).
ldap.user.number	The attribute to identify the employee number of the user.
ldap.user.empid	The attribute to identify the employee ID of the user.
ldap.user.designation	The attribute to identify the designation of the user.
ldap.user.businessUnit	The attribute to identify the business unit which the user is a part of.
ldap.user.photo	The attribute to identify the user's photo that is uploaded in the active directory. The photo has to be of the size 350*420 pixel.
ldap.user.employeeid	The attribute to identify the employee ID of the user.
ldap.user.nickname	The attribute to identify the nickname of the user, if any.
ldap.user.departmentno	The attribute to identify the department of the enterprise with which the user is associated.
ldap.user.departmentname	The attribute to identify the name of the department with which the user is associated.
ldap.user.managerempno	The attribute to identify the employee ID of the user's manager.
ldap.user.managername	The attribute to identify the name of the user's manager.
ldap.user.employeetype	The attribute to identify whether the nature of the user's employment is permanent or contractual.
ldap.user.worktype	The attribute to identify whether the worker has been assigned a location or is a mobile worker.

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

**Table 2-3 LDAP Properties (continued)**

Property Name	Description
ldap.user.publishmobile	This attribute indicates if the user's mobile number is to be displayed or not. The value should be set to yes, if the user's mobile number is to be displayed.
ldap.user.publishpager	This attribute indicates if the user's pager number is to be displayed or not. The value should be set to yes, if the user's pager number is to be displayed.
ldap.user.functional_unit	The attribute to identify the functional unit of the enterprise with which the user is associated.
ldap.user.building	The attribute to identify the building where the user is seated, if a location is assigned to the user.
ldap.user.contractcompany	The attribute to identify the name of the vendor company, if the user is a contract employee.
ldap.user.initial	The attribute to identify the initials of the user.
ldap.user.floor	The attribute to identify the floor where the user is seated, if a location is assigned to the user.
ldap.user.mailstop	The attribute to identify the central location where the mails are sent.
ldap.user.checkedInStatus	The attribute to identify the check-in status of the user.
ldap.user.publishloc	This attribute indicates if the user's location is to be displayed or not. The value should be set to yes, if the user's location is to be displayed.
ldap.user.pager	The attribute to identify the user's pager number.
ldap.user.spaceid	The attribute to identify the workspace where the user is seated, if a location is assigned to the user.
ldap.user.spacepolicy	This attribute is for future enhancements in the solution. You can leave this value blank.
ldap.user.checkedInLocation	The attribute to identify the location where the user has checked in.
ldap.user.vpdesc	The attribute to identify the vice president of the enterprise where the user is employed.
ldap.user.snr_vpdesc	The attribute to identify the senior vice president of the enterprise where the user is employed.
ldap.user.managermail	The attribute to identify the e-mail ID of the user's manager.
ldapUrl (Mandatory)	The LDAP URL to access the active directory.
ldapBase	The base DN to be used for doing a LDAP search.
ldapUserName (Mandatory)	The bind username in case of a non-anonymous bind.

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

**Table 2-3 LDAP Properties (continued)**

Property Name	Description
ldapMaxReturnSize (Mandatory)	The maximum number of users whose details will be fetched in one batch from the LDAP.
ldap.user.isroom (Mandatory)	The attribute to identify if the resource is a user or a room.

## About the JMS Properties File

Table 2-4 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 2-4 JMS Properties**

Property Name	Description	Sample Value
ips.jms.jndi	Identifies the JNDI name for the ips queue.	jms/ipsQueue <sup>1</sup>
ips.jms.connectionfactory	Identifies the Connection factory for the ips queue.	jms/ipsConnectionFactory <sup>1</sup>
ips.jms.initialContext	Identifies the Smart+Connected PS initial context url. 11099 is the listening socket port that is defined as value for the listening socket port for the Naming service (which you set up in <a href="#">Step 3</a> of the “ <a href="#">Setting Up Port</a> ” section on page 2-17).	jnp://localhost:11099
URL	Identifies the SDP topic URL. 11099 is the listening socket port that is defined as value for SDP the listening socket port for the Naming service (which you set up in <a href="#">Step 5</a> of the “ <a href="#">Setting Up Port</a> ” section on page 2-17).	jnp://<SDP_IPADDRESS>:11099 For example, jnp://10.10.10.10:11099
username	Identifies the SDP domain username.	admin
password	Identifies the SDP domain password.	admin
providerurl	Identifies the Smart+Connected PS Queue URL. 11199 is the listening socket port that is defined by adding the listening socket port for the Naming service (which you had set up in <a href="#">Step 3</a> of the “ <a href="#">Setting Up Port</a> ” section on page 2-17) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).	jnp://localhost:11199

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

**Table 2-4 JMS Properties (continued)**

Property Name	Description	Sample Value
provideruserName	Identifies the Smart+Connected PS domain admin username.	admin
providerpassword	Identifies the Smart+Connected PS domain admin password.	admin

1. This property value should not be changed.

## About the Reservation Properties File

Table 2-5 describes the reservation.properties and the default value for each property.

**Table 2-5 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



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

**Table 2-5 Reservation Properties (continued)**

Property	Description	Default Value
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=
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 profile.	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>/ipsapp. Where, 'host' is the IP address or the DNS hostname of the host on which the JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in <a href="#">"Setting Up Port" section on page 2-17</a> ) and the "ports-01" offset value in the bindings-jboss-beans.xml file (which is 100 by default).
IP_PHONE_DATE_FORMAT	Defines the format of the date as supported by CUCM.	MM/DD/YY.

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

**Table 2-5 Reservation Properties (continued)**

Property	Description	Default Value
wholeDayBookingStart Hour	Defines the start hour time for the whole day booking. To be given in a 24 hour format.	09
wholeDayBookingStart Minute	Defines the start minute time for the whole day booking.	30
wholeDayBookingEnd Hour	Defines the end hour time for the whole day booking. To be given in a 24 hour format.	17
wholeDayBookingEnd Minute	Defines the end minute time for the whole day booking.	30
availableSoonWindow	Defines the time from which the workspace should be indicated as “Available Soon” when reserved.	0.04167 (which is equal to an hour).



**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.

## About the Notificationservice Properties File

Table 2-6 describes the notificationservice.properties and the default value of each property.

**Table 2-6 Notificationservice Properties**

Field	Description	Sample Value
mail.transport.host	This attribute defines the mail server to be used.	mail.sample.com
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

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

**Table 2-6      *Notificationservice Properties***

Field	Description	Sample Value
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 2-33](#)
- [Setting Up Reservation and Notification Properties, page 2-33](#)

### 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` directory, 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 2-4](#).
- Step 4**    Make a note of the location where you save the LDAP.properties and pvoJms.properties files. This location is used for setting up run parameters for the JBoss start-up configuration.
- 

### 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 `$JBoss_HOME/server/scps/deploy/ipsapp.war` file, and double-click this file to open the Archive Manager screen.
- Step 2**    Navigate to `/WEB-INF/classes`, select the following files, and extract content of the files to a suitable location, such as Desktop:
- Reservation.properties
  - notificationservice.properties
- Step 3**    Update the Reservation.properties file:
- a. Open the Reservation.properties file, which is available at the specified location, in the edit mode and update the property values as described in [Table 2-5](#).
  - b. Save and close the file.

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

- Step 4** Update the notificationservice.properties file:
- Open the notificationservice.properties file, which is available at the specified location, in the edit mode and update the property values as described in [Table 2-6](#).
  - Save and close the file.
- Step 5** Navigate to the directory containing the `$JBOSS_HOME/server/scps/deploy/ipsapp.war` file, and double-click this file to open the Archive Manager screen.
- Step 6** Navigate to `/WEB-INF/classes`, and click **Add**.
- Step 7** Browse and select the following updated files, and click **OK**:
- Reservation.properties
  - notificationservice.properties

The updated file is replaced in the ipsapp.war file. Verify that the date and time of the Reservation.properties and the notificationservice.properties files are updated to the current date and time.

---

## Setting Up Run Parameters

To set up run parameters, perform the following steps:

- Step 1** Navigate to `$JBOSS_HOME/bin`, copy the 'run.sh' file, and create a file with the name 'run\_scps.sh'.
- Step 2** To allow JMS to work in the Smart+Connected PS application through the SDP, set the 'sdp.event.config.mode' property in the 'run\_scps.sh' file of the Smart+Connected PS profile:
- In the run\_scps.sh file, search for the following text:
 

```
# Setup JBoss specific properties
JAVA_OPTS="${JAVA_OPTS:+$JAVA_OPTS -Dprogram.name=$PROGNAME}"
JAVA_OPTS="${JAVA_OPTS:--Dprogram.name=$PROGNAME}"
```
  - Add the following text:
 

```
JAVA_OPTS="${JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true}"
```
- Step 3** Configure the LDAP properties:
- In the run\_scps.sh file, search for the following text:
 

```
JAVA_OPTS="${JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true}"
```
  - Add the following text at the end of the searched text before the ("):
 

```
-Dcom.cisco.sdp.ldap.configfilepath=<path to LDAP.properties file>/LDAP.properties
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties
```

For example:

```
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties
```
  - After adding the command line, the text is displayed as follows:

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties"
```

**Step 4** Configure the application properties:

a. In the run\_scps.sh file, search for the following text:

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true
```

b. Add the following text at the end of the line before the ("):

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

For example:

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

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties"
```

**Step 5** Save and close the run\_scps.sh file.

## Setting Up the Push-to-Phone Feature

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

**Step 1** From the file browser, navigate to *\$JBoss\_HOME/bin* directory, and open the run\_scps.sh file.

**Step 2** In the run\_scps.sh file, search for the following text:

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global
```

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

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

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
-Djboss.net.proxyAuthenticatorClassName=java.net.Authenticator
-DUseSunHttpHandler=true"
```

**Step 4** Save the file.

**Send documentation comments to [scc-docfeedback@cisco.com](mailto: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 Create a simple SSL certificate keystore:

- a. Open a terminal and navigate to the `$JBoss_HOME/server/scps/conf` directory.
- b. Remove the existing `server.keystore` file.
- c. Navigate to the `$JAVA_HOME/bin` directory, and enter the following command to create a certificate and a storefile with the name 'server.keystore':

```
./keytool -genkey -alias <keystore alias> -keyalg RSA -keystore
$JBoss_HOME/server/scps/conf/server.keystore -validity <number of days>
```

For example:

```
./keytool -genkey -alias jbosshttps -keyalg RSA -keystore
$JBoss_HOME/server/scps/conf/server.keystore -validity 3650
```

You are prompted to specify the following required details:

- Enter keystore password—Specify a password for keystore. For example, password1. You also need to use the same keystore password when prompted.
- 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 certificate with a validity of *<number of days>* days is generated. You are prompted for the key password of the *<alias name>*.

- d. Press **Enter**.

The certificate is retained in the `server.keystore` file.

### Step 2 Configuring the JBoss server to create an SSL connector:

- a. Open a terminal and navigate to the `$JBoss_HOME/server/scps/deploy/jbossweb.sar` directory.
- b. Open the `server.xml` file in an edit mode, and uncomment the following text:

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
    port="${jboss.web.https.port}" address="${jboss.bind.address}"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
    keystorePass="rmi+ssl" sslProtocol = "TLS" />
```

- c. In the above text, replace the following:

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

- `${jboss.web.https.port}` with the unique port number that will be used as the SSL port (for example, 9001)
- `${jboss.server.home.dir}` with `$JBOSS_HOME/server/scps/conf/server.keystore`
- `rmi+ssl` with the keystore password (for example, password1)

## 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 2-37](#)
- [Configuring Installer for the iPhones, page 2-39](#)

## 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 the DNS hostname of the host on which the JBoss application server is set up and 'SSL port' is the value that appears in the output after starting the JBoss server. The 'SSL port' value is obtained by adding the `jboss.web.https.port` value (which you had set up in the [“Configuring the Secured URL” section on page 36](#)) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).



**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>`

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

Where, 'host' is the IP address or the DNS hostname of the host on which the JBoss application server is set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in [“Setting Up Port” section on page 2-17](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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.
- 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
```



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

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 ipsapp.war file:

- a. Double-click the ipsapp.war file from the `$JBOSS_HOME/server/scps/deploy/ipsapp.war` directory, and open the Archive Manager screen.
- 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 ipsapp.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 `$JBOSS_HOME/server/scps/deploy/ipsapp.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 JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in "[Setting Up Port](#)" section on page 2-17) and the "ports-01" offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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>`

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

Where, 'host' is the IP address or DNS hostname of the host on which the JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in [“Setting Up Port” section on page 2-17](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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 DNS hostname of the host on which the JBoss application server has been set up and 'SSL port' is the value that appears in the output after starting the JBoss server. The 'SSL port' value is obtained by adding the jboss.web.https.port value (which you had set up in the [“Configuring the Secured URL” section on page 2-36](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).



### 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 JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in [“Setting Up Port” section on page 2-17](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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
```

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

- 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 ipsapp.war file:
- Double-click the ipsapp.war file from the `$JBOSS_HOME/server/scps/deploy` 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 ipsapp.war file.
- 

## Setting Up 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 set up Jackrabbit, perform the following steps:

- 
- Step 1** Copy the jackrabbit.war file that is available in `<PS_INSTALL_DIRECTORY>/scps/bin/war` to `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:
- ```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/jackrabbit.war $JBOSS_HOME/server/scps/deploy
```
- Step 2** Navigate to the directory containing the `$JBOSS_HOME/server/scps/deploy/jackrabbit.war` file, and double-click this file to open the Archive Manager screen.
- Step 3** Navigate to `/WEB-INF/lib`, select the `jcr-2.0.jar` file, and extract content of the file to the following location:
- ```
$JBOSS_HOME/common/lib
```
- Step 4** Start the JBoss server.
- For more information on how to start the JBoss server, see the [“Starting the JBoss Server”](#) section on page 2-43.
- Ensure that the JBoss server is now up and running.
- Step 5** In a Web browser, enter the URL <http://host:port/jackrabbit>.
- Where, ‘host’ is the IP address or DNS hostname of the host on which the JBoss application server has been set up and ‘port’ is the Jboss binding server port that you had configured in the [“Setting Up Port”](#) section on page 2-17.
- The Content Repository Setup page appears.
- Step 6** Click **Create Content Repository**.
- The `$JBOSS_HOME/bin/jackrabbit` directory repository structure is created.
-

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

## 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 Light Weight Directory Access Protocol (LDAP).

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

To import SSL certificates, perform the following steps:

**Step 1** Using a terminal session, navigate to the `$JAVA_HOME/bin` directory, where the `$JAVA_HOME` environment variable is set to the `<JDK_INSTALL_LOCATION>` directory.

**Step 2** Enter the following command:

```
./keytool -import -alias <Alias Name> -file <certificate file name with complete path>
-keystore $JAVA_HOME/jre/lib/security/cacerts -storepass changeit
```

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

For example:

```
./keytool -import -alias CM -file /home/scc-qa/CM115.cer -keystore
/home/scc-qa/Desktop/jdk1.6.0_24/jre/lib/security/cacerts -storepass changeit
```



**Note** If you have installed JDK using an RPM bundle, then you need the SUDO access to add the certificate to the keystore.

A message prompts you to trust this certificate.

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

The certificates are imported.

**Step 4** In the `$JBOSS_HOME/bin/run_scps.sh` file, append the `JAVA_OPTS` line just before (") with the following line:

```
-Djavax.net.ssl.trustStore=$JAVA_HOME/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
-Djboss.net.proxyAuthenticatorClassName=java.net.Authenticator
-DUseSunHttpHandler=true
-Djavax.net.ssl.trustStore=/usr/java/default/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit"
```

**Step 5** Save the `run_scps.sh` file.

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

## Starting the JBoss Server

To start the JBoss application server for the Smart+Connected PS application, perform the following steps:

### Step 1 Ensure that:

- SDP is up and running without any binding offset value.
- The `$JAVA_HOME` environment variable is set to the location in which JDK is installed.
- The `$JBoss_HOME` environment variable is set to the complete path where the unzipped jboss-6.0.0 files are available.

### Step 2 Using a terminal, navigate to the `$JBoss_HOME/bin` directory, and run the following command:

```
./run_scps.sh -c scps -Djboss.service.binding.set=ports-01 -b 0.0.0.0
```

The JBoss application server starts. After the server initialization is complete, an output similar to the following is listed:

```
2012-11-20 11:41:31,360 INFO [org.apache.coyote.http11.Http11Protocol] (Thread-2)
Starting Coyote HTTP/1.1 on http-0.0.0.0-7101
```

The port value that appears in the output is the value obtained by adding the `HttpConnector` port value (which you had set up in “[Setting Up Port](#)” section on page 2-17) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

## Accessing the Application and Verifying the Installation

- [Smart+Connected PS Web Application](#), page 2-43

### Smart+Connected PS Web Application

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 DNS hostname of the host on which the JBoss application server has been set up and ‘port’ is the value that appears in the output after starting the JBoss server. The ‘port’ value is obtained by adding the `HttpConnector` port value (which you had set up in “[Setting Up Port](#)” section on page 2-17) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

- `https://<host>:<SSL port>/ipsapp`—To access the application in a secured environment.

Where, ‘host’ is the IP address or DNS hostname of the host on which the JBoss application server has been set up and ‘SSL port’ is the value that appears in the output after starting the JBoss server. The ‘SSL port’ value is obtained by adding the `jboss.web.https.port` value (which you had set up in the “[Configuring the Secured URL](#)” section on page 2-36) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

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

The Smart+Connected PS login page appears.

**Step 2** 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*.

## Smart+Connected PS Mobile Application

To install the Smart+Connected PS mobile application on your smartphone, perform the following steps:

- 
- Step 1** Open a web browser on your mobile device and enter the URL for the Smart+Connected PS mobile application. For example, `http://<IP Address>:<port #>/ipsapp/mobile_download/index.jsp`
- The Smart+Connected PS mobile application welcome screen appears.
- Step 2** Tap **Download**.
- The installer for the Smart+Connected PS mobile application is downloaded on your mobile device.
- Step 3** Tap the Smart+Connected installer to begin with the installation.
- The Smart+Connected PS mobile application is installed on your mobile device.
- Step 4** Tap the Smart+Connected PS icon on your mobile device.
- The Smart+Connected PS Login screen appears.
- Step 5** Enter the username and password in the Username and Password fields.
- Step 6** (Optional) Check the **Keep me signed in** check box if you do not want to be logged off automatically.
- Step 7** Tap **Login**.
- The Smart+Connected PS home screen appears.



**Note** The first login instance directs you to the Preferences screen, where you must set the default building or floor for yourself. After this is set, the next login instance directs you to the home screen.

## Installing on a Cluster Server Setup

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

1. [Installing the Application, page 2-47](#)
2. [Configuring Audio Notification to the Cisco IP Phone, page 2-47](#)
3. [Configuring the Database, page 2-47](#)

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

4. [Configuring the JBoss Profile, page 2-48](#)
5. [Setting Up Port, page 2-49](#)
6. [Setting Up Security Configuration, page 2-49](#)
7. [Setting Up Java Messaging Service \(JMS\), page 2-50](#)
8. [Setting Up Library, page 2-50](#)
9. [Setting Up the BIRT Engine, page 2-50](#)
10. [Configuring Logging, page 2-50](#)
11. [Configuring the Cluster Server Setup, page 2-50](#)
12. [Configuring the Properties Files, page 2-54](#)
13. [Setting Up Run Parameters, page 2-54](#)
14. [Setting Up the Push-to-Phone Feature, page 2-54](#)
15. [Configuring Installer for the Mobile Devices, page 2-54](#)
16. [Setting Up Apache Jackrabbit, page 2-58](#)
17. [Configuring the Jackrabbit Repository, page 2-59](#)
18. [Importing SSL Certificates, page 2-60](#)
19. [Starting the Cluster and Proxy, page 2-61](#)
20. [Accessing the Application and Verifying the Installation, page 2-62](#)

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

## About Clustering

A JBoss server cluster consists of multiple JBoss server instances running simultaneously and working together to provide increased scalability, reliability, and high availability. A cluster appears to clients to be a single JBoss 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 JBoss version.

An example of clustered deployment in a distributed environment is as follows:

- The database is non-clustered.
- The application servers are clustered.
- Two virtual machines host the application servers. The application is deployed on these two virtual machines, Node 1 and Node 2.
- One virtual machine hosts the proxy server. This proxy server acts as a software load balancer.

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

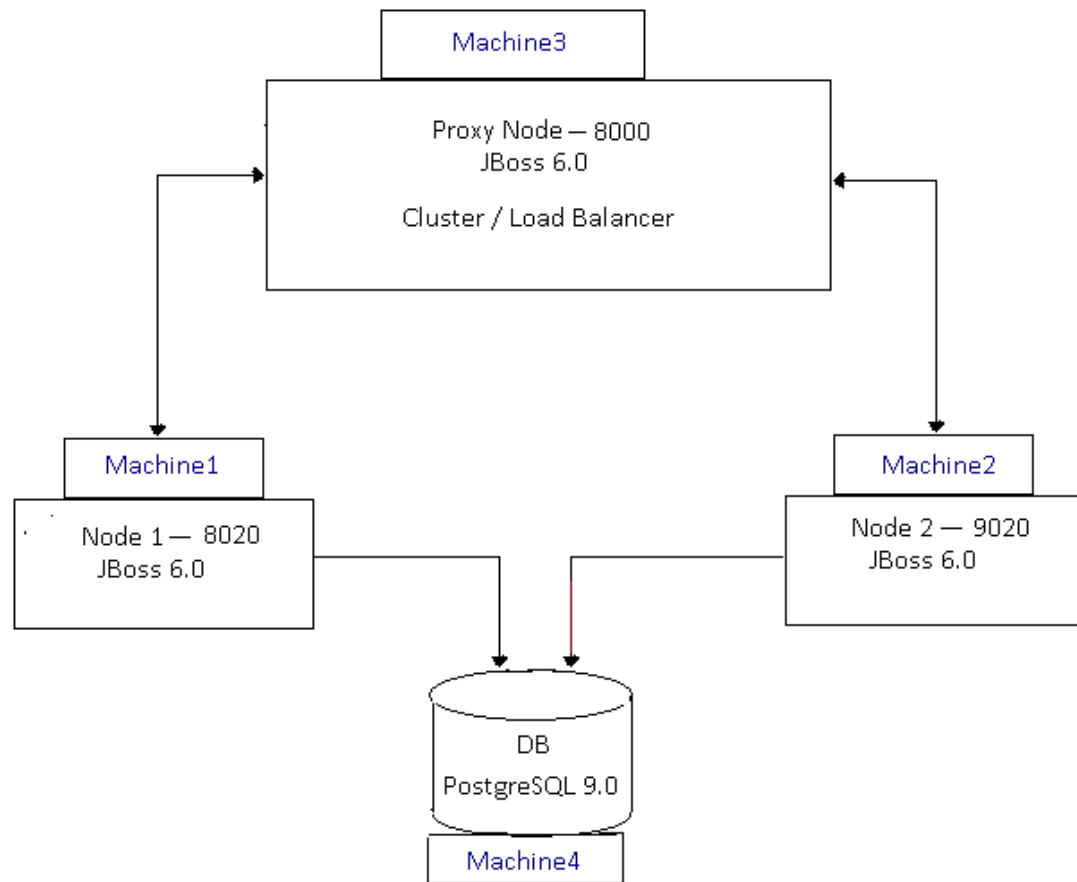
The requirements for the clustered deployment in this example, includes the following:

- Machine 1: JBoss Server Node 1 (JBoss 6.0)
- Machine 2: JBoss Server Node 2 (JBoss 6.0)
- Machine 3: Proxy Node (JBoss 6.0)
- Machine 4: Database Server (PostgreSQL 9.0)



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

**Figure 2-1 Example of a Clustering Setup**



## Installing the Application

You need to install the Smart+Connected PS application on the Node 1 and Node 2 servers.

For information on how to install the Smart+Connected PS application, see the [“Installing the Application”](#) section on page 2-13.

## Configuring Audio Notification to the Cisco IP Phone

You need to configure audio notification to the Cisco IP phone on the Node 1 and Node 2 servers.

For information on how to configure audio notification to the Cisco IP phone, see the [“Configuring Audio Notification to the Cisco IP Phone”](#) section on page 2-15.

## Configuring the Database

For information on how to configure the database, see the [“Creating JBoss Profile”](#) section on page 2-15.

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

## Configuring the JBoss Profile

You need to configure the JBoss profile on the Node 1 and Node 2 servers for a cluster deployment. To configure the JBoss profile, perform the following steps on both the Node 1 and Node 2 servers:

- 
- Step 1** Download the jboss-6.0.0.Final.zip file.
- JBoss is open source, and you can download it from the Internet. For example:
- <http://sourceforge.net/projects/jboss/files/JBoss/JBoss-6.0.0.Final/jboss-as-distribution-6.0.0.Final.zip/download>
- Step 2** Create a directory named 'jboss', and unzip the jboss-6.0.0.Final.zip file into it.
- Step 3** Set the `$JBOSS_HOME` and `$JAVA_HOME` environment variables by entering the following commands:
- ```
$ export JAVA_HOME=<JDK_INSTALL_LOCATION>
$ export JBOSS_HOME=<JBOSS_INSTALL_LOCATION>
```

Where, `<JBOSS_INSTALL_LOCATION>` is the complete path where the unzipped jboss-6.0.0 files are available and `<JDK_INSTALL_LOCATION>` is the complete path where you have installed jdk1.6.0\_24.



**Note** You can also add the preceding commands to the user's profile script so that the `$JBOSS_HOME` and `$JAVA_HOME` environment variables are automatically set up during login.

---

- Step 4** Navigate to the server directory in `$JBOSS_HOME` by entering the following command:
- ```
cd $JBOSS_HOME/server
```
- Step 5** Copy the 'all' directory with the name 'scps' by entering the following command:
- ```
cp -R all scps
```
- The 'scps' directory is created under the `$JBOSS_HOME/server` directory. The 'scps' directory is used as the Smart+Connected PS application profile.
- Step 6** Copy the ipsapp.war file, available in `<PS_INSTALL_DIRECTORY>/scps/bin/war`, to the `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:
- ```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/ipsapp.war $JBOSS_HOME/server/scps/deploy
```
- Step 7** Create a datasource file so that the Smart+Connected PS application communicates with the database machine:

- a. Create the oracle-ds.xml file under the 'scps/deploy' directory with the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<local-tx-datasource>
<jndi-name>jdbc/scc</jndi-name>
<connection-url>jdbc:oracle:thin:@IPaddress:DBport:SID</connection-url>
<driver-class>oracle.jdbc.OracleDriver</driver-class>
<user-name>DBusername</user-name>
<password>DBpassword</password>
<exception-sorter-class-name>
org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter
</exception-sorter-class-name>
</local-tx-datasource>
</datasources>
```

- b. Replace the following text with their actual values in the code that you had added in [Step 7 a.](#):

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

- ‘IPaddress’ with the database server IP address or DNS hostname
  - ‘SID’ with the oracle SID
  - ‘DBport’ with database port number (default is 1521, if not changed)
  - ‘DBusername’ with the database schema username
  - ‘DBpassword’ with the database schema password
- c. Save the file.
  - d. Provide the executable permissions to the newly created oracle-ds.xml file by entering the following command:
 

```
chmod 755 oracle-ds.xml
```

**Step 8** Add an entry for scanning deployers:

- a. Navigate to the `$JBOSS_HOME/server/scps/deployers` directory, and open the `scanning-deployers-jboss-beans.xml` file.
- b. Search for the following text:

```
<install method="addIgnored">
  <parameter>java.lang.LinkageError</parameter>
</install>
```

- c. Add the following code after the searched text.

```
<install method="addIgnored">
  <parameter>java.lang.reflect.MalformedParameterizedTypeException</parameter>
</install>
```

- d. Save the file.

**Step 9** Update the `run.conf` file to increase the memory:

- a. Open the `run.conf` file available in `$JBOSS_HOME/bin` and search for the following text:

```
JAVA_OPTS="-Xms128m -Xmx512m -XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

Replace with the following text:

```
JAVA_OPTS="-Xms256m -Xmx1024m -XX:MaxPermSize=512m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

- b. Save the file.

## Setting Up Port

You need to set up a port for the Smart+Connected PS application by changing the default port values on the Node 1 and Node 2 servers.

For more information on how to set up the port, see the [“Setting Up Port” section on page 2-17](#).

## Setting Up Security Configuration

You need to set up security configuration on the Node 1 and Node 2 servers for the following:

- Disabling the JMS message security, its value is set to ‘true’ by default.

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

- Authenticating LDAP users of the Smart+Connected PS application.

For more information on how to set up security configuration on the Node 1 and Node 2 servers, see the [“Setting Up Security Configuration” section on page 2-18](#).

## Setting Up Java Messaging Service (JMS)

For more information on how to set up JMS on the Node 1 and Node 2 servers, see the [“Setting Up Java Messaging Service \(JMS\)” section on page 2-19](#).

## Setting Up Library

To set up the library, perform the following steps in the Smart+Connected PS application server on the Node 1 and Node 2 servers:

- 
- Step 1** Copy the following jar files to the `$JBOSS_HOME/server/scps/lib` directory:
- `ojdbc14.jar`
  - `sdp-authmodules.jar`—Available at the `<SDP_INSTALL_DIRECTORY>/sdp/bin/jars` location on the server where the SDP has been installed.
- Step 2** Provide the required permissions to both the jar files that you have copied by entering the following command:
- ```
chmod 755 *
```

## 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.

For more information on how to set up the BIRT engine on the Node 1 and Node 2 servers, see the [“Setting Up the BIRT Engine” section on page 2-24](#).

## Configuring Logging

For more information on how to configure logging on the Node 1 and Node 2 servers, see the [“Configuring Logging” section on page 2-24](#).

## Configuring the Cluster Server Setup

- [Installing mod\\_cluster on the Proxy Node, page 2-51](#)
- [Configuring Cluster on Nodes, page 2-53](#)

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

## Installing mod\_cluster on the Proxy Node

The mod\_cluster is an httpd-based load balancer that uses a communication channel for forwarding requests from httpd to a set of application server nodes. The application server nodes use this connection to transmit the server-side load balance factors and events back to httpd using a set of HTTP methods.

To install mod\_cluster on the proxy node, perform the following steps:

- 
- Step 1** Create a directory in your local system where you want to install the mod\_cluster binary bundle.
- Step 2** Download the Linux 64-bit mod\_cluster 1.1.0 bundle.
- The mod\_cluster is open source, and you can download it from the Internet. For example:
- [http://www.jboss.org/mod\\_cluster/downloads.html](http://www.jboss.org/mod_cluster/downloads.html)
- Step 3** Save and untar the mod\_cluster binary bundle in the directory that you had created in [Step 1](#).
- The directory where you have extracted the mod\_cluster bundle is referred as `<MOD_CLUSTER_HOME>`.
- Step 4** Navigate to the `<MOD_CLUSTER_HOME>/opt/jboss/httpd/sbin` directory and run the “installhome.sh” file.
- The httpd now runs on port “8000”.

- Step 5** To allow the cluster nodes in the network to communicate with the proxy, perform the following:

- a. Navigate to the following location:

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/httpd/conf/
```

- b. Open the httpd.conf file and search for the following text:

```
<Directory />
    Order deny,allow
    Deny from all
</Directory>
```

- c. Replace the default values in the searched text as follows:

```
<Directory />
    Order deny,allow
    Allow from all
</Directory>
```

- d. Save the file.



**Note** By default, mod\_cluster communicates only with the server instances that run on localhost. [Step 5](#) should be performed to allow mod\_cluster to communicate with the proxy.

---

- Step 6** To modify the directory access for Manager Module, perform the following:

- a. Navigate to the following location:

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/httpd/conf/
```

- b. Open the httpd.conf file and search for the following text:

```
<IfModule manager_module>
    Listen 127.0.0.1:6666
    ManagerBalancerName mycluster
    <VirtualHost 127.0.0.1:6666>
    <Directory />
```

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

```

        Order deny,allow
        Allow from all
    </Directory>

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

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

</VirtualHost>
</IfModule>

```

- c. Replace the directory access of the Manager Module in the <Location /mod\_cluster\_manager> element as follows:

```

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

```

After replacing, the text is displayed as follows:

```

<IfModule manager_module>
    Listen 127.0.0.1:6666
    ManagerBalancerName mycluster
    <VirtualHost 127.0.0.1:6666>
    <Directory />
        Order deny,allow
        Allow from all
    </Directory>

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

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

</VirtualHost>
</IfModule>

```

- d. Save and close the file.

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

## Configuring Cluster on Nodes

To configure cluster on nodes, perform the following steps on the Node 1 and Node 2 servers:

### Step 1 Update the server.xml file:

- a. Navigate to the `$JBOSS_HOME/server/scps/deploy/jbossweb.sar` directory, and open the `server.xml` file.

- b. In the `server.xml` file, search for the following text:

```
<Engine name="jboss.web" defaultHost="localhost">
```

- c. Add `jvmRoute` to the Engine “jboss.web”. For example:

- For Node 1:

```
<Engine name="jboss.web" defaultHost="localhost" jvmRoute="node1">
```

- For Node 2:

```
<Engine name="jboss.web" defaultHost="localhost" jvmRoute="node2">
```

- d. In the `server.xml` file, uncomment the following valve, which is commented by default:

```
<Valve className="org.jboss.web.tomcat.service.sso.ClusteredSingleSignOn" />
```



**Note** The valve is uncommented to enable single sign on across web applications deployed on all the hosts in a cluster.

- e. In the `server.xml` file, set the HTTP port, for example, 8020 for Node 1 and 9020 for Node 2:

1. Search for the following text:

```
<!-- A HTTP/1.1 Connector on port 8080 -->
<Connector protocol="HTTP/1.1" port="${jboss.web.http.port}"
address="${jboss.bind.address}"
redirectPort="${jboss.web.https.port}" />
```

2. Replace the `port="${jboss.web.http.port}"` with `port="8020"` for Node 1 and `port="9020"` for Node 2.

- f. Save the `server.xml` file.

### Step 2 Add the proxy hostname and port in the proxyList:

- a. In a file browser, navigate to the `$JBOSS_HOME/server/scps/deploy/mod_cluster.sar/META-INF` directory.

- b. Open the `mod_cluster-jboss-beans.xml` file and search for the following text:

```
<property name="proxyList">
```

- c. Add proxies in the `proxyList` property as follows:

```
<property name="proxyList">${jboss.mod_cluster.proxyList:address:port}</property>
```



**Note** In the `proxyList` property format, the “address:port” refers to the host IP address and port where the proxy is running. The port number is 8000 that you had configured in [Step 4](#) in the “[Installing mod\\_cluster on the Proxy Node](#)” section on page 2-51.

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

- d. Save the mod\_cluster-jboss-beans.xml file.
- 

## Configuring the Properties Files

You need to configure the LDAP.properties, pvoJms.properties, Reservation.properties, and notificationservice.properties files on the Node 1 and Node 2 servers.

For information on how to configure the properties files, see the [“Configuring the Properties Files” section on page 2-26](#).

## Setting Up Run Parameters

For information on how to set up run parameters on the Node 1 and Node 2 servers, see the [“Setting Up Run Parameters” section on page 2-34](#).

## Setting Up the Push-to-Phone Feature

For information on how to set up the push-to-phone feature on the Node 1 and Node 2 servers, see the [“Setting Up the Push-to-Phone Feature” section on page 2-35](#).

## 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 2-54](#)
- [Configuring Installer for the iPhones, page 2-56](#)

## Configuring Installer for the Android Phones

To configure installer for the Android phones, perform the following steps on the Node 1 and Node 2 servers:

- 
- 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.



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

### 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 =http://<host>:<port>
  - Where, ‘address’ is the host IP address of the proxy server and ‘port’ is the proxy server port (default 8000) that you had configured in [Step 4](#) in the “Installing mod\_cluster on the Proxy Node” section on page 2-51.
  - serverURL = http://<host>:<port>
  - Where, ‘address’ is the host IP address of the proxy server and ‘port’ is the proxy server port (default 8000) that you had configured in [Step 4](#) in the “Installing mod\_cluster on the Proxy Node” section on page 2-51.



**Note** The secureServerURL and serverURL values are same.

- 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.
- 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**.

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

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 ipsapp.war file:

- a. Double-click the ipsapp.war file from the *\$JBoss\_HOME/server/scps/deploy/ipsapp.war* directory, and open the Archive Manager screen.
- 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 ipsapp.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 on the Node 1 and Node 2 servers:

**Step 1** Extract the download.properties file:

- a. In a file browser, navigate to the directory containing the *\$JBoss\_HOME/server/scps/deploy/ipsapp.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, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the [“Installing mod\\_cluster on the Proxy Node”](#) section on [page 2-51](#).

- c. Save and close the file.

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

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

**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, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the "Installing mod\_cluster on the Proxy Node" section on [page 2-51](#).

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

Where, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the "Installing mod\_cluster on the Proxy Node" section on [page 2-51](#).

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

Where, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the "Installing mod\_cluster on the Proxy Node" section on [page 2-51](#).



**Note** The secureServerURL and serverURL values are same.

- 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
```

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

- 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 ipsapp.war file:
- Double-click the ipsapp.war file from the `$JBOSS_HOME/server/scps/deploy` 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 ipsapp.war file.
- 

## Setting Up 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 set up Jackrabbit, perform the following steps:

- Step 1** Copy the jackrabbit.war file that is available in `<PS_INSTALL_DIRECTORY>/scps/bin/war` to the `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:
- ```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/jackrabbit.war $JBOSS_HOME/server/all/deploy
```
- Step 2** In a file browser, navigate to the directory containing the `$JBOSS_HOME/server/scps/deploy/jackrabbit.war` file, and double-click this file to open the Archive Manager screen.
- Step 3** Navigate to `/WEB-INF/lib`, select the `jcr-2.0.jar` file, and extract content of the file to the following location:
- ```
$JBOSS_HOME/common/lib
```
- Step 4** Start the proxy on the proxy node and JBoss on the Node 1 server.
- For more information on how to start the proxy and JBoss server, see the [“Starting the Cluster and Proxy” section on page 2-61](#).
- The proxy is up and running on the proxy node, and the JBoss is up and running on the Node 1 server.
- Step 5** In a Web browser, enter the URL `http://address:port/jackrabbit`.
- Where, ‘address’ is the IP address of the proxy server and ‘port’ is the proxy server port that you had configured in [Step 4](#) in the [“Installing mod\\_cluster on the Proxy Node” section on page 2-51](#).
- The Content Repository Setup page appears.
- Step 6** Click **Create Content Repository**.
- The `$JBOSS_HOME/bin/jackrabbit` directory repository structure is created.
- Step 7** Stop the proxy on the proxy node and JBoss on the Node 1 server.
- Step 8** Repeat [Step 1](#) through [Step 7](#) on the Node 2 server.
-

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

## Configuring the Jackrabbit Repository

You need to configure the Jackrabbit repository by providing the DB host IP address, DB port number (default 5432), DB schema name, PS schema username, and PS schema password.

To configure the Jackrabbit repository for clustering, perform the following steps on the Node 1 and Node 2 servers:

**Step 1** Navigate to the `$JBOSS_HOME/bin/jackrabbit` directory, and open the `repository.xml` file.

**Step 2** Search for the below text:

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

Replace with:

```
<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 3** 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 4** 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 5** Search for the below text:

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

```
<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 6** Add the following text at the end of the preceding text:

```
<Cluster id="node1" syncDelay = "1000">
<Journal class="org.apache jackrabbit.core.journal.OracleDatabaseJournal">
<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 node. For example, “node1” for the Node 1 server, “node2” for the Node 2 server, so on.

**Step 7** In the preceding steps, replace the following strings with their actual values:

- *<db host IP address>*—Database server IP address
- *<db port number>*—Database port number
- *<SID of the db>*—SID of the database
- *<schema username>*—Database user name
- *<schema password>*—Database user password

**Step 8** Navigate to the *\$JBoss\_HOME/bin/jackrabbit/workspaces/* directory, and delete the available default and security directories.

**Step 9** Start the proxy on the proxy node and JBoss on the Node 1 and Node 2 servers, and verify that 13 new tables and 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.

## 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 Light Weight Directory Access Protocol (LDAP).

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

For information on how to import SSL certificates on the Node 1 and Node 2 servers, see the “[Importing SSL Certificates](#)” section on page 2-42.

## Starting the Cluster and Proxy

To start the cluster and proxy, perform the following steps:

**Step 1** Start the cluster by performing the following steps on the Node 1 and Node 2 servers:

- a. Ensure that:
  - SDP is up and running without any binding offset value.
  - The `$JAVA_HOME` environment variable is set to the location in which JDK is installed.
  - The `$JBoss_HOME` environment variable is set to the complete path where the unzipped jboss-6.0.0 files are available.
- b. Using a terminal session, navigate to the `$JBoss_HOME/bin` directory.
- c. Enter the following command to start each node in the cluster:

```
./run_scps.sh -c scps -Djboss.service.binding.set=ports-01 -b <SERVER_IP_ADDRESS> -g
sdpPartition -Djboss.messaging.ServerPeerID=1
```

Where, `<SERVER_IP_ADDRESS>` is the IP address of the node.

The following options are used to start each node in a cluster:

- `-c`—Refers to start from “scps” configuration.
- `-b`—Refers to the address used to bind the sockets to the default host namely, the localhost.
- `-g`—Refers to the clusters’ partition name. The default name for a JBoss AS cluster is “DefaultPartition”.
- `jboss.service.binding.set`—Refers to setting another JBoss instance for the Smart+Connected PS application. The ports-01 bindings are obtained by taking the base bindings and by adding 100 to each port value.
- `jboss.messaging.ServerPeerID`—Refers to the JBoss Messaging Clustering (JBM). In JBM, each node in a cluster has a unique integer ID called the “ServerPeerID”. The “ServerPeerID” should remain the same even if the server is restarted many a times.

**Step 2** Start the proxy by performing the following steps on the proxy node:

- a. Using a terminal session, navigate to the following location:

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/sbin
```

- b. Enter the following command to start the proxy:

```
./apachectl start
```

- c. Click **Enter**.

The application can be accessed using the proxy that runs on port “8000” by default.

**Step 3** (Optional) If you want to stop the proxy, perform the following steps on the proxy node:

- a. Using a terminal session, navigate to the following location:

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/sbin
```

- b. Enter the following command to stop the proxy:

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

```
./apachectl stop
```

c. Click **Enter**.

---

## Accessing the Application and Verifying the Installation

- [Smart+Connected PS Web Application, page 2-62](#)
- [Smart+Connected PS Mobile Application, page 2-62](#)

### Smart+Connected PS Web Application

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

---

**Step 1** In the Address field of a Web browser, type the application server URL, `http://<address:port>/ipsapp`, and then press **Enter**.

Where, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the “[Installing mod\\_cluster on the Proxy Node](#)” section on [page 2-51](#).

The Smart+Connected PS login page appears.

**Step 2** 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*.

---

### Smart+Connected PS Mobile Application

For information on how to access the Smart+Connected PS mobile application and verify the installation, see the [Smart+Connected PS Mobile Application, page 2-44](#).





## Installing the Smart+Connected PS on JBoss and Postgres

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

- [Prerequisites, page 3-63](#)
- [Installing on a Colocated or Non-Cluster Server Setup, page 3-64](#)
- [Installing on a Cluster Server Setup, page 3-92](#)

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

### Prerequisites

- [Gathering Required Information, page 3-63](#)
- [Verifying Network Configurations, page 3-64](#)

### Gathering Required Information

You need to provide the following information during installation:

- Database Details:
  - Database server IP address.
  - Database name.
  - Port number on which PostgreSQL is to run. The default port number is 5432.
  - Database schema username.
  - Database schema password.
  - SSH credentials.
- Application Server Details:
  - Location of the `<JBoss_INSTALL_LOCATION>` directory if the JBoss server has been pre-installed. The `<JBoss_INSTALL_LOCATION>` directory is the complete path where the jboss files are available. Ensure that the `$JBoss_HOME` environment variable is set to the `<JBoss_INSTALL_LOCATION>` directory.

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

- Location of the `<JDK_INSTALL_LOCATION>` directory if the JDK has been pre-installed. The `<JDK_INSTALL_LOCATION>` directory is the complete path where you have installed JDK. Ensure that the `$JAVA_HOME` environment variable is set to the `<JDK_INSTALL_LOCATION>` directory and the `PATH` environment variable includes the `$JAVA_HOME/bin` directory.
- SSH credentials.

## Verifying Network Configurations

Verify the following network configurations:

- All machines in the setup are in the same network domain.
- All machines are in the same LAN.
- All machines are configured to be on the same locale.
- System time is synchronized on all machines by using the Network Time Protocol (NTP).
- All dependent components for the Smart+Connected PS application 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 3-65](#)
2. [Configuring Audio Notification to the Cisco IP Phone, page 3-65](#)
3. [Configuring the Database, page 3-65](#)
4. [Creating JBoss Profile, page 3-69](#)
5. [Setting Up Port, page 3-71](#)
6. [Setting Up Security Configuration, page 3-72](#)
7. [Setting Up Java Messaging Service \(JMS\), page 3-73](#)
8. [Setting Up Library, page 3-77](#)
9. [Setting Up the BIRT Engine, page 3-78](#)
10. [Configuring Logging, page 3-78](#)
11. [Configuring the Properties Files, page 3-80](#)
12. [Setting Up Run Parameters, page 3-82](#)
13. [Setting Up the Push-to-Phone Feature, page 3-83](#)
14. [Configuring the Secured URL, page 3-84](#)
15. [Configuring Installer for the Mobile Devices, page 3-85](#)
16. [Setting Up Apache Jackrabbit, page 3-89](#)
17. [Importing SSL Certificates, page 3-90](#)
18. [Starting the JBoss Server, page 3-91](#)
19. [Accessing the Application and Verifying the Installation, page 3-91](#)

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

## Installing the Application

For information on how to install the Smart+Connected PS application, see the [“Installing the Application”](#) section on page 2-13.

## Configuring Audio Notification to the Cisco IP Phone

For information on how to configure audio notification to the Cisco IP phone, see the [“Configuring Audio Notification to the Cisco IP Phone”](#) section on page 2-15.

## Configuring the Database

- [Requirements, page 3-65](#)
- [About Database Scripts, page 3-65](#)
- [Executing Database Scripts, page 3-68](#)

### 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 PostgreSQL is installed on your database server, and is ready for use.  
This document does not include information on how to set up the PostgreSQL database. For more information, see the PostgreSQL documentation.
- Ensure that you have provided the ‘ALL’ privilege to the PostgreSQL database.
- Ensure that the following SDP database SQL scripts are already executed:
  - setup-sdp-base.sql
  - setup-sdp-types.sql

For more information on how to execute the SDP database SQL scripts, see the [“Executing Database Scripts”](#) section on page 3-68.

### About 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 or 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.

- [SDP Database Scripts, page 3-66](#)
- [PS Application Database Scripts, page 3-66](#)

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

## SDP Database Scripts

The SDP database scripts are available at the following directory on the server where you have installed the SDP application:

`<SDP_INSTALL_DIRECTORY>/sdp/`

**Table 3-1** *SDP Database Script - Details*

Script	Description
<code>clean-sdp-objects.sql</code>	Cleans all SDP-related objects from the user schema if an instance of SDP was running earlier. Executing this script is not necessary if you are installing the SDP for the first time.
<code>setup-sdp-base.sql</code>	<ul style="list-style-type: none"> <li>Creates the tables, constraints, sequences, and indexes.</li> <li>Loads only the basic data that is required to bootstrap the application.</li> <li>Enables the local database authentication.</li> <li>Creates a user with the default username/password as superadmin/superadmin.</li> <li>Adds the locations that are defined in the seed data.</li> <li>Grants access rights to the locations to SuperAdmin (super administrator).</li> </ul>
<code>setup-sdp-types.sql</code>	Loads the device types and device properties data.

## PS Application Database Scripts

The Smart+Connected PS database scripts are available at the following directory in the system where you have installed the application:

`<PS_INSTALL_DIRECTORY>/scps/scripts/postgres`

These scripts create the appropriate Smart+Connected PS database objects in the database.

**Table 3-2** *Smart+Connected PS Database Script - Details*

Script	Description
<code>clean-pvo-objects.sql</code>	Cleans all the Smart+Connected PS-related objects from the user schema. Executing this script is not necessary if you are installing the application for the first time.

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

**Table 3-2 Smart+Connected PS Database Script - Details**

Script	Description
setup-pvo-base.sql	<ul style="list-style-type: none"><li>Creates the tables, constraints, sequences, and indexes.</li><li>Loads the basic data that is required to bootstrap the application.</li></ul>
insert-seed-data.sql	Inserts the required seed data in the tables. This is available in the <PS_INSTALL_DIRECTORY>/scps/scripts/postgres/commonsript directory.

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

## Executing Database Scripts

To execute the SDP and Smart+Connected PS database scripts, perform the following steps:

- 
- Step 1** Copy the SDP and Smart+Connected PS database scripts:
- From the `<SDP_INSTALL_DIRECTORY>/sdp/scripts/` directory on the server where you have installed the SDP application, copy the 'postgres' directory to a location `<PATH_OF_SDPDBSCRIPTS>` in the database server.
  - From the `<PS_INSTALL_DIRECTORY>/scps/scripts/` directory on the server where you have installed the Smart+Connected PS application, copy the 'postgres' directory to a location `<PATH_OF_PSDBSCRIPTS>` in the database server.
- Step 2** Open the PG SQL Shell.
- Step 3** Enter the IP address of the database server, database name, port number (if you have changed it), schema username, and schema password.
- Step 4** For the SDP database scripts, do the following:
- To set the script path, enter the following command:  

```
\cd <PATH_OF_SDPDBSCRIPTS>/postgres
```

Where, `<PATH_OF_SDPDBSCRIPTS>` is the location where you had copied the SDP scripts directory.
  - To run the scripts, enter the following commands in order:  

```
\i setup-sdp-base.sql
\i setup-sdp-types.sql
```

The SDP application-related tables and basic data are created.



**Note** When you run the database scripts, a log file is automatically generated and saved in the `<PATH_OF_SDPDBSCRIPTS>` directory. You must check this log file to ensure that there are no errors logged. If the log file displays errors, these errors must be corrected before you proceed with the installation.

---

- Step 5** For the Smart+Connected PS database scripts, do the following:
- To set the common script path, enter the following command:  

```
\cd<PATH_OF_PSDBSCRIPTS>/postgres/commonsript
```

Where, `<PATH_OF_PSDBSCRIPTS>` is the location where you had copied the Smart+Connected PS scripts directory.
  - To run the database common script, enter the following command:  

```
\i insert-seed-data.sql
```
  - To set the PS script path, enter the following command:  

```
\cd <PATH_OF_PSDBSCRIPTS>/postgres
```

Where, `<PATH_OF_PSDBSCRIPTS>` is the location where you had copied the Smart+Connected PS scripts directory.
  - To run the database scripts, enter the following command:  

```
\i insert-seed-data.sql
```

The Smart+Connected PS application-related tables and basic data are created.

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

**Note**

When you run the database scripts, a log file is automatically generated and saved in the `<PATH_OF_PSDBSCRIPTS>` directory. You must check this log file to ensure that there are no errors logged. If the log file displays errors, these errors must be corrected before you proceed with the installation.

## Creating JBoss Profile

After configuring the database, you need to create a profile in the JBoss server for running the Smart+Connected PS application.

To create a profile in the JBoss server, perform the following steps:

- Step 1** Download `jboss-6.0.0.Final.zip`.

JBoss is open source, and you can download it from the Internet. For example:

<http://sourceforge.net/projects/jboss/files/JBoss/JBoss-6.0.0.Final/jboss-as-distribution-6.0.0.Final.zip/download>

- Step 2** Create a directory named 'jboss', and unzip the `jboss-6.0.0.Final.zip` file into that directory.

- Step 3** Set the `$JBOSS_HOME` and `$JAVA_HOME` environment variables by entering the following commands:

```
$ export JAVA_HOME=<JDK_INSTALL_LOCATION>
$ export JBOSS_HOME=<JBOSS_INSTALL_LOCATION>
```

Where, `<JBOSS_INSTALL_LOCATION>` is the complete path where the unzipped `jboss-6.0.0` files are available and `<JDK_INSTALL_LOCATION>` is the complete path where you have installed `jdk1.6.0_24`.

**Note**

You can also add the preceding commands to the user's profile script so that the `$JBOSS_HOME` and `$JAVA_HOME` environment variables are automatically set up during login.

- Step 4** Navigate to the server directory in `$JBOSS_HOME` by entering the following command:

```
cd $JBOSS_HOME/server
```

- Step 5** Copy the 'default' directory with the name 'scps' by entering the following command:

```
cp -R default scps
```

The 'scps' directory is created under the `$JBOSS_HOME/server` directory. The 'scps' directory is used as the Smart+Connected PS application profile.

- Step 6** Copy the `ipsapp.war` file, which is available in `<PS_INSTALL_DIRECTORY>/scps/bin/war`, to the `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:

```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/ipsapp.war $JBOSS_HOME/server/scps/deploy
```

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

**Step 7** Create a datasource file so that the Smart+Connected PS application communicates with the database machine:

a. Create the postgres-ds.xml file under the 'scps/deploy' directory with the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<local-tx-datasource>
<jndi-name>jdbc/scc</jndi-name>
<connection-url>jdbc:postgresql://IPaddress:5432/schemaName</connection-url>
<driver-class>org.postgresql.Driver</driver-class>
<user-name>DBusername</user-name>
<password>DBpassword</password>
<min-pool-size>10</min-pool-size>
<max-pool-size>50</max-pool-size>
</local-tx-datasource>
</datasources>
```

b. Replace the following text with their actual values in the code that you had added in [Step 7 a.](#):

- 'IPaddress' with the database server IP address or DNS hostname
- 'schemaName' with the database name
- '5432' with the database port number if changed during the PostgreSQL installation
- 'DBusername' with the database schema username
- 'DBpassword' with the database schema password

c. Save the file.

d. Provide the executable permissions to the newly created postgres-ds.xml file by entering the following command:

```
chmod 755 postgres-ds.xml
```

**Step 8** Add an entry for scanning deployers:

a. Navigate to the `$JBOSS_HOME/server/scps/deployers` directory, and open the `scanning-deployers-jboss-beans.xml` file.

b. Search for the following text:

```
<install method="addIgnored">
  <parameter>java.lang.LinkageError</parameter>
</install>
```

c. Add the following code after the searched text:

```
<install method="addIgnored">
  <parameter>java.lang.reflect.MalformedParameterizedTypeException</parameter>
</install>
```

d. Save the file.

**Step 9** Update the run.conf file to increase the memory:

a. Open the run.conf file available in `$JBOSS_HOME/bin` and search for the following text:

```
JAVA_OPTS="-Xms128m -Xmx512m -XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

Replace with the following text:

```
JAVA_OPTS="-Xms256m -Xmx1024m -XX:MaxPermSize=512m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```



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

- b. Save the file.

## Setting Up Port

You need to set up a port for the Smart+Connected PS application by changing the following default port values:

- JBoss web HTTP connector socket value. By default, the 'HttpConnector' value is 8080.
- Listening socket for the naming service. By default, the 'Port' value is 1099.



### Note

While changing the default port values, ensure that you do not change any other port number apart from the 'HttpConnector' and 'Port' values for the property name 'bindingName'.

To set up a port for the Smart+Connected PS application, perform the following steps:

- Step 1** Open the following file:  
`$JBoss_HOME/server/scps/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml`
- Step 2** Search for the port number 8080 that has the 'bindingName' value as 'HttpConnector' and replace with a port number that is not in use, for example 7001.

After changing the value, the text is displayed as follows:

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">
  <property name="serviceName">jboss.web:service=WebServer</property>
  <property name="bindingName">HttpConnector</property>
  <property name="port">7001</property>
  <property name="description">JBoss Web HTTP connector socket; also drives the values
for the HTTPS and AJP sockets</property>
</bean>
```

- Step 3** Search for the port number 1099 that has the 'bindingName' value as 'Port' and replace with a port number 11099.

After changing the value, the text is displayed as follows:

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">
  <property name="serviceName">jboss.service=Naming</property>
  <property name="bindingName">Port</property>
  <property name="port">11099</property>
  <property name="description">The listening socket for the Naming service</property>
</bean>
```

- Step 4** Save the file.
- Step 5** Repeat [Step 1](#) through [Step 4](#) in the bindings-jboss-beans.xml file for the SDP profile.

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

## Setting Up Security Configuration

You need to set up security configuration in the Smart+Connected PS application for the following:

- Disabling the JMS message security, its value is set to 'true' by default.
- Authenticating LDAP users of the Smart+Connected PS application.

To set up security configuration, perform the following steps:

**Step 1** To disable the JMS message security:

- In the `$JBOSS_HOME/server/scps/deploy/hornetq/hornetq-configuration.xml` file, add the tag `<security-enabled>>false</security-enabled>` after the `</security-settings>` end tag.
- Save the file.

The JMS message security is now set to false.

**Step 2** To enable the LDAP authentication for application users:

- In the `$JBOSS_HOME/server/scps/conf/login-config.xml` file, search for the following text:

```
<application-policy name="JBossWS">
  <authentication>
    <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule"
      flag="required">
      <module-option
name="usersProperties">props/jbossws-users.properties</module-option>
      <module-option
name="rolesProperties">props/jbossws-roles.properties</module-option>
      <module-option name="unauthenticatedIdentity">anonymous</module-option>
    </login-module>
  </authentication>
</application-policy>
```

- Add the following code after the preceding text:

```
<application-policy name="SDP">
  <authentication>
    <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
      flag="sufficient">
      <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.SDPDataSourceLoginMod
ule</module-option>
      <module-option name="jndiName">java:jdbc/scc</module-option>
      <module-option name="debug">true</module-option>
    </login-module>
    <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
      flag="sufficient">
      <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.ldap.SDPLdapLoginModu
le</module-option>
      <module-option name="jndiName">java:jdbc/scc</module-option>
      <module-option
name="initialContextFactory">com.sun.jndi.ldap.LdapCtxFactory</module-option>
      <module-option
name="connectionURL">ldap://ldap.example.com:389</module-option>
      <module-option
name="connectionUsername">uid=name1,ou=people,ou=com</module-option>
      <module-option name="connectionPassword">password123</module-option>
      <module-option name="authentication">simple</module-option>
      <module-option
name="userBase">ou=active,ou=employees,ou=people,o=example.com</module-option>
      <module-option name="userSearchMatching">uid={0}</module-option>
```

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

```

        <module-option name="userSearchSubtree">true</module-option>
        <module-option name="debug">true</module-option>
    </login-module>
</authentication>
</application-policy>

```

- c. Replace the following LDAP server and LDAP user details with their actual values in the code that you added in [Step 2 b.](#):

- connectionURL
- connectionUsername
- connectionPassword
- authentication
- userBase
- userSearchMatching
- userSearchSubtree



**Note** If LDAP does not require authentication or uses anonymous bind, the connectionUsername and connectionPassword values can be left blank.

- d. Save the file.  
The LDAP configuration is complete.

## Setting Up Java Messaging Service (JMS)

- [Creating a Connection Factory, page 3-73](#)
- [Creating an Event Topic, page 3-75](#)
- [Configuring an Event Topic, page 3-76](#)
- [Creating a Queue, page 3-77](#)

### Creating a Connection Factory

You need to create a connection factory in the SDP and Smart+Connected PS application.

- [Creating a Connection Factory in the SDP, page 3-73](#)
- [Creating a Connection Factory in the Smart+Connected PS, page 3-75](#)

#### Creating a Connection Factory in the SDP

You need to create a connection factory in the SDP for the Smart+Connected PS application to work properly.

To create a connection factory in the SDP, perform the following steps:

- Step 1** Navigate to the `$JBOSS_HOME/server/<SDP_PROFILE_DIR>/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.

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

Where, `<SDP_PROFILE_DIR>` is the SDP JBoss profile directory.

**Step 2** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="NettyConnectionFactory">
  <connectors>
    <connector-ref connector-name="netty" />
  </connectors>
  <entries>
    <entry name="/ConnectionFactory" />
    <entry name="/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 3** Replace `'/ConnectionFactory'` with `'/SDPXConnectionFactory'` as follows:

```
<entries>
  <entry name="/SDPXConnectionFactory" />
  <entry name="/XAConnectionFactory" />
</entries>
```

**Step 4** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="InVMConnectionFactory">
  <connectors>
    <connector-ref connector-name="in-vm" />
  </connectors>
  <entries>
    <entry name="/ConnectionFactory" />
    <entry name="/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 5** Replace `'/ConnectionFactory'` with `'/SDPXConnectionFactory'` as follows:

```
<entries>
  <entry name="/SDPXConnectionFactory" />
  <entry name="/XAConnectionFactory" />
</entries>
```

**Step 6** Save the file.

The connection factory is created in the SDP.

---

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

## Creating a Connection Factory in the Smart+Connected PS

To create a connection factory in the Smart+Connected PS, perform the following steps:

**Step 1** Navigate to the `$JBOSS_HOME/server/scps/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.

**Step 2** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="NettyConnectionFactory">
  <connectors>
    <connector-ref connector-name="netty" />
  </connectors>
  <entries>
    <entry name="/ConnectionFactory" />
    <entry name="/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 3** Replace `/ConnectionFactory` with `/jms/ipsConnectionFactory` as follows:

```
<entries>
  <entry name="/jms/ipsConnectionFactory" />
  <entry name="/XAConnectionFactory" />
</entries>
```

**Step 4** In the `hornetq-jms.xml` file, search for the following text:

```
<connection-factory name="InVMConnectionFactory">
  <connectors>
    <connector-ref connector-name="in-vm" />
  </connectors>
  <entries>
    <entry name="java:/ConnectionFactory" />
    <entry name="java:/XAConnectionFactory" />
  </entries>
</connection-factory>
```

**Step 5** Replace `/ConnectionFactory` with `/jms/ipsConnectionFactory` as follows:

```
<entries>
  <entry name="java:/jms/ipsConnectionFactory" />
  <entry name="java:/XAConnectionFactory" />
</entries>
```

**Step 6** Save the file.

The connection factory for the Smart+Connected PS is created.

## Creating an Event Topic

You need to create an event topic in the SDP server.

To create an event topic, perform the following steps in the SDP server:

**Step 1** Navigate to the `$JBOSS_HOME/server/<SDP_PROFILE_DIR>/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.

Where, `<SDP_PROFILE_DIR>` is the SDP JBoss profile directory.

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

**Step 2** In the `hornetq-jms.xml` file, search for the following text:

```
<queue name="ExpiryQueue">
  <entry name="/queue/ExpiryQueue"/>
</queue>
```

**Step 3** At the end of the preceding text, add an entry for “`/jms/sdp.event.Topic`” as follows:

```
<topic name="sdp.event.Topic">
<entry name="/jms/sdp.event.Topic"/>
</topic>
```

**Step 4** Save the file.

An event topic is created in the SDP server.

---

## Configuring an Event Topic

After creating an event topic in the SDP, perform the following steps to configure events in the SDP server:

**Step 1** In a file browser, navigate to the `$JBOSS_HOME/server/<SDP_PROFILE_DIR>/deploy/hornetq` directory, and open the `hornetq-configuration.xml` file.

Where, `<SDP_PROFILE_DIR>` is the SDP JBoss profile directory.

**Step 2** In the `hornetq-configuration.xml` file, add the following to disable the JMS message security:

```
<security-enabled>false</security-enabled>
```



**Note** The value of the JMS message security is set to ‘true’ by default.

---

**Step 3** Navigate to `$JBOSS_HOME/bin`, and open the `run.sh` file for the SDP profile.

**Step 4** In the `run.sh` file, search for the following text:

```
JAVA_OPTS="$ {JAVA_OPTS:--Dprogram.name=$PROGNAME}
-DANTLR_USE_DIRECT_CLASS_LOADING=true -Dshared.dir=$JBOSS_HOME/shared
-Dcom.sun.xml.bind.v2.bytecode.ClassTailor.noOptimize=true
-Dsdp.af.cache.root=$JBOSS_HOME/server/default/tmp"
```

**Step 5** Add the following command line to the text that you have searched for:

```
"-Dsdp.event.config.mode=global"
```

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

```
JAVA_OPTS="$ {JAVA_OPTS:--Dprogram.name=$PROGNAME}
-DANTLR_USE_DIRECT_CLASS_LOADING=true -Dsdp.event.config.mode=global
-Dshared.dir=$JBOSS_HOME/shared
-Dcom.sun.xml.bind.v2.bytecode.ClassTailor.noOptimize=true
-Dsdp.af.cache.root=$JBOSS_HOME/server/default/tmp"
```

**Step 6** Save the file.

---

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

## Creating a Queue

You need to create a queue in the Smart+Connected PS application server.

To create a queue, perform the following steps in the Smart+Connected PS application server:

- 
- Step 1** Navigate to the `$JBOSS_HOME/server/scps/deploy/hornetq` directory, and open the `hornetq-jms.xml` file.
- Step 2** In the `hornetq-jms.xml` file, search for the following text:
- ```
<queue name="ExpiryQueue">
  <entry name="/queue/ExpiryQueue"/>
</queue>
```
- Step 3** After the preceding text, add an entry for “/jms/ipsQueue” as follows:
- ```
<queue name="ipsQueue">
  <entry name="/jms/ipsQueue"/>
</queue>
```
- Step 4** Save the file.
- A queue for the Smart+Connected PS application is created.
- 

## Setting Up Library

To set up the library, perform the following steps in the Smart+Connected PS application server:


- 
- Step 1** Copy the following jar files to the `$JBOSS_HOME/server/scps/lib` directory:
- `postgresql-9.0-801.jdbc4.jar`—It is open source, and you can download it from the Internet. For example:  
<http://jdbc.postgresql.org/download/postgresql-9.0-801.jdbc4.jar>
  - `sdp-authmodules.jar`—Available at the `<SDP_INSTALL_DIRECTORY>/sdp/bin/jars` location on the server where the SDP has been installed.
- Step 2** Navigate to the `$JBOSS_HOME/server/scps/lib` directory, and provide the required permissions to the saved files (`postgresql-9.0-801.jdbc4.jar` and `sdp-authmodules.jar`) by entering the following command:
- ```
chmod 755 *
```
-

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

## 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 application. The BIRT runtime reporting engine is automatically installed while installing the Smart+Connected PS application.

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

- 
- Step 1** Create the 'SCPS\_Log' directory in the `<PS_INSTALL_DIRECTORY>`, and provide the read and write permissions to the users who run the JBoss profile for the Smart+Connected PS application.
- Step 2** Navigate to the `$JBOSS_HOME/server/scps/deploy/` directory, and open the 'jboss-logging.xml' file in a text editor.
- Step 3** Below the existing 'periodic-rotating-file-handler' tag, add the following text:  
`<periodic-rotating-file-handler`



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

```

        file-name="<PS_INSTALL_DIRECTORY>/SCPS_Log/PS_Server.log"
        name="SDPFILEHANDLER"
        autoflush="true"
        append="true"
        suffix=".yyyy-MM-dd">
    <error-manager>
        <only-once/>
    </error-manager>
    <formatter>
        <pattern-formatter pattern="%d %-5p [%c] (%t) %s%E%n"/>
    </formatter>
</periodic-rotating-file-handler>

```

For example:

```

<periodic-rotating-file-handler
    file-name="/home/scc-qa/scps/SCPS_Log/PS_Server.log"
    name="SDPFILEHANDLER"
    autoflush="true"
    append="true"
    suffix=".yyyy-MM-dd">
    <error-manager>
        <only-once/>
    </error-manager>
    <formatter>
        <pattern-formatter pattern="%d %-5p [%c] (%t) %s%E%n"/>
    </formatter>
</periodic-rotating-file-handler>

```

The logs are created after the application is up and running at the location that you had specified in the 'file-name' attribute.

**Step 4** Search for the following text:

```

<root-logger>
    <!-- Set the root logger priority via a system property, with a default value. -->
    <level name="{jboss.server.log.threshold:INFO}"/>
    <handlers>
        <handler-ref name="CONSOLE"/>
        <handler-ref name="FILE"/>
    </handlers>
</root-logger>

```

Replace the text as follows:

```

<root-logger>
    <!-- Set the root logger priority via a system property, with a default value. -->
    <level name="{jboss.server.log.threshold:INFO}"/>
    <handlers>
        <handler-ref name="CONSOLE"/>
        <handler-ref name="FILE"/>
        <handler-ref name="SDPFILEHANDLER"/>
    </handlers>
</root-logger>

```

**Step 5** Save the 'jboss-logging.xml' file.

Logging is configured for the Smart+Connected PS application.

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

## Configuring the Properties Files

- [About the Properties Files, page 3-80](#)
- [Updating the Properties Files, page 3-81](#)

### About the Properties Files

- [About the LDAP Properties File, page 3-80](#)
- [About the JMS Properties File, page 3-80](#)
- [About the Reservation Properties File, page 3-81](#)
- [About the Notificationservice Properties File, page 3-81](#)

#### About the LDAP Properties File

For information on the LDAP properties file, see [“About the LDAP Properties File” section on page 3-80](#).

#### About the JMS Properties File

[Table 3-3](#) 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 3-3 JMS Properties**

| Property Name             | Description  | Sample Value   |
|---------------------------|--|--|
| ips.jms.jndi              | Identifies the JNDI name for the ips queue.  | jms/ipsQueue <sup>1</sup>  |
| ips.jms.connectionfactory | Identifies the Connection factory for the ips queue.   | jms/ipsConnectionFactory <sup>1</sup>                                  |
| ips.jms.initialContext    | Identifies the Smart+Connected PS initial context url. 11099 is the listening socket port that is defined as value for the listening socket port for the Naming service (which you had set up in <a href="#">Step 3</a> of the <a href="#">“Setting Up Port” section on page 3-71</a> ). | jnp://localhost:11099  |
| URL                       | Identifies the SDP topic URL. 11099 is the listening socket port that is defined as value for SDP listening socket port for the Naming service (which you had set up in <a href="#">Step 5</a> of the <a href="#">“Setting Up Port” section on page 3-71</a> ).                          | jnp://<SDP_IPADDRESS>:11099<br>For example,<br>jnp://10.10.10.10:11099 |
| username                  | Identifies the SDP domain username.  | admin  |
| password                  | Identifies the SDP domain password.  | admin  |

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

**Table 3-3 JMS Properties (continued)**

| Property Name    | Description   | Sample Value          |
|------------------|---|-----------------------|
| providerurl      | Identifies the Smart+Connected PS Queue URL. 11199 is the listening socket port that is defined by adding the listening socket port for the Naming service value (which you had set up in <a href="#">Step 3</a> of the “ <a href="#">Setting Up Port</a> ” section on page 3-71) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default). | jnp://localhost:11199 |
| provideruserName | Identifies the Smart+Connected PS domain admin username.  | admin                 |
| providerpassword | Identifies the Smart+Connected PS domain admin password.  | admin                 |

1. This property value should not be changed.

### About the Reservation Properties File

For information on the reservation properties file, see “[About the Reservation Properties File](#)” section on page 2-30.

### About the Notificationservice Properties File

For information on the notification service properties file, see “[About the Notificationservice Properties File](#)” section on page 2-32.

## Updating the Properties Files

- [Preparing the Properties File](#), page 3-81
- [Setting Up Reservation and Notification Properties](#), page 3-82

### 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` directory, 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 2-3](#).
  - Step 3** Edit the pvoJms.properties file to provide the values for each of the property names as listed in [Table 2-4](#).
  - Step 4** Make a note of the location where you save the LDAP.properties and pvoJms.properties files. This location is used for setting up run parameters for the JBoss start-up configuration.
-

***Send documentation comments to [scc-docfeedback@cisco.com](mailto:scc-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 `$JBOSS_HOME/server/scps/deploy/ipsapp.war` file, and double-click this file to open the Archive Manager screen.
- Step 2** Navigate to `/WEB-INF/classes`, select the following files, and extract content of the files to a suitable location, such as Desktop:
- `Reservation.properties`
  - `notification.service.properties`
- Step 3** Update the `Reservation.properties` file:
- Open the `Reservation.properties` file, which is available at the specified location, in the edit mode and update the property values as described in [Table 2-5](#).
  - Save and close the file.
- Step 4** Update the `notification.service.properties` file:
- Open the `notification.service.properties` file, which is available at the specified location, in the edit mode and update the property values as described in [Table 2-6](#).
  - Save and close the file.
- Step 5** Navigate to the directory containing the `$JBOSS_HOME/server/scps/deploy/ipsapp.war` file, and double-click this file to open the Archive Manager screen.
- Step 6** Navigate to `/WEB-INF/classes`, and click **Add**.
- Step 7** Browse and select the following updated files, and click **OK**:
- `Reservation.properties`
  - `notification.service.properties`

The updated file is replaced in the `ipsapp.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.

---

## Setting Up Run Parameters

To set up run parameters, perform the following steps:

- 
- Step 1** Navigate to `$JBOSS_HOME/bin`, copy the 'run.sh' file, and create a file with the name 'run\_scps.sh'.
- Step 2** To allow JMS to work in the Smart+Connected PS application through the SDP, set the 'sdp.event.config.mode' property in the 'run\_scps.sh' file of the Smart+Connected PS profile:
- In the `run_scps.sh` file, search for the following text:
 

```
# Setup JBoss specific properties
JAVA_OPTS="${JAVA_OPTS:+$JAVA_OPTS -Dprogram.name=$PROGNAME}"
JAVA_OPTS="${JAVA_OPTS:--Dprogram.name=$PROGNAME}"
```
  - Add the following text:

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true"
```

**Step 3** Configure the LDAP properties:

- a. In the run\_scps.sh file, search for the following text:

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true"
```

- b. Add the following text at the end of the searched text before the (""):

```
-Dcom.cisco.sdp.ldap.configfilepath=<path to LDAP.properties file>/LDAP.properties
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties
```

For example:

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

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_ldap_props=/u01/scps/config/LDAP.properties"
```

**Step 4** Configure the application properties:

- a. In the run\_scps.sh file, search for the following text:

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true"
```

- b. Add the following text at the end of the line before the (""):

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

For example:

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

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global -DUseSunHttpHandler=true
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties"
```

**Step 5** Save and close the run\_scps.sh file.

## Setting Up the Push-to-Phone Feature

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

- Step 1** From the file browser, navigate to `$JBOSS_HOME/bin` directory, and open the run\_scps.sh file.

- Step 2** In the run\_scps.sh file, search for the following text:

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global"
```

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

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

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

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
-Djboss.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.

To configure the secured URL, perform the following steps:

---

**Step 1** Create a simple SSL certificate keystore:

- a. Open a terminal and navigate to the `$JBOSS_HOME/server/scps/conf` directory.
- b. Remove the existing `server.keystore` file.
- c. Navigate to the `$JAVA_HOME/bin` directory, and enter the following command to create a certificate and a storefile with the name 'server.keystore':

```
./keytool -genkey -alias <keystore alias> -keyalg RSA -keystore
$JBOSS_HOME/server/scps/conf/server.keystore -validity <number of days>
```

For example:

```
./keytool -genkey -alias jbosshttps -keyalg RSA -keystore
$JBOSS_HOME/server/scps/conf/server.keystore -validity 3650
```

You are prompted to specify the following required details:

- Enter keystore password—Specify a password for keystore. For example, password1. You also need to use the same keystore password when prompted.
- 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**.

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

The certificate with a validity of *<number of days>* days is generated. You are prompted for the key password of the *<alias name>*.

- d. Press **Enter**.

The certificate is retained in the `server.keystore` file.

**Step 2** Configuring the JBoss server to create an SSL connector:

- a. Open a terminal and navigate to the `$JBOSS_HOME/server/scps/deploy/jbossweb.sar` directory.
- b. Open the `server.xml` file in an edit mode, and uncomment the following text:

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
    port="${jboss.web.https.port}" address="${jboss.bind.address}"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
    keystorePass="rmi+ssl" sslProtocol = "TLS" />
```

- c. In the above text, replace the following:
  - `${jboss.web.https.port}` with the unique port number that will be used as the SSL port (for example, 9001)
  - `${jboss.server.home.dir}` with `$JBOSS_HOME/server/scps/conf/server.keystore`
  - `rmi+ssl` with the keystore password (for example, password1)

## 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 3-85](#)
- [Configuring Installer for the iPhones, page 3-87](#)

## 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:

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

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

Where, 'host' is the IP address or the DNS hostname of the host on which the JBoss application server is set up and 'SSL port' is the value that appears in the output after starting the JBoss server. The 'SSL port' value is obtained by adding the `jboss.web.https.port` value (which you had set up in the [“Configuring the Secured URL”](#) section on page 2-36) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).



**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 JBoss application server is set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the `HttpConnector` port value (which you had set up in [“Setting Up Port”](#) section on page 3-97) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

- Save and close the file.

**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.



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

- 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 ipsapp.war file:

- Double-click the ipsapp.war file from the *\$JBOSS\_HOME/server/scps/deploy/ipsapp.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 ipsapp.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 *\$JBOSS\_HOME/server/scps/deploy/ipsapp.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](mailto:scc-docfeedback@cisco.com)**

Where, 'host' is the IP address or DNS hostname of the host on which the JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in [“Setting Up Port” section on page 3-71](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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 JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in [“Setting Up Port” section on page 3-97](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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 DNS hostname of the host on which the JBoss application server has been set up and 'SSL port' is the value that appears in the output after starting the JBoss server. The 'SSL port' value is obtained by adding the jboss.web.https.port value (which you had set up in the [“Configuring the Secured URL” section on page 3-84](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

**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>

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

Where, 'host' is the IP address or DNS hostname of the host on which the JBoss application server has been set up and 'port' is the value that appears in the output after starting the JBoss server. The 'port' value is obtained by adding the HttpConnector port value (which you had set up in [“Setting Up Port” section on page 3-71](#)) and the “ports-01” offset value in the bindings-jboss-beans.xml file (which is 100 by default).

- 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 ipsapp.war file:
  - a. Double-click the ipsapp.war file from the `$JBOSS_HOME/server/scps/deploy` 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 ipsapp.war file.

## Setting Up 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 set up Jackrabbit, perform the following steps:

- Step 1** Copy the jackrabbit.war file that is available in `<PS_INSTALL_DIRECTORY>/scps/bin/war` to `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:
 

```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/jackrabbit.war $JBOSS_HOME/server/scps/deploy
```
- Step 2** Navigate to the directory containing the `$JBOSS_HOME/server/scps/deploy/jackrabbit.war` file, and double-click this file to open the Archive Manager screen.
- Step 3** Navigate to /WEB-INF/lib, select the jcr-2.0.jar file, and extract content of the file to the following location:
 

```
$JBOSS_HOME/common/lib
```
- Step 4** Start the JBoss server.

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

For more information on how to start the JBoss server, see the “Starting the JBoss Server” section on page 3-91.

Ensure that the JBoss server is now up and running.

**Step 5** In a Web browser, enter the URL <http://host:port/jackrabbit>.

Where, ‘host’ is the IP address or DNS hostname of the host on which the JBoss application server has been set up and ‘port’ is the Jboss binding server port that you had configured in the “Setting Up Port” section on page 3-71.

The Content Repository Setup page appears.

**Step 6** Click **Create Content Repository**.

The `$JBOSS_HOME/bin/jackrabbit` directory repository structure is created.

## 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 Light Weight Directory Access Protocol (LDAP).

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

To import SSL certificates, perform the following steps:

**Step 1** Using a terminal session, navigate to the `$JAVA_HOME/bin` directory, where the `$JAVA_HOME` environment variable is set to the `<JDK_INSTALL_LOCATION>` directory.

**Step 2** Enter the following command:

```
./keytool -import -alias <Alias Name> -file <certificate file name with complete path>
-keystore $JAVA_HOME/jre/lib/security/cacerts -storepass changeit
```

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

For example:

```
./keytool -import -alias CM -file /home/scc-qa/CM115.cer -keystore
/home/scc-qa/Desktop/jdk1.6.0_24/jre/lib/security/cacerts -storepass changeit
```



**Note** If you have installed JDK using an RPM bundle, then you need the SUDO access to add the certificate to the keystore.

A message prompts you to trust this certificate.

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

The certificates are imported.

**Step 4** In the `$JBOSS_HOME/bin/run_scps.sh` file, append the `JAVA_OPTS` line just before (“) with the following line:

```
-Djavax.net.ssl.trustStore=$JAVA_HOME/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

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

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

```
JAVA_OPTS="$JAVA_OPTS -DANTLR_USE_DIRECT_CLASS_LOADING=true
-Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/u01/scps/config/LDAP.properties
-Dpvo_jms_props=/u01/scps/config/pvoJms.properties
-Djboss.net.proxyAuthenticatorClassName=java.net.Authenticator
-DUseSunHttpHandler=true
-Djavax.net.ssl.trustStore=/usr/java/default/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit"
```

**Step 5** Save the run\_scps.sh file.

## Starting the JBoss Server

To start the JBoss application server for the Smart+Connected PS application, perform the following steps:

**Step 1** Ensure that:

- SDP is up and running without any binding offset value.
- The `$JAVA_HOME` environment variable is set to the location in which JDK is installed.
- The `$JBOSS_HOME` environment variable is set to the complete path where the unzipped jboss-6.0.0 files are available.

**Step 2** Using a terminal, navigate to the `$JBOSS_HOME/bin` directory, and run the following command:

```
./run_scps.sh -c scps -Djboss.service.binding.set=ports-01 -b 0.0.0.0
```

The JBoss application server starts. After the server initialization is complete, an output similar to the following is listed:

```
2012-11-20 11:41:31,360 INFO [org.apache.coyote.http11.Http11Protocol] (Thread-2)
Starting Coyote HTTP/1.1 on http-0.0.0.0-7101
```

The port value that appears in the output is the value obtained by adding the `HttpConnector` port value (which you had set up in “[Setting Up Port](#)” section on page 3-71) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

## Accessing the Application and Verifying the Installation

- [Smart+Connected PS Web Application, page 3-91](#)

### Smart+Connected PS Web Application

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**:

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

- <http://<host>:<port>/ipsapp>—To access the application in a non-secured environment.

Where, ‘host’ is the IP address or DNS hostname of the host on which the JBoss application server has been set up and ‘port’ is the value that appears in the output after starting the JBoss server. The ‘port’ value is obtained by adding the `HttpConnector` port value (which you had set up in “[Setting Up Port](#)” section on page 3-71) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

- <https://<host>:<SSL port>/ipsapp>—To access the application in a secured environment.

Where, ‘host’ is the IP address or DNS hostname of the host on which the JBoss application server has been set up and ‘SSL port’ is the value that appears in the output after starting the JBoss server. The ‘SSL port’ value is obtained by adding the `jboss.web.https.port` value (which you had set up in the “[Configuring the Secured URL](#)” section on page 3-84) and the “ports-01” offset value in the `bindings-jboss-beans.xml` file (which is 100 by default).

The Smart+Connected PS login page appears.

**Step 2** 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*.

## Smart+Connected PS Mobile Application

For information on how to access the Smart+Connected PS mobile application and verify the installation, see the [Smart+Connected PS Mobile Application, page 2-44](#).

# Installing on a Cluster Server Setup

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

1. [Installing the Application, page 3-95](#)
2. [Configuring Audio Notification to the Cisco IP Phone, page 3-95](#)
3. [Configuring the Database, page 3-95](#)
4. [Configuring the JBoss Profile, page 3-96](#)
5. [Setting Up Port, page 3-97](#)
6. [Setting Up Security Configuration, page 3-97](#)
7. [Setting Up Java Messaging Service \(JMS\), page 3-98](#)
8. [Setting Up Library, page 3-98](#)
9. [Setting Up the BIRT Engine, page 3-98](#)
10. [Configuring Logging, page 3-98](#)

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

11. [Configuring the Cluster Server Setup, page 3-98](#)
12. [Configuring the Properties Files, page 3-102](#)
13. [Setting Up Run Parameters, page 3-102](#)
14. [Setting Up the Push-to-Phone Feature, page 3-102](#)
15. [Configuring Installer for the Mobile Devices, page 3-102](#)
16. [Setting Up Apache Jackrabbit, page 3-106](#)
17. [Configuring the Jackrabbit Repository, page 3-107](#)
18. [Importing SSL Certificates, page 3-109](#)
19. [Starting the Cluster and Proxy, page 3-109](#)
20. [Accessing the Application and Verifying the Installation, page 3-110](#)

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

## About Clustering

A JBoss server cluster consists of multiple JBoss server instances running simultaneously and working together to provide increased scalability, reliability, and high availability. A cluster appears to clients to be a single JBoss 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 JBoss version.

An example of clustered deployment in a distributed environment is as follows:

- The database is non-clustered.
- The application servers are clustered.
- Two virtual machines host the application servers. The application is deployed on these two virtual machines, Node 1 and Node 2.
- One virtual machine hosts the proxy server. This proxy server acts as a software load balancer.

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

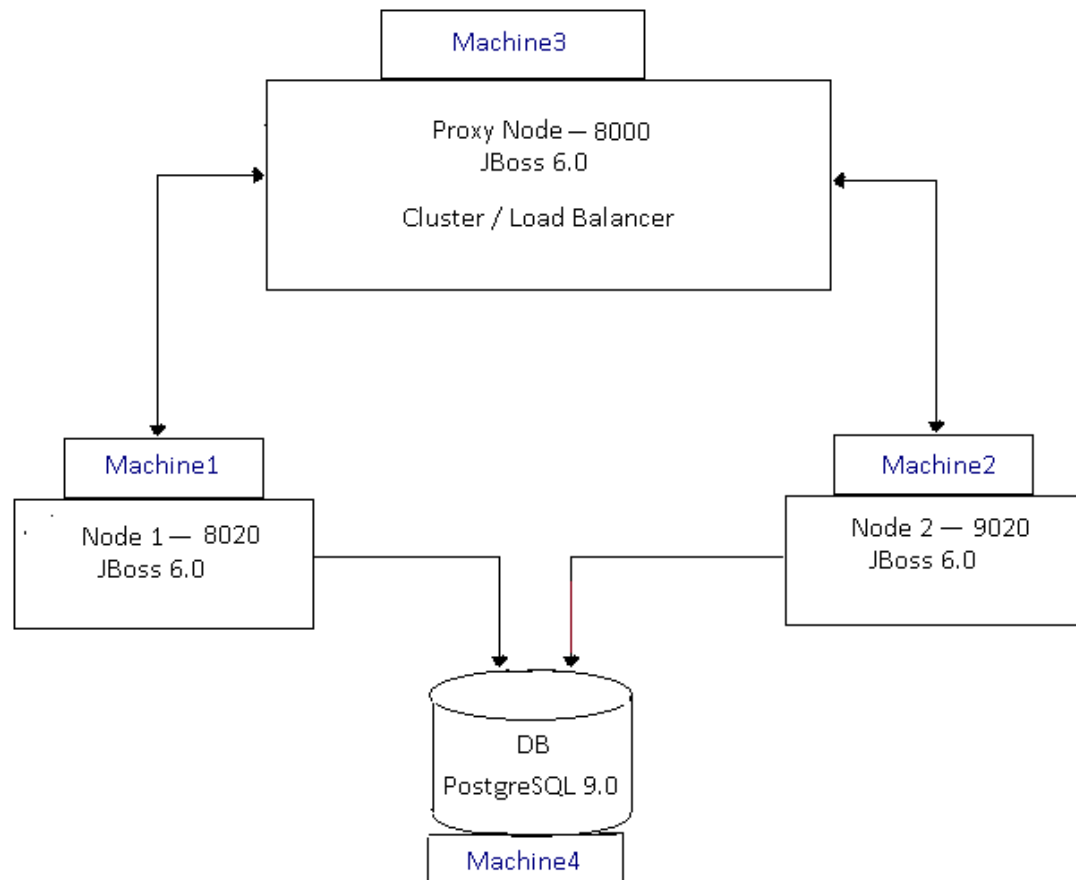
The requirements for the clustered deployment in this example, includes the following:

- Machine 1: JBoss Server Node 1 (JBoss 6.0)
- Machine 2: JBoss Server Node 2 (JBoss 6.0)
- Machine 3: Proxy Node (JBoss 6.0)
- Machine 4: Database Server (PostgreSQL 9.0)



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

**Figure 3-1 Example of a Clustering Setup**



## Installing the Application

You need to install the Smart+Connected PS application on the Node 1 and Node 2 servers.

For information on how to install the Smart+Connected PS application, see the [“Installing the Application”](#) section on page 2-13.

## Configuring Audio Notification to the Cisco IP Phone

You need to configure audio notification to the Cisco IP phone on the Node 1 and Node 2 servers.

For information on how to configure audio notification to the Cisco IP phone, see the [“Configuring Audio Notification to the Cisco IP Phone”](#) section on page 2-15.

## Configuring the Database

For information on how to configure the database, see the [“Configuring the Database”](#) section on page 3-65.

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

## Configuring the JBoss Profile

You need to configure the JBoss profile on the Node 1 and Node 2 servers for a cluster deployment. To configure the JBoss profile, perform the following steps on both the Node 1 and Node 2 servers:

**Step 1** Download the jboss-6.0.0.Final.zip file.

JBoss is open source, and you can download it from the Internet. For example:

<http://sourceforge.net/projects/jboss/files/JBoss/JBoss-6.0.0.Final/jboss-as-distribution-6.0.0.Final.zip/download>

**Step 2** Create a directory named 'jboss', and unzip the jboss-6.0.0.Final.zip file into it.

**Step 3** Set the `$JBOSS_HOME` and `$JAVA_HOME` environment variables by entering the following commands:

```
$ export JAVA_HOME=<JDK_INSTALL_LOCATION>
$ export JBOSS_HOME=<JBOSS_INSTALL_LOCATION>
```

Where, `<JBOSS_INSTALL_LOCATION>` is the complete path where the unzipped jboss-6.0.0 files are available and `<JDK_INSTALL_LOCATION>` is the complete path where you have installed jdk1.6.0\_24.



**Note** You can also add the preceding commands to the user's profile script so that the `$JBOSS_HOME` and `$JAVA_HOME` environment variables are automatically set up during login.

**Step 4** Navigate to the server directory in `$JBOSS_HOME` by entering the following command:

```
cd $JBOSS_HOME/server
```

**Step 5** Copy the 'all' directory with the name 'scps' by entering the following command:

```
cp -R all scps
```

The 'scps' directory is created under the `$JBOSS_HOME/server` directory. The 'scps' directory is used as the Smart+Connected PS application profile.

**Step 6** Copy the ipsapp.war file, available in `<PS_INSTALL_DIRECTORY>/scps/bin/war`, to the `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:

```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/ipsapp.war $JBOSS_HOME/server/scps/deploy
```

**Step 7** Create a datasource file so that the Smart+Connected PS application communicates with the database machine:

**a.** Create the postgres-ds.xml file under the 'scps/deploy' directory with the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<local-tx-datasource>
<jndi-name>jdbc/scc</jndi-name>
<connection-url>jdbc:postgresql://IPaddress:5432/schemaName</connection-url>
<driver-class>org.postgresql.Driver</driver-class>
<user-name>DBusername</user-name>
<password>DBpassword</password>
<min-pool-size>10</min-pool-size>
<max-pool-size>50</max-pool-size>
</local-tx-datasource>
</datasources>
```

**b.** Replace the following text with their actual values in the code that you had added in [Step 7 a.](#):

- 'IPaddress' with the database server IP address or DNS hostname

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

- ‘schemaName’ with the database name
  - ‘5432’ with the database port number, if changed during the PostgreSQL installation
  - ‘DBusername’ with the database schema username
  - ‘DBpassword’ with the database schema password
- c. Save the file.
  - d. Provide the executable permissions to the newly created postgres-ds.xml file by entering the following command:
 

```
chmod 755 postgres-ds.xml
```

**Step 8** Add an entry for scanning deployers:

- a. Navigate to the `$JBOSS_HOME/server/scps/deployers` directory, and open the scanning-deployers-jboss-beans.xml file.
- b. Search for the following text:
 

```
<install method="addIgnored">
  <parameter>java.lang.LinkageError</parameter>
</install>
```
- c. Add the following code after the searched text.
 

```
<install method="addIgnored">
  <parameter>java.lang.reflect.MalformedParameterizedTypeException</parameter>
</install>
```
- d. Save the file.

**Step 9** Update the run.conf file to increase the memory:

- a. Open the run.conf file available in `$JBOSS_HOME/bin` and search for the following text:
 

```
JAVA_OPTS="-Xms128m -Xmx512m -XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

Replace with the following text:

```
JAVA_OPTS="-Xms256m -Xmx1024m -XX:MaxPermSize=512m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```
- b. Save the file.

## Setting Up Port

You need to set up a port for the Smart+Connected PS application by changing the default port values on the Node 1 and Node 2 servers.

For more information on how to set up the port, see the [“Setting Up Port” section on page 3-71](#).

## Setting Up Security Configuration

You need to set up security configuration on the Node 1 and Node 2 servers for the following:

- Disabling the JMS message security, its value is set to ‘true’ by default.
- Authenticating LDAP users of the Smart+Connected PS application.

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

For more information on how to set up security configuration on the Node 1 and Node 2 servers, see the [“Setting Up Security Configuration” section on page 3-72](#).

## Setting Up Java Messaging Service (JMS)

For more information on how to set up JMS on the Node 1 and Node 2 servers, see the [“Setting Up Java Messaging Service \(JMS\)” section on page 3-73](#).

## Setting Up Library

To set up the library, perform the following steps in the Smart+Connected PS application server on the Node 1 and Node 2 servers:

- 
- Step 1** Copy the following jar files to the `$JBOSS_HOME/server/scps/lib` directory:
- `postgresql-9.0-801.jdbc4.jar`—It is open source, and you can be download it from the Internet. For example:  
<http://jdbc.postgresql.org/download/postgresql-9.0-801.jdbc4.jar>
  - `sdp-authmodules.jar`—Available in the `<SDP_INSTALL_DIRECTORY>/sdp/bin/jars` location on the server where the SDP has been installed.
- Step 2** Navigate to the `$JBOSS_HOME/server/scps/lib` directory, and provide the required permissions to the saved files (`postgresql-9.0-801.jdbc4.jar` and `sdp-authmodules.jar`) by entering the following command:
- ```
chmod 755 *
```

## 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.

For more information on how to set up the BIRT engine on the Node 1 and Node 2 servers, see the [“Setting Up the BIRT Engine” section on page 3-78](#).

## Configuring Logging

For more information on how to configure logging on the Node 1 and Node 2 servers, see the [“Configuring Logging” section on page 3-78](#).

## Configuring the Cluster Server Setup

- [Installing mod\\_cluster on the Proxy Node, page 3-99](#)
- [Configuring Cluster on Nodes, page 3-101](#)

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

## Installing mod\_cluster on the Proxy Node

The mod\_cluster is an httpd-based load balancer that uses a communication channel for forwarding requests from httpd to a set of application server nodes. The application server nodes use this connection to transmit the server-side load balance factors and events back to httpd using a set of HTTP methods.

To install mod\_cluster on the proxy node, perform the following steps:

- 
- Step 1** Create a directory in your local system where you want to install the mod\_cluster binary bundle.
- Step 2** Download the Linux 64-bit mod\_cluster 1.1.0 bundle.
- The mod\_cluster is open source, and you can download it from the Internet. For example:
- [http://www.jboss.org/mod\\_cluster/downloads.html](http://www.jboss.org/mod_cluster/downloads.html)
- Step 3** Save and untar the mod\_cluster binary bundle in the directory that you had created in [Step 1](#).
- The directory where you have extracted the mod\_cluster bundle is referred as `<MOD_CLUSTER_HOME>`.
- Step 4** Navigate to the `<MOD_CLUSTER_HOME>/opt/jboss/httpd/sbin` directory and run the “installhome.sh” file.
- The httpd now runs on port “8000”.

- Step 5** To allow the cluster nodes in the network to communicate with the proxy, perform the following:

- a. Navigate to the following location:

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/httpd/conf/
```

- b. Open the httpd.conf file and search for the following text:

```
<Directory />
    Order deny,allow
    Deny from all
</Directory>
```

- c. Replace the default values in the searched text as follows:

```
<Directory />
    Order deny,allow
    Allow from all
</Directory>
```

- d. Save the file.



**Note** By default, mod\_cluster communicates only with the server instances that run on localhost. [Step 5](#) should be performed to allow mod\_cluster to communicate with the proxy.

---

- Step 6** To modify the directory access for Manager Module, perform the following:

- a. Navigate to the following location:

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/httpd/conf/
```

- b. Open the httpd.conf file and search for the following text:

```
<IfModule manager_module>
    Listen 127.0.0.1:6666
    ManagerBalancerName mycluster
    <VirtualHost 127.0.0.1:6666>
    <Directory />
```

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

```

        Order deny,allow
        Allow from all
    </Directory>

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

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

</VirtualHost>
</IfModule>

```

- c. Replace the directory access of the Manager Module in the <Location /mod\_cluster\_manager> element as follows:

```

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

```

After replacing, the text is displayed as follows:

```

<IfModule manager_module>
    Listen 127.0.0.1:6666
    ManagerBalancerName mycluster
    <VirtualHost 127.0.0.1:6666>
    <Directory />
        Order deny,allow
        Allow from all
    </Directory>

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

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

</VirtualHost>
</IfModule>

```

- d. Save and close the file.

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

## Configuring Cluster on Nodes

To configure cluster on nodes, perform the following steps on the Node 1 and Node 2 servers:

### Step 1 Update the server.xml file:

- a. Navigate to the `$JBOSS_HOME/server/scps/deploy/jbossweb.sar` directory, and open the `server.xml` file.

- b. In the `server.xml` file, search for the following text:

```
<Engine name="jboss.web" defaultHost="localhost">
```

- c. Add `jvmRoute` to the Engine “jboss.web”. For example:

- For Node 1:

```
<Engine name="jboss.web" defaultHost="localhost" jvmRoute="node1">
```

- For Node 2:

```
<Engine name="jboss.web" defaultHost="localhost" jvmRoute="node2">
```

- d. In the `server.xml` file, uncomment the following valve, which is commented by default:

```
<Valve className="org.jboss.web.tomcat.service.sso.ClusteredSingleSignOn" />
```



**Note** The valve is uncommented to enable single sign on across web applications deployed on all the hosts in a cluster.

- e. In the `server.xml` file, set the HTTP port, for example, 8020 for Node 1 and 9020 for Node 2:

1. Search for the following text:

```
<!-- A HTTP/1.1 Connector on port 8080 -->
<Connector protocol="HTTP/1.1" port="${jboss.web.http.port}"
address="${jboss.bind.address}"
redirectPort="${jboss.web.https.port}" />
```

2. Replace the `port="${jboss.web.http.port}"` with `port="8020"` for Node 1 and `port="9020"` for Node 2.

- f. Save the `server.xml` file.

### Step 2 Add the proxy hostname and port in the proxyList:

- a. In a file browser, navigate to the `$JBOSS_HOME/server/scps/deploy/mod_cluster.sar/META-INF` directory.

- b. Open the `mod_cluster-jboss-beans.xml` file and search for the following text:

```
<property name="proxyList">
```

- c. Add proxies in the `proxyList` property as follows:

```
<property name="proxyList">${jboss.mod_cluster.proxyList:address:port}</property>
```



**Note** In the `proxyList` property format, the “address:port” refers to the host IP address and port where the proxy is running. The port number is 8000 that you had configured in [Step 4](#) in the “[Installing mod\\_cluster on the Proxy Node](#)” section on page 3-99.

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

- d. Save the `mod_cluster-jboss-beans.xml` file.
- 

## Configuring the Properties Files

You need to configure the `LDAP.properties`, `pvoJms.properties`, `Reservation.properties`, and `notification.service.properties` files on the Node 1 and Node 2 servers.

For information on how to configure the properties files, see the [“Configuring the Properties Files” section on page 3-80](#).

## Setting Up Run Parameters

For information on how to set up run parameters on the Node 1 and Node 2 servers, see the [“Setting Up Run Parameters” section on page 3-82](#).

## Setting Up the Push-to-Phone Feature

For information on how to set up the push-to-phone feature on the Node 1 and Node 2 servers, see the [“Setting Up the Push-to-Phone Feature” section on page 3-83](#).

## 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 3-102](#)
- [Configuring Installer for the iPhones, page 3-104](#)

## Configuring Installer for the Android Phones

To configure installer for the Android phones, perform the following steps on the Node 1 and Node 2 servers:

- 
- 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.



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

### 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 =http://<host>:<port>
  - Where, ‘address’ is the host IP address of the proxy server and ‘port’ is the proxy server port (default 8000) that you had configured in [Step 4](#) in the “Installing mod\_cluster on the Proxy Node” section on page 3-99.
  - serverURL = http://<host>:<port>
  - Where, ‘address’ is the host IP address of the proxy server and ‘port’ is the proxy server port (default 8000) that you had configured in [Step 4](#) in the “Installing mod\_cluster on the Proxy Node” section on page 3-99.



**Note** The secureServerURL and serverURL values are same.

- 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.
- 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**.

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

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 ipsapp.war file:

- a. Double-click the ipsapp.war file from the *\$JBoss\_HOME/server/scps/deploy/ipsapp.war* directory, and open the Archive Manager screen.
- 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 ipsapp.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 on the Node 1 and Node 2 servers:

**Step 1** Extract the download.properties file:

- a. In a file browser, navigate to the directory containing the *\$JBoss\_HOME/server/scps/deploy/ipsapp.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, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the [“Installing mod\\_cluster on the Proxy Node”](#) section on [page 3-99](#).

- c. Save and close the file.

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

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

**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, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the "Installing mod\_cluster on the Proxy Node" section on [page 3-99](#).

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

Where, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the "Installing mod\_cluster on the Proxy Node" section on [page 3-99](#).

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

Where, 'address' is the host IP address of the proxy server and 'port' is the proxy server port (default 8000) that you had configured in [Step 4](#) in the "Installing mod\_cluster on the Proxy Node" section on [page 3-99](#).



**Note** The secureServerURL and serverURL values are same.

- 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
```

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

- 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 ipsapp.war file:
- Double-click the ipsapp.war file from the `$JBOSS_HOME/server/scps/deploy` 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 ipsapp.war file.
- 

## Setting Up 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 set up Jackrabbit, perform the following steps:

- Step 1** Copy the jackrabbit.war file that is available in `<PS_INSTALL_DIRECTORY>/scps/bin/war` to the `$JBOSS_HOME/server/scps/deploy` directory by entering the following command:
- ```
cp <PS_INSTALL_DIRECTORY>/scps/bin/war/jackrabbit.war $JBOSS_HOME/server/all/deploy
```
- Step 2** In a file browser, navigate to the directory containing the `$JBOSS_HOME/server/scps/deploy/jackrabbit.war` file, and double-click this file to open the Archive Manager screen.
- Step 3** Navigate to `/WEB-INF/lib`, select the `jcr-2.0.jar` file, and extract content of the file to the following location:
- ```
$JBOSS_HOME/common/lib
```
- Step 4** Start the proxy on the proxy node and JBoss on the Node 1 server.
- For more information on how to start the proxy and JBoss server, see the [“Starting the Cluster and Proxy” section on page 3-109](#).
- The proxy is up and running on the proxy node, and the JBoss is up and running on the Node 1 server.
- Step 5** In a Web browser, enter the URL `http://address:port/jackrabbit`.
- Where, ‘address’ is the IP address of the proxy server and ‘port’ is the proxy server port that you had configured in [Step 4](#) in the [“Installing mod\\_cluster on the Proxy Node” section on page 3-99](#).
- The Content Repository Setup page appears.
- Step 6** Click **Create Content Repository**.
- The `$JBOSS_HOME/bin/jackrabbit` directory repository structure is created.
- Step 7** Stop the proxy on the proxy node and JBoss on the Node 1 server.
- Step 8** Repeat [Step 1](#) through [Step 7](#) on the Node 2 server.
-

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

## Configuring the Jackrabbit Repository

You need to configure the Jackrabbit repository by providing the DB host IP address, DB port number (default 5432), DB schema name, PS schema username, and PS schema password.

To configure the Jackrabbit repository for clustering, perform the following steps on the Node 1 and Node 2 servers:

**Step 1** Navigate to the `$JBOSS_HOME/bin/jackrabbit` directory, and open the `repository.xml` file.

**Step 2** Search for the below text:

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

Replace with:

```
<FileSystem class="org.apache.jackrabbit.core.fs.db.DbFileSystem">
  <param name="driver" value="org.postgresql.Driver"/>
  <param name="url" value="jdbc:postgresql://<db host IP address>:<db port
number>/<db schemaName>"/>
  <param name="schema" value="postgresql"/>
  <param name="user" value="<schema username>"/>
  <param name="password" value="<schema password>"/>
  <param name="schemaObjectPrefix" value="F_1_"/>
</FileSystem>
```

**Step 3** 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="url" value="jdbc:postgresql://<db host IP address>:<db port number>/<db
schemaName>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="databaseType" value="postgresql"/>
<param name="driver" value="org.postgresql.Driver"/>
<param name="minRecordLength" value="1024"/>
<param name="copyWhenReading" value="true"/>
<param name="tablePrefix" value=""/>
<param name="schemaObjectPrefix" value="D_1_"/>
<param name="schemaCheckEnabled" value="true"/>
</DataStore>
```

**Step 4** 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.PostgreSQLPersistenceManager">
<param name="url" value="jdbc:postgresql://<db host IP address>:<db port number>/<db
schemaName>"/>
<param name="schema" value="postgresql"/>
```

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

```
<param name="user" value="<schema username>" />
<param name="password" value="<schema password>" />
<param name="schemaObjectPrefix" value="W_1_" />
</PersistenceManager>
```

**Step 5** 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.PostgreSQLPersistenceManager">
  <param name="url" value="jdbc:postgresql://<db host IP address>:<db port
number>/<db schemaName>" />
  <param name="schema" value="postgresql" />
  <param name="user" value="<schema username>" />
  <param name="password" value="<schema password>" />
  <param name="schemaObjectPrefix" value="V_1_" />
</PersistenceManager>
```

**Step 6** Add the following text at the end of the preceding text:

```
<Cluster id="node1" syncDelay="1000">
  <Journal class="org.apache.jackrabbit.core.journal.DatabaseJournal">
    <param name="driver" value="org.postgresql.Driver" />
    <param name="url" value="jdbc:postgresql://<db host IP address>:<db port
number>/<db schemaName>" />
    <param name="schema" value="postgresql" />
    <param name="user" value="<schema username>" />
    <param name="password" value="<schema password>3" />
    <param name="schemaObjectPrefix" value="C_1_" />
  </Journal>
</Cluster>
```



**Note** Change the cluster ID accordingly for each node. For example, “node1” for the Node 1 server, “node2” for the Node 2 server, so on.

**Step 7** In the preceding steps, replace the following strings with their actual values:

- *<db host IP address>*—Database server IP address
- *<db port number>*—Database port number
- *<db schemaName>*—Schema name of the database
- *<schema username>*—Database username
- *<schema password>*—Database user password

**Step 8** Navigate to the *\$JBoss\_HOME/bin/jackrabbit/workspaces/* directory, and delete the available default and security directories.

**Step 9** Start the proxy on the proxy node and JBoss on the Node 1 and Node 2 servers, and verify that 13 new tables and 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.

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

## 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 Light Weight Directory Access Protocol (LDAP).

For information on how to import SSL certificates on the Node 1 and Node 2 servers, see the [“Importing SSL Certificates”](#) section on page 3-90.

## Starting the Cluster and Proxy

To start the cluster and proxy, perform the following steps:

**Step 1** Start the cluster by performing the following steps on the Node 1 and Node 2 servers:

- a. Ensure that:
  - SDP is up and running without any binding offset value.
  - The `$JAVA_HOME` environment variable is set to the location in which JDK is installed.
  - The `$JBOSS_HOME` environment variable is set to the complete path where the unzipped jboss-6.0.0 files are available.
- b. Using a terminal session, navigate to the `$JBOSS_HOME/bin` directory.
- c. Enter the following command to start each node in the cluster:
 

```
./run_scps.sh -c scps -Djboss.service.binding.set=ports-01 -b <SERVER_IP_ADDRESS> -g
sdpPartition -Djboss.messaging.ServerPeerID=1
```

Where, `<SERVER_IP_ADDRESS>` is the IP address of the node.

The following options are used to start each node in a cluster:

- `-c`—Refers to start from “scps” configuration.
- `-b`—Refers to the address used to bind the sockets to the default host namely, the localhost.
- `-g`—Refers to the clusters’ partition name. The default name for a JBoss AS cluster is “DefaultPartition”.
- `jboss.service.binding.set`—Refers to setting another JBoss instance for the Smart+Connected PS application. The `ports-01` bindings are obtained by taking the base bindings and by adding 100 to each port value.
- `jboss.messaging.ServerPeerID`—Refers to the JBoss Messaging Clustering (JBM). In JBM, each node in a cluster has a unique integer ID called the “ServerPeerID”. The “ServerPeerID” should remain the same even if the server is restarted many a times.

**Step 2** Start the proxy by performing the following steps on the proxy node:

- a. Using a terminal session, navigate to the following location:
 

```
<MOD_CLUSTER_HOME>/opt/jboss/httpd/sbin
```
- b. Enter the following command to start the proxy:
 

```
./apachectl start
```
- c. Click **Enter**.

The application can be accessed using the proxy that runs on port “8000” by default.

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

**Step 3** (Optional) If you want to stop the proxy, perform the following steps on the proxy node:

- a. Using a terminal session, navigate to the following location:

`<MOD_CLUSTER_HOME>/opt/jboss/httpd/sbin`

- b. Enter the following command to stop the proxy:

`./apachectl stop`

- c. Click **Enter**.
- 

## Accessing the Application and Verifying the Installation

- [Smart+Connected PS Web Application, page 3-110](#)
- [Smart+Connected PS Mobile Application, page 3-110](#)

### Smart+Connected PS Web Application

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

**Step 1** In the Address field of a Web browser, type the application server URL, `http://<address:port>/ipsapp`, and then press **Enter**.

Where, ‘address’ is the host IP address of the proxy server and ‘port’ is the proxy server port (default 8000) that you had configured in [Step 4](#) in the “[Installing mod\\_cluster on the Proxy Node](#)” section on [page 3-99](#).

The Smart+Connected PS login page appears.

**Step 2** 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*.

---

### Smart+Connected PS Mobile Application

For information on how to access the Smart+Connected PS mobile application and verify the installation, see the “[Smart+Connected PS Mobile Application](#)” section on [page 2-44](#).





## Configuring the Smart+Connected PS

---

This chapter describes how to configure locations, devices, room types, and adapters in the Cisco Smart+Connected Personalized Spaces (Smart+Connected PS) application through the Cisco Service Delivery Platform (SDP) interface. It also describes how to modify the branding images for the Smart+Connected PS application.

- [Configuring Locations, page 4-111](#)
- [Configuring Devices, page 4-114](#)
- [Configuring Room Types, page 4-123](#)
- [Configuring Adapters, page 4-123](#)
- [Assigning Roles \(groups\) to the Application User, page 4-130](#)
- [Customizing the Branding Images, page 4-131](#)

### Configuring Locations

You need to configure locations from where the users can search for workspaces in Smart+Connected PS. Because the Smart+Connected PS application depends on SDP for location management, you need to access the Location Management module from the web interface of the SDP application.

To access the SDP web application, you need the DNS hostname or the IP address of the SDP web portal and the port number on which the SDP is configured. The default credentials are superadmin/superadmin. If the default credentials have been updated, then you require the updated credentials.

For detailed information on configuring locations, see the *Cisco Service Delivery Platform User Guide*.

- [Adding Locations, page 4-111](#)
- [Editing a Location, page 4-113](#)
- [Deleting a Location, page 4-113](#)

### Adding Locations

The Smart+Connected PS is used to reserve locations, that are identified as workspaces. When the word ‘workspace’ is used in context of the Smart+Connected PS application, we are referring to location types, such as cubicles and offices.

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

You need to add locations to the Location Hierarchy tree in the following recommended hierarchical order: Location>Country>State>City>Campus>Floor>Wing>Cubicles. For example, Cisco, India, Karnataka, Bangalore, Cessna Park, Floor1, Leftwing, Cubicle 15.

To add a new location to the location hierarchy, perform the following steps:

---



**Step 1** Log in to the SDP application.

**Step 2** Click the **Locations** tab.

The Locations page appears. The left pane displays the location hierarchy, and the right pane displays the main content area.


**Step 3** Select a location for which you want to add the child location in one of the following ways:


a. Searching for a location:

1. Click  in the shortcut tools.
2. In the Search field, enter a location keyword, and click .


The Search Results page appears with the location details. You can select the location for which you want to add the child location.

b. Expanding location hierarchy:

1. Click  before a parent location.


If the  is not displayed before a parent location, the location does not have any child location.

2. Click a location for which you want to add the child location.

Alternatively, click  (**Expand Immediate Child Nodes of Selection** tool), and click a location for which you want to add the child location.

The following details are displayed for the selected location in the Location Details area:

- **Location Type**—Type of location under which the selected location has been categorized.
- **Location Name**—Name of the selected location.
- **Parent Location**—Parent of the selected location.
- Any custom property that has been setup for the location type.

**Step 4** In the main content area, click .

The Add Location page appears. The Parent Location field displays the selected parent location for which you want to add the child location.

**Step 5** Enter the following details:

- **Location Type**—From the Location Type drop-down list, choose the type of the location under which the selected location has to be categorized.
- **Location Name**—Enter the name of the location. The location name can be alpha-numeric, and you can use a maximum of 500 characters.

**Step 6** Click **Save** to save the location details. The newly added location is displayed in the location hierarchy.


---

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

## Editing a Location


After adding a location to the location hierarchy, you can modify the location name, property definition, and description.

To modify the existing location details, perform the following steps:

- 
- Step 1** On the Locations page, select a location for which you want to modify the location details in one of the following ways:
- For more information on how to select a location, perform [Step 1](#) through [Step 3](#) in [Adding Locations](#), page 4-111.
- The following details are displayed for the selected location in the Location Details area:
- **Location Type**— Type of location under which the selected location has been categorized.
  - **Location Name**— Name of the selected location.
  - **Parent Location**—Parent of the selected location.
- Step 2** In the right pane, click .
- The Edit Location page appears. The Parent Location field displays the selected parent location. The Location Type drop-down list displays the type of the selected location.
- Step 3** Modify the following fields as necessary:
- **Location Name**— Name of the selected location. The location name can be alpha-numeric, and you can use a maximum of 500 characters.
  - **Edit Location Properties**—Property definitions that you defined for the location type during installation of the SDP application. For more information, see the sections “Defining Location Properties” and “Creating Custom Location Types” in the *Cisco Service Delivery Platform Installation Guide*.
- Step 4** Click **Save** to save the location details.
- The modified details are updated and appear in the location hierarchy.
- 

## Deleting a Location

To delete a location, perform the following steps:

- 
- Step 1** On the Locations page, select a location that you want to delete.
- For more information on how to select a location, perform [Step 1](#) through [Step 3](#) in [Adding Locations](#), page 4-111.
- The following details are displayed for the selected location in the Location Details area:
- **Location Type**— Type of location under which the selected location has been categorized.
  - **Location Name**— Name of the selected location.
  - **Parent Location**— Parent of the selected location.
- Step 2** In the right pane, click .

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

After a location is deleted, all the child locations, defined property definitions, and the role and device associations for the location are automatically removed from the SDP application.

## Configuring Devices

To avail building system services such as light settings, blinds, dimmer, and air conditioner for locations through the Smart+Connecte PS application, you must configure devices. You must use the SDP interface to access the Device Management module.

- [Adding Device Types, page 4-114](#)
- [Adding a Device, page 4-118](#)
- [Deleting a Devices, page 4-123](#)

## Adding Device Types

Device type definitions for some device types (such as light settings, dimmer, and blind) are added as a part of the SDP seed data. For all Smart+Connected PS needed device type definitions (such as Cisco IP Phone, DMP, and Extension mobility), you need to run additional SQL statements. These scripts are to be run against the schema created earlier.

- [Adding Device Types in the Oracle Database, page 4-114](#)
- [Adding Device Types in the PostgreSQL Database, page 4-116](#)

## Adding Device Types in the Oracle Database

To add device types, run the following scripts using any SQL tool:

- **SSP\_DEVICE\_TYPE**

```
--SSP_DEVICE TYPE inserts
Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID)
values (44,44,1,'Generic','superadmin',sysdate,'superadmin',sysdate,0);

Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID)
values (46,46,1,'Generic','superadmin',sysdate,'superadmin',sysdate,0);

Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID)
values (49,49,1,'Generic','superadmin',sysdate,'superadmin',sysdate,0);

Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID) values
(50,50,1,'Generic','superadmin',sysdate,'superadmin',sysdate,0);
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEFAULT
_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQUIRED_FL
AG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,CREATED_DT,UP
```

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

```
DATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(10038,51,'MACADDRESS',1,0,null,null,null,null,0,'0','1','0','0',4,'superadmin',sysdat
e,'superadmin',sysdate,10001,0);
```

Recreate sequence with updated start value:

```
DROP SEQUENCE SSP_DM_PROP_DEF_ID_SEQ;
CREATE SEQUENCE SSP_DM_PROP_DEF_ID_SEQ INCREMENT BY 1 START WITH 10026 MAXVALUE
99999999999999999999999999999999 MINVALUE 0 NOCACHE;
```

- SSP\_DM\_PROPERTY\_DEFINITION

- Extension Mobility properties:

```
Insert into SSP_DM_PROPERTY_DEFINITION
 (PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEFAULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQUIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,CREATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
 (SSP_DM_PROP_DEF_ID_SEQ.nextval,44,'mobilityaddress',1,0,'0',null,null,null,100,'0',1,'0','0',1,'superadmin',sysdate,'superadmin',sysdate,44,0);
```

- IP Phone properties:

```
Insert into SSP_DM_PROPERTY_DEFINITION
 (PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
  DEFAULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
  UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
  RELATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
 (SSP_DM_PROP_DEF_ID_SEQ.nextval,46,'IP_MACADDRESS',1,0,'0',null,null,null,100,'0',
 '1','0','0',1,'superadmin',sysdate,'superadmin',sysdate,46,0);
```

```
Insert into SSP_DM_PROPERTY_DEFINITION
(
  PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
  DEFAULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
  UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
  REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
  (SSP_DM_PROP_DEF_ID_SEQ.nextval,46,'Application_UserName',1,0,'0',null,null,1
  00,'0','1','0','0',1,'superadmin',sysdate,'superadmin',sysdate,46,0);
```

```
Insert into SSP_DM_PROPERTY_DEFINITION
(
  PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
  AULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
  UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
  REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(SSP_DM_PROP_DEF_ID_SEQ.nextval,46,'Application_Password',1,0,'0',null,null,null,1
00,'0','1','0','0',1,'superadmin',sysdate,'superadmin',sysdate,46,0);
```

```
Insert into SSP_DM_PROPERTY_DEFINITION
(
  PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
  AULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
  UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
  REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(
  (SSP_DM_PROP_DEF_ID_SEQ.nextval,46,'Audio_Loop',1,0,'0',null,null,null,100,'0','1'
  ,'0','0',1,'superadmin',sysdate,'superadmin',sysdate,46,0);
```

```
Insert into SSP_DM_PROPERTY_DEFINITION
(
  PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
  ALT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
  Uired_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
  REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(
  (SSP_DM_PROP_DEF_ID_SEQ.nextval,46,'Audio-Timetoplay',1,0,'0',null,null,100,'
  0','1','0','0',1,'superadmin',sysdate,'superadmin',sysdate,46.0);
```

- DMP Properties:

```
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
AULT VALUE,PROP DEFAULT STRING,PROP DEFAULT NUMBER,PROP DEFAULT DATE,PROP SIZE,REO
```

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

```
UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(SSP_DM_PROP_DEF_ID_SEQ.nextval,49,'TOUCH',1,0,null,null,null,null,0,'0','1','0','
0',1,'superadmin',sysdate,'superadmin',sysdate,49,0);
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
AULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(SSP_DM_PROP_DEF_ID_SEQ.nextval,49,'URL',1,0,null,null,null,null,0,'0','1','0','0'
,2,'superadmin',sysdate,'superadmin',sysdate,49,0);
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
AULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(SSP_DM_PROP_DEF_ID_SEQ.nextval,49,'Password',1,0,null,null,null,null,0,'0','1','0'
,'0',3,'superadmin',sysdate,'superadmin',sysdate,49,0);
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
AULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(SSP_DM_PROP_DEF_ID_SEQ.nextval,49,'Username',1,0,null,null,null,null,0,'0','1','0'
,'0',4,'superadmin',sysdate,'superadmin',sysdate,49,0);
```

Commit;

#### – Interactive Experience Client (IEC) Properties:

```
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID,PROP_GROUP_ID,PROP_NAME,PROP_DATA_TYPE_ID,PROP_CONSTRAINT_ID,PROP_DEF
AULT_VALUE,PROP_DEFAULT_STRING,PROP_DEFAULT_NUMBER,PROP_DEFAULT_DATE,PROP_SIZE,REQ
UIRED_FLAG,APPLICATION_FLAG,UNIQUE_ID_FLAG,SECURE_FLAG,PROP_ORDER_NUM,CREATED_BY,C
REATED_DT,UPDATED_BY,UPDATED_DT,DEVICE_TYPE_ID,TENANT_ID) values
(10038,51,'MACADDRESS',1,0,null,null,null,null,0,'0','1','0','0',4,'superadmin',sy
sdate,'superadmin',sysdate,10001,0);
```

Commit;

## Adding Device Types in the PostgreSQL Database

To add device types, run the following scripts using the pgAdmin tool:

#### • SSP\_DEVICE\_TYPE

```
Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID) values
(10000,44,1,'Generic','superadmin',CURRENT_DATE,'superadmin',CURRENT_DATE,0);
Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID) values
(10001,46,1,'Generic','superadmin',CURRENT_DATE,'superadmin',CURRENT_DATE,0);
Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID,DEVICE_TYPE_MASTER_ID,MANUFACTURER_ID,MODEL,CREATED_BY,CREATED_DT,UPDA
TED_BY,UPDATED_DT,TENANT_ID) values
(10003,45,1,'Generic','superadmin',CURRENT_DATE,'superadmin',CURRENT_DATE,0);
INSERT INTO ssp_device_type
(device_type_id,device_type_master_id,manufacturer_id,model,created_by,created_dt,upda
ted_by,updated_dt,tenant_id) VALUES
(10002,49,1,'dmp','superadmin',CURRENT_DATE,'superadmin',CURRENT_DATE,0);
```

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

```
Insert into SSP_DEVICE_TYPE
(DEVICE_TYPE_ID, DEVICE_TYPE_MASTER_ID, MANUFACTURER_ID, MODEL, CREATED_BY, CREATED_DT, UPDA
TED_BY, UPDATED_DT, TENANT_ID) values
(50, 50, 1, 'Generic', 'superadmin', CURRENT_DATE, 'superadmin', CURRENT_DATE, 0);
Insert into SSP_DM_PROPERTY_DEFINITION
(PROP_DEF_ID, PROP_GROUP_ID, PROP_NAME, PROP_DATA_TYPE_ID, PROP_CONSTRAINT_ID, PROP_DEFAULT
_VALUE, PROP_DEFAULT_STRING, PROP_DEFAULT_NUMBER, PROP_DEFAULT_DATE, PROP_SIZE, REQUIRED_FL
AG, APPLICATION_FLAG, UNIQUE_ID_FLAG, SECURE_FLAG, PROP_ORDER_NUM, CREATED_BY, CREATED_DT, UP
DATED_BY, UPDATED_DT, DEVICE_TYPE_ID, TENANT_ID) values
(10038, 51, 'MACADDRESS', 1, 0, null, null, null, null, 0, '0', '1', '0', '0', 4, 'superadmin', CURREN
T_DATE, 'superadmin', CURRENT_DATE, 10001, 0);
```

Recreate sequence with updated start value:

```
DROP SEQUENCE SSP_DM_PROP_DEF_ID_SEQ;
CREATE SEQUENCE SSP_DM_PROP_DEF_ID_SEQ START WITH 10026 MAXVALUE 9223372036854775807
MINVALUE 0 NO CYCLE;
```

- **SSP\_DM\_PROPERTY\_DEFINITION**

- **Extension Mobility properties:**

```
INSERT INTO ssp_dm_property_definition
(prop_def_id, prop_group_id, prop_name, prop_data_type_id, prop_constraint_id, prop_def
ault_value, prop_default_string, prop_default_number, prop_default_date, prop_size, req
uired_flag, application_flag, unique_id_flag, secure_flag, prop_order_num, created_by, c
reated_dt, updated_by, updated_dt, device_type_id, tenant_id) VALUES
(10000, 44, 'mobilityaddress', 1, 0, null, '', null, null, 0, '0', '1', '0', '0', 1, 'superadmin',
CURRENT_DATE, 'superadmin', CURRENT_DATE, 10000, 0);
```

- **IP Phone properties:**

```
INSERT INTO ssp_dm_property_definition
(prop_def_id, prop_group_id, prop_name, prop_data_type_id, prop_constraint_id, prop_def
ault_value, prop_default_string, prop_default_number, prop_default_date, prop_size, req
uired_flag, application_flag, unique_id_flag, secure_flag, prop_order_num, created_by, c
reated_dt, updated_by, updated_dt, device_type_id, tenant_id) VALUES
(10001, 46, 'IP_MACADDRESS', 1, 0, null, '', null, null, 0, '0', '1', '0', '0', 1, 'superadmin', C
URRENT_DATE, 'superadmin', CURRENT_DATE, 10001, 0);
INSERT INTO ssp_dm_property_definition
(prop_def_id, prop_group_id, prop_name, prop_data_type_id, prop_constraint_id, prop_def
ault_value, prop_default_string, prop_default_number, prop_default_date, prop_size, req
uired_flag, application_flag, unique_id_flag, secure_flag, prop_order_num, created_by, c
reated_dt, updated_by, updated_dt, device_type_id, tenant_id) VALUES
(10002, 46, 'Application_Password', 1, 0, null, '', null, null, 0, '0', '1', '0', '0', 2, 'supera
dmin', CURRENT_DATE, 'superadmin', CURRENT_DATE, 10001, 0);
INSERT INTO ssp_dm_property_definition
(prop_def_id, prop_group_id, prop_name, prop_data_type_id, prop_constraint_id, prop_def
ault_value, prop_default_string, prop_default_number, prop_default_date, prop_size, req
uired_flag, application_flag, unique_id_flag, secure_flag, prop_order_num, created_by, c
reated_dt, updated_by, updated_dt, device_type_id, tenant_id) VALUES
(10003, 46, 'Audio_Loop', 1, 0, null, '', null, null, 0, '0', '1', '0', '0', 3, 'superadmin', CURR
ENT_DATE, 'superadmin', CURRENT_DATE, 10001, 0);
INSERT INTO ssp_dm_property_definition
(prop_def_id, prop_group_id, prop_name, prop_data_type_id, prop_constraint_id, prop_def
ault_value, prop_default_string, prop_default_number, prop_default_date, prop_size, req
uired_flag, application_flag, unique_id_flag, secure_flag, prop_order_num, created_by, c
reated_dt, updated_by, updated_dt, device_type_id, tenant_id) VALUES
(10004, 46, 'Application_UserName', 1, 0, null, '', null, null, 0, '0', '1', '0', '0', 4, 'supera
dmin', CURRENT_DATE, 'superadmin', CURRENT_DATE, 10001, 0);
INSERT INTO ssp_dm_property_definition
(prop_def_id, prop_group_id, prop_name, prop_data_type_id, prop_constraint_id, prop_def
ault_value, prop_default_string, prop_default_number, prop_default_date, prop_size, req
uired_flag, application_flag, unique_id_flag, secure_flag, prop_order_num, created_by, c
```

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

```
reated_dt,updated_by,updated_dt,device_type_id,tenant_id) VALUES
(10005,46,'Audio_Timetoplay',1,0,null,'',null,null,0,'0','1','0','0',5,'superadmin',
',CURRENT_DATE','superadmin',CURRENT_DATE,10001,0);
```

– DMP properties:

```
INSERT INTO ssp_dm_property_definition
(prop_def_id,prop_group_id,prop_name,prop_data_type_id,prop_constraint_id,prop_def
ault_value,prop_default_string,prop_default_number,prop_default_date,prop_size,req
uired_flag,application_flag,unique_id_flag,secure_flag,prop_order_num,created_by,c
reated_dt,updated_by,updated_dt,device_type_id,tenant_id) VALUES
(10026,49,'TOUCH',1,0,null,null,null,0,'0','1','0','0',1,'superadmin',CURRENT
_DATE,'superadmin',CURRENT_DATE,10002,0);
INSERT INTO ssp_dm_property_definition
(prop_def_id,prop_group_id,prop_name,prop_data_type_id,prop_constraint_id,prop_def
ault_value,prop_default_string,prop_default_number,prop_default_date,prop_size,req
uired_flag,application_flag,unique_id_flag,secure_flag,prop_order_num,created_by,c
reated_dt,updated_by,updated_dt,device_type_id,tenant_id) VALUES
(10027,49,'URL',1,0,null,null,null,null,0,'0','1','0','0',2,'superadmin',CURR
ENT_DATE,'superadmin',CURRENT_DATE,10002,0);
INSERT INTO ssp_dm_property_definition
(prop_def_id,prop_group_id,prop_name,prop_data_type_id,prop_constraint_id,prop_def
ault_value,prop_default_string,prop_default_number,prop_default_date,prop_size,req
uired_flag,application_flag,unique_id_flag,secure_flag,prop_order_num,created_by,c
reated_dt,updated_by,updated_dt,device_type_id,tenant_id) VALUES
(10028,49,'Password',1,0,null,null,null,null,0,'0','1','0','0',3,'superadmin',CURR
ENT_DATE,'superadmin',CURRENT_DATE,10002,0);
INSERT INTO ssp_dm_property_definition
(prop_def_id,prop_group_id,prop_name,prop_data_type_id,prop_constraint_id,prop_def
ault_value,prop_default_string,prop_default_number,prop_default_date,prop_size,req
uired_flag,application_flag,unique_id_flag,secure_flag,prop_order_num,created_by,c
reated_dt,updated_by,updated_dt,device_type_id,tenant_id) VALUES
(10029,49,'Username',1,0,null,null,null,null,0,'0','1','0','0',4,'superadmin',CURR
ENT_DATE,'superadmin',CURRENT_DATE,10002,0);
```

– IEC Properties:

```
Insert into SSP_DM_PROPERTY_DEFINITION
(Prop_Def_Id,Prop_Group_Id,Prop_Name,Prop_Data_Type_Id,Prop_Constraint_Id,Prop_Def
ault_Value,Prop_Default_String,Prop_Default_Number,Prop_Default_Date,Prop_Size,Req
uired_Flag,Application_Flag,Unique_Id_Flag,Secure_Flag,Prop_Order_Num,Created_By,C
reated_Dt,Updated_By,Updated_Dt,Device_Type_Id,Tenant_Id) values
(10038,51,'MACADDRESS',1,0,null,null,null,null,0,'0','1','0','0',4,'superadmin',CU
RRENT_DATE,'superadmin',CURRENT_DATE,10001,0);
```

```
Commit;
```

## Adding a Device

The following devices are supported by the Smart+Connected PS application:

- Cisco IP Phones
- Blinds
- Lights
- Dimmer
- DMP
- Extension Mobility
- VAV



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

- IEC

You can add any of these devices to the selected location in the Location Hierarchy tree if they are available at the location. Before adding devices, ensure that the device types are created. You can create a new device type that is supported by SDP by utilizing the device type properties that are shipped along with SDP.

Table 4-1 lists the device properties of the devices that have been added by the Smart+Connected PS scripts.

**Table 4-1**      **Device Properties and Values**

Device	Model	Device Properties	Value Description	Sample Data
IP Phone	Model name	MAC Address	The MAC Address of the IP phone.	SEP0021CCBA8B34
		Audio_Loop	The number of times the audio loop needs to play.	1
		Audio_Timetoplay	The time set for the audio play.	1
		Application_UserName	The Call Manager Application UserID username	examd
		Application_Password	The Call Manager Application User password	examd
Mobility	Model name	mobilityaddress	MAC address of the IP phone	SEP0021CCBA8B34
Digital Media Player	Generic	username	DMP username	admin
		Touch	The configuration to enable touch.	No
		url	The https URL for the DMP.	https ://10.255.255.254
		password	DMP password	exam123
IEC	Generic	MAC Address	The MAC Address of the IEC device.	00:21:CC:BA:8B:34

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

**Table 4-1**      **Device Properties and Values (continued)**

Device	Model	Device Properties	Value Description	Sample Data
Blinds	Generic	Open Value	Value to be set on open path to open the blinds.	true
		Close Value	Value to be set on close path to close the blinds.	false
		Stop Value	Value to be set on stop path to stop the blinds.	true
		Open Path	The node path in the BMS gateway for opening the blinds.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conferance_Room/Blinds/BO/Blind_Open_Close/
		Stop Path	The node path in the BMS gateway for stopping the blinds, when the blinds is opening or closing.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conferance_Room/Blinds/BO/Blind_Stop/
		Close Path	The node path in the BMS gateway for closing the blinds.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conferance_Room/Blinds/BO/Blind_Open_Close/
		Blinds Value	Value to be set on blinds URL to open or close the blinds.	0
Lights	Generic	On Value	Value to be set on On/Off URL to switch on the lights.	true
		On/Off URL	The node path in the BMS gateway for switching On/Off the lights.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_HA/HallMark/BGL10/Floor_01/Conferance_Room/Light_Switch/BO/Lights_ON_OFF/
		Off Value	Value to be set on On/Off URL to switch off the lights.	false

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

**Table 4-1**      **Device Properties and Values (continued)**

Device	Model	Device Properties	Value Description	Sample Data
Dimmer	Generic	Min Value	The minimum luminosity value.	0.0
		Max Value	The maximum luminosity value.	100.0
		Dim URL	The node path in the BMS gateway for configuring the dimmer luminosity.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_HA/HallMark/BGL10/Floor_01/Conference_Room/Light_Dimmer/AO/Light_Dimmer_Control/
	Wattstopper Light Dimmer	Dimmer Values	The scene value to be set on the BMS gateway.	50.0
		dimmer_ URL	Node path in the BMS gateway for setting the light scene.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_HA/HallMark/BGL10/Floor_01/Conference_Room/WattstopperLight_Dimmer/AO/Light_Dimmer_Control/
VAV	Generic	Current Temperature URL	The node path in the BMS gateway for getting the current temperature.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/AV/SpaceTemp_Setpt/
		Occupancy Status URL	The node path in the BMS gateway for getting the status for occupancy.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/BI/OccUnocc_Sts/
		Occupied Temperature URL	The node path in the BMS gateway for getting occupied cool values.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/AV/RoomTemp_OccSetpt/

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

**Table 4-1**      **Device Properties and Values (continued)**

Device	Model	Device Properties	Value Description	Sample Data
		Min Temperature Value	Minimum temperature to which the room temperature can be set.	18
		Max Temperature Value	The maximum range of the room temperature that can be set.	28
		Temperature Unit	The unit of temperature.	C or F
		Occupied Value	Value to be set on occupancy status URL to move the device to occupied mode.	true
		Unoccupied Value	Value to be set on occupancy status URL to move the device to unoccupied mode.	false
		Temperature Setpoint URL	The node path in the BMS gateway for configuring and reading back the current setpoint temperature.	/config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/AV/SpaceTemp_Setpt/

To add a device, perform the following steps:

- 
- Step 1**    On the SDP home page, click **Devices**.  
The List of Devices page appears.
- Step 2**    Select a location in the left pane.
- Step 3**    Click **Add a Device** in the right pane.  
The Add Device page appears.
- Step 4**    Select a **Device Category**.
- Step 5**    Select the **Manufacturer**.
- Step 6**    Select the **Model**.  
Properties of the selected device are displayed when the model is selected in the Add Device Properties box.
- Step 7**    To select the properties for the device, perform the following steps:
- Select the property of the device in the Add Device Properties box.

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

The value box is displayed on the right side.

- b. Select or enter the corresponding value.
- c. Click **Save**.

**Step 8** Type the name of the device in the **Device Name** field.

**Step 9** Click **Save**.

The new device is added to the selected location.

## Deleting a Devices

To delete a device, perform the following steps:

- Step 1** In the SDP home page, click the **Devices** tab.
- Step 2** To view devices in child locations, select the **Show devices from child locations** check box.
- Step 3** In the Location Hierarchy tree, select the location from where you want to delete an associated device. The list of associated devices appear on the right, if available.
- Step 4** Select the check box corresponding to the device that you want to delete, and click **Delete**.

## Configuring Room Types

By default, the Office and Cubicle location types are configured as workspaces in the Smart+Connected PS solution. If any other location type is also to be treated as workspaces, then the necessary configuration needs to be done in SSP\_PVO\_LOCATION\_TYPE table.

Table 4-2 displays the LOC\_TYPE\_ID, which is the location type ID mapping in the SSP\_LOCATION\_TYPE table that is available in SDP.

**Table 4-2 Room Types Properties**

Location Type ID (LOC_TYPE_ID)	Name (LOC_TYPE_NAME)
15	Cubicle
23	Office

## Configuring Adapters

- [Adapter Description, page 4-124](#)
- [Configuring Adapter Properties, page 4-124](#)
- [Configuring the Adapters to a Location, page 4-127](#)

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

## Adapter Description

Table 4-3 lists the adapters you must configure and the purpose these adapters serve for the functioning of the Smart+Connected PS application.

**Table 4-3 Adapter Description**

Adapter	Description
ObixBean	Configure this adapter to interface with the Tridium BMS.
ExchangeBean	Configure this adapter to interface with Microsoft Exchange.
RemedyBean	Configure this adapter to interface with the Remedy case management system.
EmailBean	Configure this adapter to use e-mail based case notifications, in the absence of a case management system.
IPPhoneOperationBean	Configure this adapter to interface with Cisco JTAPI for sending emergency notifications.
DMPBean	Configure this adapter to interface with the digital media players.

## Configuring Adapter Properties

You need to configure the adapter properties for available adapters. The adapter definitions are inserted in the Smart+Connected PS database, when you execute the SDP and Smart+Connected PS database scripts. Adapter configuration needs to be performed in the database by inserting data into the SDP\_ADAPTER\_PROPERTIES table.

Table 4-4 provides information on the properties of the adapters. These can be used to come up with the SQL scripts that must be run against the database. All these properties are mandatory.

**Table 4-4 Adapter Properties**

Adapter (SDP_ADAPTER_DEFN)	Defined Adapter Property (SDP_ADAPTER_PROP_DEFN)	Adapter Properties (SDP_ADAPTER_PROPERTIES)	Sample Values
com.cisco.cre.ssp.adapter.iphone.IPPhoneOperationBean	cucmurl	The url of the configured Call Manager	<a href="https://198.51.100.254/realtimeservice/services/RisPort70">https://198.51.100.254/realtimeservice/services/RisPort70</a>
	cucmusername	The CUCM admin username.	exam @123
	cucmpassword	The CUCM admin password.	ccmadmin

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

**Table 4-4 Adapter Properties (continued)**

Adapter (SDP_ADAPTER_DEFN)	Defined Adapter Property (SDP_ADAPTER_PROP _DEFN)	Adapter Properties (SDP_ADAPTER_PRO PERTIES)	Sample Values
	audiourl	The url of the audio to be played on the phone <x> minutes before the auto logout.	http: //10.255.255.254:10020/ipsapp/audio/audio_IpPhone.avi
	message	The audio message.	You will be autochecked out in five minutes.
com.cisco.cre.ssp.adapter.casemanagement.EmailBean	fromaddress	The address from which the e-mail needs to be sent for a case management. Typically, this is set up as a no reply mailbox.	somebody @example.com
	mailsmtphost	The IP Address or the hostname of the SMTP server.	mailman. example.com
	mailsmtpport	The SMTP server port.	25
	toaddress	The address to which the e-mail needs to be sent for the case management. Typically, this is the facilities team helpdesk mail alias.	support @example.com
com.cisco.cre.ssp.adapter.mobility.MobilityBean	mobappcertificate	The userid of the CUCM application user account that allows the solution to do an extension mobility login/logout on behalf of the user.	exam @123
	mobappid	Password of the CUCM application user account that allows the solution to do extension mobility login/logout on behalf of the user.	ccmadmin
	mobilityurl	The url to the callmanager	https ://198.51.100.254:8443/emservice/EMServiceServlet

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

**Table 4-4 Adapter Properties (continued)**

<b>Adapter (SDP_ADAPTER_DEFN)</b>	<b>Defined Adapter Property (SDP_ADAPTER_PROP _DEFN)</b>	<b>Adapter Properties (SDP_ADAPTER_PRO PERTIES)</b>	<b>Sample Values</b>
com.cisco.cre.ssp.adapter.obix.ObixBean	obixUrl	The obix url	http ://10.255.255.254/obix
	url	The obix url	http ://10.255.255.254/obix
	username	The obix username	admin
	password	The obix username	admin
com.cisco.cre.ssp.adapter.remedy.RemedyBean	password	The password of the Remedy user.	WPRcreIT4
	userName	The username of the Remedy user.	RA_WPRIT.gen
	scheme	The Protocol to invoke the remedy HTTP/HTTPS.	http
	appPath	The path of the Remedy application.	/arsys/servlet/RemedyIncidentWrapper
	remedyurl	The Remedy server URL	http: //remedy.example.com /arsys/servlet/RemedyIncidentWrapper
	hostName	The Remedy server IP Adress or the DNS Hostname	remedy.example.com
	portNumber	The Remedy server port number.	80



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

**Table 4-4 Adapter Properties (continued)**

Adapter (SDP_ADAPTER_DEFN)	Defined Adapter Property (SDP_ADAPTER_PROP _DEFN)	Adapter Properties (SDP_ADAPTER_PRO PERTIES)	Sample Values
com.cisco.cre.ssp.adapter.exchangeBean	exch_udpserverip	The MS application server IP address/DNS hostname	10.106.13.15
	exch_filepath	The path of the file in Exchange Server.	/apps/exchange-xml/
	exch_defaulttimezone	The timezone of the Exchange Server.	Asia/Shanghai
	exch_domain	The domain name of the Exchange Server.	EXCH2K10
	exch_host	The IP address/DNS hostname Exchange Server.	10.106.13.143
	mail.smtp.host	This property is not used currently.	–
	exch_url	Exchange URL	https://10.106.13.143/ews/exchange.asmx
	exch_username	The Exchange server username.	scc-qa
	exch_password	The Exchange server password.	Cisco_123
	mail.smtp.port	This property is not used currently.	–
	exch_udpserverport	The MS Application server listen port.	7001
com.cisco.cre.ssp.adapter.dmp.DMPBean	dmp_url	The DMP URL.	https://scc-qa-dmp-1.cisco.com:8443
	dmp_username	The DMP username.	superuser
	dmp_domain	The domain of DMP.	scc-qa-dmp-1.cisco.com
	dmp_password	The DMP password.	Cisco_123

## Configuring the Adapters to a Location

The adapters are configured to the specific location by mapping the adapter instance id with the corresponding location in the SDP\_ADAPTER\_LOCATION\_LINK table.

When an adapter is associated to a location, the adapter instances are automatically applied to all the child locations for that location.

See the “[Sample Adapter Configurations](#)” section on page 4-128 for a sample configuration for the ObixBean mapped to the location ID 10011.

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

## Sample Adapter Configurations

### SDP\_ADAPTER\_DEFN table

This configuration is part of the seed data.

Table 4-5 displays the adapter definition mapped to an adapter definition ID.

**Table 4-5** *SDP\_ADAPTER\_DEFN table*

ADAPTER_DEFN_ID	ADAPTER	ADAPTER_JAR_LOCATION	VERSION	CREATE_D_BY	CREATE_D_DT	UPDATED_BY	UPDATED_DT	TENANT_ID
10	com.cisco.cre.ssp.adapter.obixBean		version1	superadmin	27-JUN-12	superadmin	27-JUN-12	0

### SDP\_ADAPTER\_INSTANCE

Table 4-6 displays the adapter definition ID mapped to an adapter instance ID

**Table 4-6** *SDP\_ADAPTER\_INSTANCE*

ADAPTER_INSTANCE_ID	ADAPTER_DEFN_ID	VERSION	CREATED_BY	CREATED_DT	UPDATED_BY	UPDATED_DT	TENANT_ID
10	10	version1	superadmin	27-JUN-12	superadmin	27-JUN-12	0

### SDP\_ADAPTER\_LOCATION\_LINK table

This table allows you to link the adapter instances with a specific location(s).

Table 4-7 displays the adapter instance ID configured to the preferred location

**Table 4-7** *SDP\_ADAPTER\_LOCATION\_LINK table*

ADAPTER_INSTANCE_ID	LOCATION_ID	CREATED_BY	CREATED_DT	UPDATED_BY	UPDATED_DT	TENANT_ID
10	10011	versions	18-NOV-11	versions	18-NOV-11	0

For more information on configuring adapters, refer to the *Cisco Service Delivery Platform Installation Guide*.



#### Note

If you change values in these tables, then you must restart the application to enable the changes done.

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

## Configuring Services in CUCM

The Smart+Connected PS services appear on the Cisco IP phone only after you configure the Smart+Connected PS URL on the CUCM. It is assumed that the Extension Mobility is enabled for the device and the end-user. Typically, these tasks must be performed by the CUCM Administrator.

To configure the services in the CUCM, perform the following steps:

- 
- Step 1** In the browser, enter the CUCM URL.
- Step 2** Click **Cisco Unified Communications Manager**.  
The Cisco Unified CM Administration home page appears.
- Step 3** new
- Step 4** Enter the CUCM administration username and password, and then click **Login**.
- Step 5** Navigate to **Device>Device Settings>Phone Services**.
- Step 6** Click **Add New**.  
To add a new service, perform the following steps:
- a. Enter the service name in the Service Name field. For example, SCPS service.
  - b. Enter the service description in the Service Description field.
  - c. Enter the service URL in the Service URL field. The format is as follows:  
`http://<IP Address>:<port number>/ipsapp/pvoipphone.ip`  
  
Where, the 'IP Address' of Smart+Connected PS server specifies the IP address of server where the Smart+Connected PS application is running and the 'Port Number' is the the port number that you have configured for launching the Smart+Connected PS application.
  - d. From the Service Category drop-down list, choose **XML Service**.
  - e. From the Service Type drop-down list, choose **Standard IP Phone Service**.
  - f. Select the **Enable** checkbox.
- Step 7** Click **Save**.
- Step 8** Click **Device>Phone**. The Find and List Phones page appears.
- Step 9** From the "Find Phone where" drop-down list, choose **Device Name**.
- Step 10** Choose **contains** from the drop-down list adjacent to the "Find Phone where" drop-down list.
- Step 11** Enter the MAC address of the Cisco IP phone for which you want to subscribe the service.
- Step 12** Click **Find**.
- Step 13** Select the Cisco IP phone. The Phone Configuration page appears.




---

**Note** Ensure that the Web Access drop-down list displays an enabled value.

---

- Step 14** In the Related Links drop-down list, choose **Subscribe/Unsubscribe Services**, and then click **Go**.
- Step 15** Select the service name that you have provided in Step a.
- Step 16** Click **Next**.
- Step 17** Click **Subscribe**.

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

- Step 18** Click **Reset** in the Phone Configuration page. A device reset pop-up appears.
  - Step 19** Click **Reset**. The configured service name appears under the Services menu, in the Cisco IP Phone.
  - Step 20** Subscribe the "SCPS service" for the default Extension Mobility profile or the extension mobility profile of an individual user.
  - Step 21** Subscribe the "SCPS service" to the Extension Mobility logout profile (if enabled for IP phone).
- 

## Assigning Roles (groups) to the Application User

The Smart+Connected PS solution require an application user to be created in CUCM for the following reasons:

- To do an Extension Mobility login on the behalf of an user.
- To push the audio unicast and text messages to the Cisco IP phone.

The application user needs the following privileges minimally to allow the Smart+Connected PS solution to work properly:

- Standard CTI Enabled—This user group, which is required for all CTI applications, allows an application to connect to Cisco CallManager to access CTI functionality.
- Standard CTI Allow Control of All Devices—This user group allows an application to control or monitor any CTI-controllable device in the system.
- Standard EM Authentication Proxy rights -- This user group manages Cisco Extension Mobility authentication rights for application users that interact with Cisco Extension Mobility.
- Standard CCM Admin Users—This grants log-in rights to Cisco Unified Communications Manager Administration. A user with only the Standard CCM Admin Users role can access Cisco Unified Communications Manager Administration but cannot make any changes.
- Standard CCMADMIN Read only— This allows an administrator to view configuration in Cisco Unified Communications Manager Administration page
- Copy of Standard CCM Phone Administration which includes Service URL Page, User Web Page and Phone Services Subscribe.
- Copy of Standard Serviceability named as roles for Web Services which has only SOAP related services as read and write access.

To create and assign a role to an application user, perform the followin steps:

- 
- Step 1** In the browser, enter the URL to access the Call Manager application.
  - Step 2** Click **Cisco Unified Communications Manager**.  
The Cisco Unified CM Administration home page appears.
  - Step 3** Enter the username and password and click **Login**.
  - Step 4** Navigate to **User Management > Application User** to create application users and assign roles to the application users.
-

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

## Customizing the Branding Images

The branding images include the logo and the login screen. You can customize the Smart+Connected PS user interface by changing one or both of these images.

To customize the branding images, perform the following steps:

- Step 1** Open the scps.war file using any archive utility.
- Step 2** Navigate to the images directory and replace the login and the logo images.

[Table 4-8](#) displays the specifications of the branding images.

**Table 4-8**      **Branding Image Specification**

Image Type	File Name	Width	Height
Logo	cisco_logo.png	607 pixels	686 pixels
Login Background	IPS_Login_Image.jpg	750 pixels	664 pixels



**Note**

Branding images that you replace must have the same name and resolution as per the specification provided in [Table 4-8](#).



**Note**

You must re-deploy the scps.war file to enable changes to the branding images.

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



---

## A

### about

- cluster server setup [1-7](#)
- JMS properties file for JBoss [2-29, 3-80](#)
- LDAP properties file for JBoss [2-26, 3-80](#)
- mod\_cluster [2-51, 3-99](#)
- non-cluster server setup [1-6](#)
- notification properties file for JBoss [2-32, 3-81](#)
- properties file for JBoss [2-26, 3-80](#)
- reservation properties file for JBoss [2-30, 3-81](#)
- Smart+Connected PS [1-1](#)
- system architecture [1-1](#)

### adapter

- about [4-128](#)
- sample configuration [4-128](#)

---

## C

### cluster

- configuring Apache Jackrabbit on JBoss [2-59, 3-107](#)
- configuring cluster for JBoss [2-53, 3-101](#)
- configuring JBoss profile [2-48, 3-96](#)
- installing mod\_cluster for JBoss [2-51, 3-99](#)
- installing on JBoss [2-44, 3-92](#)
- overview [1-7](#)
- setting up Apache Jackrabbit on JBoss [2-58, 3-106](#)
- starting server for JBoss [2-61, 3-109](#)

### colocated

- deploying Apache Jackrabbit on JBoss [2-41, 3-85, 3-89, 3-102](#)
- deploying Apache Jackrabbit on Oracle [2-37, 2-54](#)

### configuring

### adapter [4-123](#)

- adapter description [4-124](#)
- adapter properties [4-124](#)
- adapter to location [4-127](#)
- cluster for JBoss [2-53, 3-101](#)
- customizing branding image [4-131](#)
- device [4-114, 4-118, 4-123](#)
- location [4-111](#)
- push-to-phone for JBoss [2-35, 3-83](#)
- room types [4-123](#)

---

## D

### database script

- database script for JBoss [3-65](#)
- executing for JBoss [3-68](#)
- executing for JBoss and Oracle [2-13](#)

### device

- adding [4-118](#)
- configuring [4-114](#)
- deleting [4-123](#)

---

## E

### emergency notification system

- JTAPI [4-124](#)

---

## I

### installing

- JBoss
  - cluster server setup [2-44, 3-92](#)

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

configuring Apache Jackrabbit for cluster [2-59, 3-107](#)

configuring cluster [2-53, 3-101](#)

configuring JBoss profile for cluster [2-48, 3-96](#)

deploying Apache Jackrabbit for non-cluster or colocated [2-41, 3-89](#)

importing SSL certificate [2-42, 3-90](#)

installing mod\_cluster for cluster [2-51, 3-99](#)

non-cluster server setup [2-10, 3-64](#)

prerequisite [2-9, 3-63](#)

setting up Apache Jackrabbit for cluster [2-58, 3-106](#)

setting up push-to-push feature [2-35, 3-83](#)

setting up run parameter [2-34, 3-82](#)

starting server [2-61, 3-109](#)

updating LDAP and JMS properties files [2-33, 3-81](#)

updating reservation and notification properties files [2-33, 3-82](#)

#### JBoss and Oracle

deploying Apache Jackrabbit for non-cluster or colocated [2-37](#)

#### Oracle

deploying Apache Jackrabbit for non-cluster or colocated [2-54, 3-85, 3-102](#)

verifying for JBoss [2-43, 2-62, 3-91, 3-110](#)

location name [4-112](#)

location type [4-112](#)

## N

### non-cluster

deploying Apache Jackrabbit on JBoss [2-41, 3-85, 3-89, 3-102](#)

deploying Apache Jackrabbit on Oracle [2-37, 2-54](#)

installing on JBoss [2-10, 3-64](#)

overview [1-6](#)

## O

### overview

cluster server setup [1-7](#)

JMS properties file for JBoss [2-29, 3-80](#)

LDAP properties file for JBoss [2-26, 3-80](#)

mod\_cluster [2-51, 3-99](#)

non-cluster server setup [1-6](#)

notification properties file for JBoss [2-32, 3-81](#)

properties file for JBoss [2-26, 3-80](#)

reservation properties file for JBoss [2-30, 3-81](#)

Smart+Connected PS [1-1](#)

## J

### JBoss

application server details [2-9, 3-63](#)

configuring profile [2-48, 3-96](#)

database server details [2-9, 3-63](#)

setting up run parameter [2-34, 3-82](#)

verifying network configuration [2-10, 3-64](#)

## L

### location

adding location [4-111, 4-112](#)

configuring [4-111](#)

## P

### prerequisite

for installing on JBoss [2-9, 3-63](#)

### properties file

#### JBoss

about [2-26, 3-80](#)

updating LDAP and JMS properties files for JBoss [2-33, 3-81](#)

updating reservation and notification properties files for JBoss [2-33, 3-82](#)



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

---

## **S**

### server setup

cluster [1-7](#)

non-cluster [1-6](#)

type [1-5](#)

### Smart+Connected PS

about [1-1](#)

accessing or verifying for JBoss [2-43, 2-62, 3-91, 3-110](#)

acronyms and abbreviations [1-3](#)

cluster server setup [1-7](#)

installing application [2-13, 2-37, 2-54, 3-85, 3-102](#)

installing on JBoss [2-9, 3-63](#)

cluster [2-44, 3-92](#)

colocated or non-cluster [2-10, 3-64](#)

non-cluster server setup [1-6](#)

server setup type [1-5](#)

system architecture [1-1](#)

### SSL certificate

importing for JBoss [2-42, 3-90](#)

### starting

cluster for JBoss [2-61, 3-109](#)

JBoss server for colocated or non-cluster [2-43, 3-91](#)

proxy server for JBoss [2-61, 3-109](#)

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