



Send documentation comments to scc-docfeedback@cisco.com



Cisco Smart+Connected Spaces Installation Guide

Release 2.5

December, 2014

Cisco Systems, Inc.
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.

Text Part Number:

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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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)

Cisco Smart+Connected Spaces Installation Guide
© 2014 Cisco Systems, Inc. All rights reserved.



Preface iii

- Audience iii
- Organization iii
- Document Conventions iv
- Related Documentation iv
- Documentation Feedback iv

CHAPTER 1

Getting Started 1-1

- Overview 1-1
- System Architecture 1-4
- List of Acronyms and Abbreviations 1-6
- System Requirements 1-7
- Supported Software/Hardware 1-11
- Deployment Model 1-11
 - Non-cluster Server Setup 1-11

1-13

CHAPTER 2

Installing the Smart+Connected Spaces 2-1

- Prerequisites 2-1
 - Gathering Required Information 2-1
 - Verifying Network Configurations 2-3
- Installing the Smart+Connected Spaces Application 2-3
 - Accessing the Application and Verifying the Installation 2-6
 - Accessing the Web Calendar 2-6
 - Accessing the Kiosk Web Portal 2-7
 - Accessing the Personalized Spaces Portal 2-7

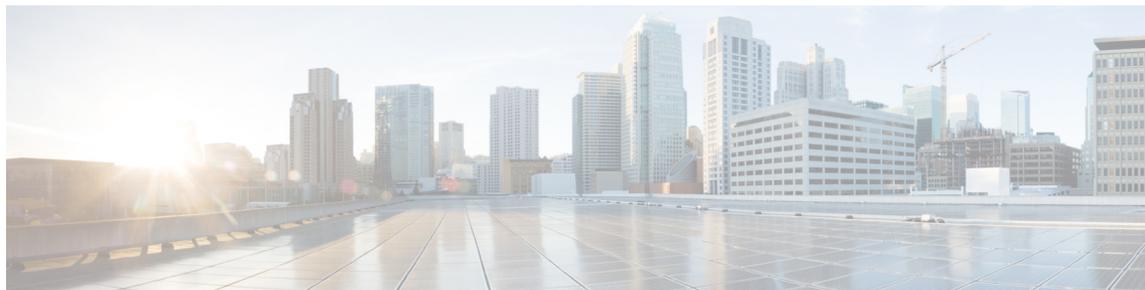
CHAPTER 3

Configuring the Smart+Connected Spaces 3-1

- Configuring Services in CUCM 3-1
- Assigning Roles (Groups) to the Application User 3-2
- Managing Users 3-3
 - Users 3-3
 - Creating and Configuring Users 3-4

Send documentation comments to scc-docfeedback@cisco.com

- Importing Multiple Users 3-5
- Viewing User Details 3-6
- Editing User Details 3-7
- Exporting User Details 3-8
- Deleting Users 3-9
- Configuring Audio Notification to IP Phone 3-9
- Configuring Locations 3-10
 - Adding Locations 3-10
 - Editing Locations 3-13
 - Deleting Locations 3-13
- Configuring Devices 3-14
 - Adding Devices 3-14
 - Deleting Devices 3-22
 - Setting up Crestron Controller for the Projector 3-23
- Configuring Room Types 3-23
- Configuring Adapters 3-24
 - Adapter Description 3-24
 - Configuring Adapter Properties 3-25
 - Configuring Adapters to a Location 3-33
 - Sample Adapter Configurations 3-34
- Setting up Data Collection 3-35
- Integrating CUCM and InformaCast 3-36
- Integrating Jabber with Smart+Connected Spaces 3-36
- Importing SSL Certificates 3-37
- Changing the JBoss Port 3-37
- Configuring the Property Files 3-38
 - Configuring the Property Files for Non-Clustered Setup 3-38
- Changing the Theme of the Room Booking Portal 3-48
- Customizing the Branding Images of the Workspaces Portal 3-48



Preface

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

- [Audience, page iii](#)
- [Organization, page iii](#)
- [Document Conventions, page iv](#)
- [Related Documentation, page iv](#)
- [Documentation Feedback, page iv](#)

Audience

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

Organization

| Title | Description |
|---|---|
| Chapter 1, “Getting Started” | Describes information on the architecture, prerequisites, and deployment models of the Smart+Connected Spaces application. |
| Chapter 2, “Installing the Smart+Connected Spaces” | Describes how to install and deploy the Smart+Connected Spaces application by using the Postgres database and the JBoss application server. |
| Chapter 3, “Configuring the Smart+Connected Spaces” | Describes how to configure the Smart+Connected Spaces application after installation. |

Document Conventions

| Convention | Indication |
|---------------------------|---|
| Boldface | Commands, command options, and keywords are in boldface. |
| <i>Italics</i> | Arguments for which you supply values are in italics. |
| Option > Option | Used to describe a series of menu options. |
| <code>courier font</code> | Terminal sessions and information the system displays appear in courier font. |



Note

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

Related Documentation

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

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to scc-docfeedback@cisco.com. We appreciate your feedback.



Getting Started

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

- [Overview, page 1-1](#)
- [System Architecture, page 1-4](#)
- [List of Acronyms and Abbreviations, page 1-6](#)
- [System Requirements, page 1-7](#)
- [Deployment Model, page 1-11](#)

Overview

The Smart+Connected Spaces is a solution that leverages the Cisco Service Delivery Platform (SDP). The solution allows you to easily access information about conference/TelePresence (TP) rooms, workspaces, people, and the enterprise by using digital signage/IEC, kiosks, room panels, IP phones, smartphones, Smart Spaces Outlook Plug-in, and the web portals. For example, you can easily view information, such as meeting details, room and workspace availability, people who have checked into workspaces, news, energy consumption data, energy saving tips, and so on.

The solution also allows you to book conference or TP rooms and check into workspaces instantly using touchscreen signage, kiosks, room panels, IP phones, and smartphones, manage conference room resources, and report the issues, if any, in the conference rooms. The automatic energy saving settings lead to reduced power consumption and contribute to the eco-friendly policies of the organization. In case of any mishaps, emergency notifications are sent out to the users through IP phones and signage.

The Smart+Connected Spaces leads to enhanced enterprise communication as the updated meeting room, and workspace occupancy information is widely available and easily accessible to employees. It also leads to better resource management and energy savings which translate to reduced energy bills and more environment-friendly corporate practices.

The Smart+Connected Spaces application allows the end user to access the following features/solutions:

- Using kiosks
 - Book conference rooms and TP rooms.
 - Check into any available workspace.
 - View the availability and check-in status of your Jabber contacts.
 - View the route to locate a workspace, office, or conference/TP room on a floor.

Send documentation comments to scc-docfeedback@cisco.com

- View the overall conference/TP room and workspace availability on all of the floors of all of the buildings in the organization and book/check into any of these spaces.
- View the neighborhoods/zones on a floor.
- View the building, floor, and name of the workspace or office that you have checked into.
- Access the floor plans for any building in the enterprise to view the locations and availability of the conference room/TP rooms and workspaces.
- Search for the available conference rooms and TP rooms based on your requirements such as the features available, seating capacity, location, and time and book them.
- Search for the people within the enterprise.



Note You can also perform all these tasks by using the web portal.

- Reset the PIN by using the Forgot PIN option. The new PIN will be sent on your email ID and get updated in the kiosk web portal.
- Using the kiosk web portal (In addition to the above mentioned features that you can access using kiosks)
 - Locate the workspace you have checked into.
 - View the building, floor, and name of the workspace you have checked into.
 - Choose not to display your current check in location.



Note This option is available only if it is configured by the administrator.

- Change the kiosk PIN that you use for authentication while checking in, booking rooms, and viewing the list of your Jabber contacts.
- Check out from the workspace that you have occupied.
- Login and logout of the kiosk web portal.
- Using the mobile phone application
 - View your upcoming meeting and workspace reservation details.
 - Check into and checking out of a reserved workspace using your mobile device.
 - Search for the required conference/TP room.
 - View the availability status of all of the rooms on any floor in any building within the enterprise.
 - Book conference/TP rooms using your mobile device based on your requirements such as the features available, seating capacity, location, and time.
 - Invite people in your enterprise to participate in meetings (during the room booking process).
 - Ad-Hoc checking in from the list of available workspaces and checking out using the QR code scanning feature.
 - Mark workspaces and people within an enterprise as favorites.
 - Set your preferences for building and floor.
 - Search for people within the enterprise.
 - Initiate either a call or sending text messages and emails using the mobile device.
- Using IP phones

Send documentation comments to scc-docfeedback@cisco.com

- Quickly book the conference room wherever the IP phone is located based on the room availability.
- Control the meeting room devices and equipment.
- Save energy by manually releasing a room for the duration that it is unoccupied, in addition to the energy savings made when the solution automatically switches off devices.
- Configure multiple devices to suit your meeting and presentation needs using a single menu option.
- Create a case to notify the facilities team of any issues/problems that might be present in the conference room, and convey the same to the others in the organization by sending messages to the Cisco IP phone in the conference room. Once the case is created, the facilities team of the building can try to resolve the fault.
- Send preconfigured messages and emergency notifications to signages.
- Using the Smart+Connected Spaces user portals for room booking (calendar) and workspaces (ipsapp)
 - Search for the available conference/TP rooms based on your requirements such as room setup, room size, location, and so on and book them. Rooms that closely meet your search criteria are displayed if no exact match is found.
 - Search for the available workspaces based on your requirements such as date, time, location, workspace type and so on and reserve them.
 - View the current and upcoming meetings that you are part of or have organized.
 - View the current and upcoming workspace bookings
 - Accept, decline, or tentatively accept meeting invites.
 - View all the scheduled meetings as a day, week, or month based calendar view.
 - Book conference rooms easily by holding down the mouse key and dragging across the required time slot in the calendar view.
 - Book conference rooms instantly using the Quick Booking option. Reservation is made simpler as you can key in the number of participants. Booking duration options range from 30 (the default duration) to 60 minutes. Location is by default the one specified in your Preferences.
 - Book the room on behalf of other users by using the Proxy Booking option. For example, an executive administrator can book a workspace for a visiting executive.
 - Use the detailed booking option where you can request for change in the room setup, book equipment, add meeting agenda, and so on.
 - Edit the details of and reschedule the meetings that you have organized.
 - Save drafts of the bookings and edit them later.
 - Personalize your workspace by setting preference for lights, blinds, dimmers, air conditioner, and digital signage. You can activate the personalized settings when you check into a workspace.
 - Check in and check out of a reserved workspace.
 - Manage configurations for all the devices located at a workspace.
 - Generate and view reports for usage trends, user statistics, and so on.
 - Save your preferred settings such as favorite rooms, location, and time zone.
 - Create messages for the various fault cases, such as a non-functioning air conditioner in the workspace or faulty projector in a conference room.

Send documentation comments to scc-docfeedback@cisco.com

- Using room panels
 - View the conference/TelePresence room schedule and availability/occupancy status.
 - Book conference/TelePresence rooms.
 - Confirm conference/TelePresence room occupancy.
 - Release conference/TelePresence rooms.
- Using digital signage/IEC
 - Book conference/TP rooms.
 - View detailed floor plans with the locations of the conference rooms.
 - View the conference room schedule in different views—Building level, Floor level, and Conference Room level.
 - Cisco Smart+Connected Emergency Notifications™ (Smart+Connected EN)—Displays the notifications and exit routes on the digital signage in times of an emergency and sends audio and visual notifications on the Cisco IP phones during a crisis.
 - Cisco Smart+Connected Information Signage™ (Smart+Connected IS)—Displays the general information and news on the digital signage.
 - Cisco Smart+Connected Green Advisor™ (Smart+Connected GA)—Displays energy consumption data, energy saving tips, and green information.
- Using Smart Spaces Outlook Plug-in
 - Schedule a meeting and reserve resources, such as conference rooms with A/V Control, Digital Signage, TelePresence, and WebEx for face-to-face or online meetings.
 - View the organizer, attendee, and room availability status.
 - View the current and upcoming meetings that you are part of or have organized.
 - Accept, decline, or tentatively accept meeting invites.
 - Set your preferred meeting location.

In addition, the solution can help in energy savings by automatically switching devices to a standby mode when the meeting room is unoccupied and based on the configuration, turn them back on before the actual occupancy.

As an administrator, you have to manage the overall configuration, maintenance, and content creation for the Smart+Connected Spaces solution through a web portal. You have to add locations and devices, create users, and associate devices to locations for the solution in the SDP. For more information on performing these tasks, see the *Cisco Service Delivery Platform User Guide* and *Cisco Service Delivery Platform Installation Guide*. After the locations are added, and the devices are associated to them in the SDP, they are available in the Smart+Connected Spaces portal. You can select a location and associate a configuration to it. The features such as fault messages, device control options, signage menu messaging, and room booking that are added to the configuration can be accessed by the end user from the Cisco IP phones at the location.

System Architecture

The Smart+Connected Spaces solution communicates with the following:

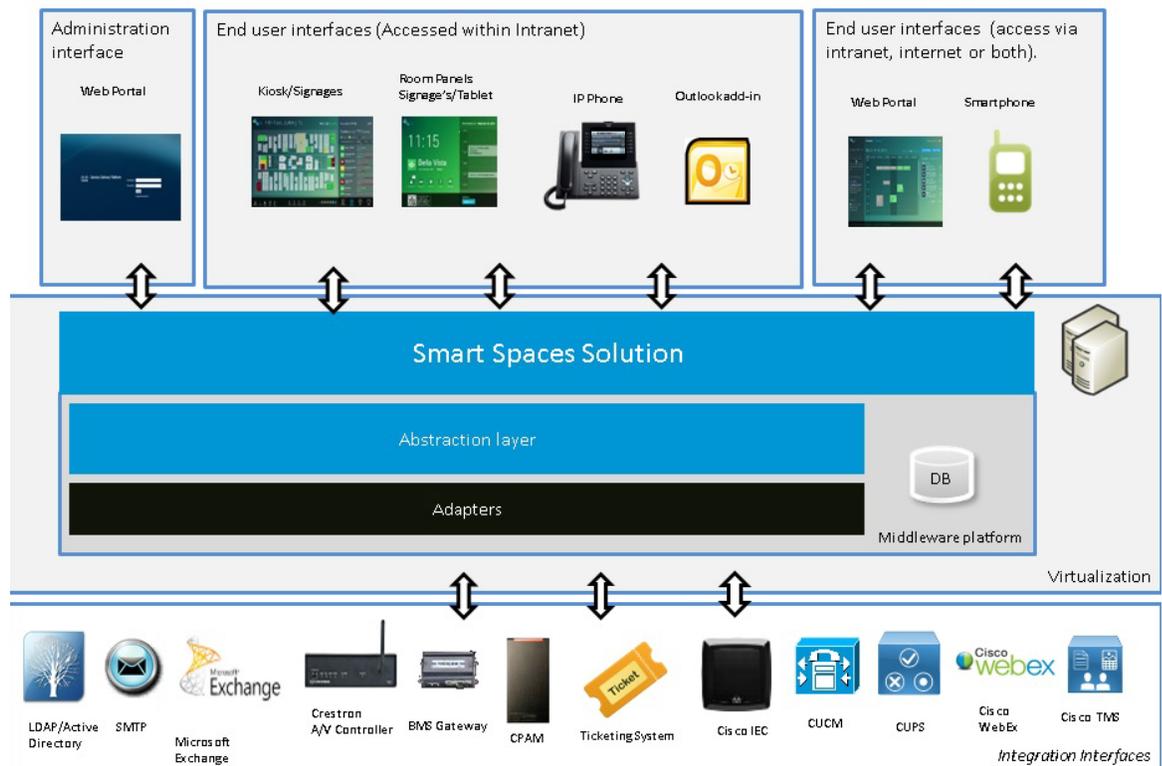
- Microsoft Exchange—To book meetings and retrieve meeting details.
- Building Management System (BMS)—To control and monitor devices, such as lights, blinds, and air conditioners.

Send documentation comments to scc-docfeedback@cisco.com

- Content Management System (CMS)—To store the application data.
- Crestron Controller—To control projectors and projector screens.
- Digital Media Player (DMP) and Cisco Interactive Experience Client (IEC)—To display meeting details, notifications, general information, news, energy consumption data, energy saving tips, and so on, on the signages.
- Remedy—To raise trouble tickets for the conference room issues.
- Cisco Jabber—To fetch the list of your contacts who are checked into a workspace or office.
- Cisco TelePresence Management Suite—To book TP meetings and retrieve the TP meeting details.
- Call Manager—For Cisco IP Phone interface integration with Smart+Connected Spaces.
- Cisco Physical Access Manager (CPAM)—To fetch user IDs and verify the check-in by users.

The Smart+Connected Spaces solution leverages the SDP. For more information on the SDP, see the *Cisco Service Delivery Platform User Guide*.

Figure 1-1 Smart+Connected Spaces– System Architecture



Send documentation comments to scc-docfeedback@cisco.com

List of Acronyms and Abbreviations

Table 1-1 List of Acronyms and Abbreviations

| Acronym | Expansion |
|----------------|--|
| ALC | Automated Logic Corporation |
| APR | Acoustic Pulse Recognition |
| BIRT | Business Intelligence and Reporting Tools |
| BMS | Building Management Systems |
| CMS | Content Management System |
| CPAM | Cisco Physical Access Manager |
| CPU | Central Processing Unit |
| CTI | Computer Telephony Integration |
| CUCM | Cisco Unified Communications Manager |
| DB | Database |
| DBMS | Database Management System |
| DMP | Digital Media Player |
| DMM | Digital Media Manager |
| DNS | Domain Name System |
| EWS | Exchange Web Services |
| EM | Extension Mobility |
| HDD | Hard Disk Drive |
| HTTP | Hypertext Transfer Protocol |
| IEC | Cisco Interactive Experience Client |
| IEM | Cisco Interactive Experience Manager |
| IEP | Cisco Interactive Experience Platform |
| JDBC | Java Database Connectivity |
| JDK | Java Development Kit |
| JMS | Java Message Service |
| JNDI | Java Naming and Directory Interface |
| JTAPI | Java Telephony Application Programming Interface |
| JVM | Java Virtual Machine |
| LAN | Local Area Network |
| LDAP | Light Weight Directory Access Protocol |
| MAC | Media Access Control |
| NBM | Cisco Network Building Mediator |
| MS | Meeting Spaces |

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

Table 1-1 *List of Acronyms and Abbreviations (continued)*

| Acronym | Expansion |
|---------|--|
| NIC | Network Interface Card |
| NTP | Network Time Protocol |
| OS | Operating System |
| PS | Personalized Spaces |
| 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 | Service Delivery Platform |
| SNMP | Simple Network Management Protocol |
| SP | Service Pack |
| SQL | Structured Query Language |
| TMS | Cisco TelePresence Management Suite |
| TP | Cisco TelePresence |
| UCS | Unified Computing System |
| UI | User Interface |
| vCPU | Virtual CPU |
| VM | Virtual Machine |

System Requirements

Before installing the Smart+Connected Spaces solution, ensure that all of the following system requirements are met.

Table 1-2 *System Requirements*

| Software/Hardware | Smart+Connected Spaces |
|-------------------------|--|
| Operating System | Red Hat Enterprise Linux (RHEL) 6.3 (64-bit) |
| Mobile Operating System | <ul style="list-style-type: none"> • iOS Version 6.x • Android <ul style="list-style-type: none"> – Jelly Bean 4.x.x – KitKat 4.x |

Send documentation comments to scc-docfeedback@cisco.com

Table 1-2 System Requirements (continued)

| Software/Hardware | Smart+Connected Spaces |
|---|--|
| Hardware - For Application Server and Database Note: <ul style="list-style-type: none"> • This requirement is for one VM (for example, collocated) or one physical machine. • For a non-cluster setup, you need two VMs—one for the application server and another for the database. Also, each VM must meet the requirements that are mentioned here. | Minimum requirements are: <ul style="list-style-type: none"> • Hard Disc Space—200 GB • RAM—Minimum configuration of 4 GB or above • Processor <ul style="list-style-type: none"> – 2 vCPU dual core for Virtual Machine (VM) – Intel x86/i386 Architecture for physical machines – Certified on Cisco UCS B-Series and C-Series with Intel CPUs. |
| Crestron A/V integration (if applicable) | <ul style="list-style-type: none"> • Separate host or VM with Windows 2008 R2 Standard SP1 or Windows 7 • IIS 7.5 with .NET framework 3.5 or higher |
| Browser | <ul style="list-style-type: none"> • Google Chrome Version 31 • Internet Explorer 10 • Mozilla Firefox Version 25 |
| Database | PostgreSQL 9.0 with character set configured to UTF8. For more information on how to install the PostgreSQL database, see the PostgreSQL documentation. |
| Application Server | JBoss EAP 6.2 |
| Java Development Kit (JDK) | Oracle JDK 1.6.0_24 |

Send documentation comments to scc-docfeedback@cisco.com

Table 1-2 System Requirements (continued)

| Software/Hardware | Smart+Connected Spaces |
|------------------------------|--|
| Exchange Server | <ul style="list-style-type: none"> • Microsoft Exchange Server 2007 SP3 • Microsoft Exchange Server 2010 SP1, SP2 • Microsoft Exchange Server 2013 CU3 <p>Exchange Web Services (EWS) integration is supported using only the BasicAuth authentication scheme. This needs to be configured in the Microsoft Internet Information Services.</p> <ul style="list-style-type: none"> • For conference room mailboxes, the ‘AutomateProcessing’ property must be set to ‘AutoAccept’ so that recurring meeting updates are sent correctly to the solution through notifications. • For user mailboxes, ‘AddOrganizerToSubject’ and ‘DeleteSubject’ must be set to \$false. If this is not done, then the meeting organizer’s name appears in the Subject field instead of meeting subject. <p>Impersonation rights are required on the conference room mailboxes and user mailboxes for the service account. This allows the service account to connect to the Exchange server and retrieve meeting details from the conference room mailboxes and the user mailboxes.</p> <p>For more information on Exchange impersonation, see:</p> <ul style="list-style-type: none"> • Exchange 2007: http://msdn.microsoft.com/en-us/library/bb204095(v=exchg.80).aspx • Exchange 2010: http://msdn.microsoft.com/en-us/library/bb204095.aspx • Exchange 2013: http://technet.microsoft.com/en-us/library/dd776119%28v=exchg.150%29.aspx |
| Smart Spaces Outlook Plug-in | <ul style="list-style-type: none"> • Microsoft .NET Framework 4.5 • Microsoft Visual Studio 2010 tools for office Runtime (x64) |
| Trouble Ticketing | BMC Remedy Version 7.5 |
| Audio/Visual | <p>The certified Crestron controllers that have been tested with the .NET SDK are:</p> <ul style="list-style-type: none"> • MC2E (one controller for one projector) • PRO2 (one controller for two projectors) <p>However, the Crestron Control System with Ethernet port supports the Crestron .NET SDK, and therefore can be integrated with the solution.</p> |
| Mediation Gateway | Tridium with Obix Versions 3.5.34, 3.7.x |

Send documentation comments to scc-docfeedback@cisco.com

Table 1-2 System Requirements (continued)

| Software/Hardware | Smart+Connected Spaces |
|--|---|
| Cisco Interactive Experience Client (IEC) | IEP-4610-HW-K9 and 4632-HW-K9 Firmware 4.243.497 |
| Cisco Interactive Experience Manager (IEM) | Version 2.0.0 |
| Digital Signage | Ensure that the aspect ratio of the signage screens is 16:9 (Resolutions: 1920 x 1080 and 1366 x 768). |
| Touchscreen | The Smart+Connected Spaces application is certified on the eLO Touchscreen APR technology model. For information about the touchscreen models supported for IEC, see: http://www.cisco.com/c/en/us/products/video/interactive-experience-clients/datasheet-listing.html |
| Cisco IP Phone Models | <ul style="list-style-type: none"> • Touchscreen: 7975 and 9971 • Non-Touchscreen: 8945 and 9951 |
| Call Manager | Cisco Call Manager Version 9.x |
| Emergency Notification System | Cisco JTAPI |
| Directory Services | <ul style="list-style-type: none"> • Active Directory <ul style="list-style-type: none"> – Windows 2008 Version 6.0 – Windows 2003 Version 5.2 R2 |
| Cisco TelePresence Management Suite | Cisco TMS 9.x |
| Service Delivery Platform (SDP) | Cisco SDP 2.0.2 |
| Language | U.S. English |

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

Supported Software/Hardware

Though the following software/hardware versions that are supported for the Smart+Connected Spaces 2.2 release even though they are not certified.

Table 1-3 *Supported Software/Hardware*

| Software/Hardware | Smart+Connected Spaces |
|--|---|
| Digital Media Manager (DMM) | Version 5.2.1 |
| Digital Media Player (DMP) | DMP 4400 Firmware 5.3 for https |
| Call Manager | <ul style="list-style-type: none"> • Cisco Call Manager Version 7.1 • Cisco Call Manager Version 8.x <p>The audio notification feature does not work with Cisco Call Manager 7.1.</p> |
| Emergency Notification via IP phones | Singlewire InformaCast 8.1.0 |
| Cisco Interactive Experience Manager (IEM) | 1.0.0 |

Deployment Model

You can install and deploy the Smart+Connected Spaces solution in the non-cluster server setup model.



Note

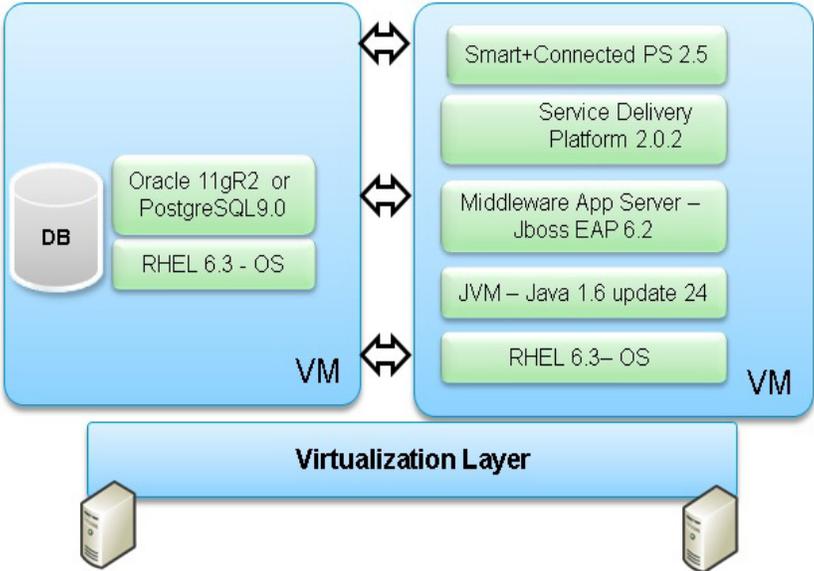
This document describes the installation process in a collocated/non-cluster setup.

Non-cluster Server Setup

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

Send documentation comments to scc-docfeedback@cisco.com

Figure 1-2 Non-Cluster Server Setup



Send documentation comments to scc-docfeedback@cisco.com

Send documentation comments to scc-docfeedback@cisco.com



Installing the Smart+Connected Spaces

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

- [Prerequisites, page 2-1](#)
- [Installing the Smart+Connected Spaces Application, page 2-3](#)

After successfully installing the Smart+Connected Spaces application, you can configure the application by performing tasks that are listed in [Chapter 3, “Configuring the Smart+Connected Spaces”](#).

Prerequisites

- [Gathering Required Information, page 2-1](#)
- [Verifying Network Configurations, page 2-3](#)
- [Installing the Smart+Connected Spaces Application, page 2-3](#)

Gathering Required Information

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

- Database details:
 - Database SID
 - Database IP address or the DNS hostname
 - Database port number. The default port number for PostgreSQL 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 application server is installed. Ensure that the `$JBOSS_HOME` environment variable is set to the `<JBOSS_INSTALL_LOCATION>` directory.

Send documentation comments to 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` folder.
- SSH credentials
- SDP Server details:
 - SDP Server IP Address
 - SDP Naming Service Port
 - SDP Server Console User
 - SDP Server Console Password
- LDAP details:
 - LDAP Server
 - LDAP Port
 - LDAP User Base
 - LDAP Search String
 - LDAP Connection User
 - LDAP Connection Password
- SMTP details:
 - SMTP Host
 - SMTP Port
 - System Admin Mail Address
 - Admin Email ID
 - From Email ID
 - Reply To Email ID
 - To Email ID
- WebEx details:
 - WebEx Site ID
 - WebEx Site Name
 - WebEx Partner ID
 - WebEx XML Server URL
 - WebEx Admin User
 - WebEx Admin Password
 - WebEx User
 - WebEx Password
 - WebEx Timezone
- Presence server details:
 - Presence Server IP
 - Presence Server Domain

Send documentation comments to scc-docfeedback@cisco.com

- Presence Server Port

Verifying Network Configurations

Verify the following network configuration:

- All machines in the setup are in the same network domain.
- All the machines are in the same LAN.
- All machines are configured to be on the same locale.
- System time is synchronized on all the machines using Network Time Protocol (NTP).
- All the interface components within the application are accessible over the network.

Installing the Smart+Connected Spaces Application

Before you run the installer, ensure that all of the conditions listed in the “Prerequisites” section on page 2-1 are met and you have the required information.

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

-
- Step 1** Copy the installer `CiscoSmartSpacesv2.5.<BuildNumber>.bin` to any preferred location in the application server.
- The installer can be obtained from the product DVD.
- Step 2** Change the access mode for the installer using the following command:
- ```
chmod u+x CiscoSmartSpacesv2.5.<BuildNumber>.bin
```
- Replace `<BuildNumber>` with the actual build number that is a part of the name of the installer file.
- Step 3** Run the installer using the following command:
- ```
./CiscoSmartSpacesv2.5.<BuildNumber>.bin
```
- The `CiscoSmartSpaces_v2.5` Introduction screen appears.
- Step 4** Click **Next**.
- The License Agreement screen appears.
- Step 5** Select the **I accept the terms of the License Agreement** radio button, and click **Next**.
- The Choose Install Folder screen appears.
- Step 6** Click **Choose** to select the directory where you want the applications to be installed. Alternatively, you can manually enter the path.
- Step 7** (Optional) If you want to revert to the default directory, click **Restore Default Folder**.
- Step 8** Click **Next**.
- The JBoss Configuration screen appears.
- Step 9** Click **Choose** to select the directory where you have installed JBoss. Alternatively, you can enter the path manually.
- Step 10** (Optional) Click **Restore Default Folder** if you want to revert to the default directory.
- Step 11** Click **Next**.
- The Java Home screen appears.

Send documentation comments to scc-docfeedback@cisco.com

- Step 12** Click **Choose** to select the directory where you have installed Java. Alternatively, you can enter the path manually.
- Step 13** (Optional) Click **Restore Default Folder** if you want to revert to the default directory
- Step 14** Click **Next**.
The Pre-Installation Summary screen appears.
- Step 15** Click **Install**.
A progress bar appears indicating that the installation is in progress. After the installation is completed, the Configuration screen appears informing you that the application is successfully installed.
- Step 16** Click **Next** to begin the configurations.
The Smart Spaces DB details screen appears.
- Step 17** Enter the details for the server where you have installed the Smart+Connected Spaces database in the following fields:
- Database Server IP Address
 - Database Server Port
 - Database Name
 - Database User
 - Database Password
- Step 18** Click **Next**.
The DB Execution Log Verification dialog box appears. Verify the log file, and then click **OK** on the dialog box.
The JBoss Application Credentials screen appears.
- Step 19** Enter the following JBoss application user credentials:
- Application User
 - Application Password
-  **Note** The password must be alphanumeric with at least one special character.
-
- Step 20** Click **Next**.
The LDAP details for Smart Spaces screen appears.
- Step 21** Enter the following LDAP details:
- LDAP Server
 - LDAP Port
 - LDAP User Base
 - LDAP Search String
 - LDAP Bind Root
 - LDAP Connection User
 - LDAP Connection Password
 - LDAP SSL Enabled
- Step 22** Click **Next**.

Send documentation comments to scc-docfeedback@cisco.com

The SMTP details for Smart Spaces screen appears.

Step 23 Enter the following SMTP details:

- SMTP Host
- SMTP Port
- System Admin Email Address
- Admin Email ID
- From Email ID
- Reply To Email ID
- To Email ID

Step 24 Click **Next**.

The WebEx details screen appears.

Step 25 Enter the following WebEx details:

- WebEx Site ID
- WebEx Site Name
- WebEx Partner ID
- WebEx User
- WebEx Password

Step 26 Click **Next**.

The Presence Server details screen appears.

Step 27 Enter the following Presence server details:

- Presence Server IP
- Presence Server Domain
- Presence Server Port

Step 28 Click **Next**.

The API Access details screen appears.

Step 29 Enter the following API access details:

- Secure Username
- Secure Password

Step 30 Click **Next**.

A message appears informing you that the configuration is in progress. Once the configuration is completed, the Installation Complete dialog box appears informing you that the application is successfully installed.

Step 31 Click **Finish**.

You will now be able to access the application. For more information, see the [“Accessing the Application and Verifying the Installation”](#) section on page 2-6, [“Accessing the Web Calendar”](#) section on page 2-6, [“Accessing the Kiosk Web Portal”](#) section on page 2-7, and [“Accessing the Personalized Spaces Portal”](#) section on page 2-7.

Send documentation comments to scc-docfeedback@cisco.com

Accessing the Application and Verifying the Installation

To access the Smart+Connected Spaces application, perform the following steps:

-
- Step 1** In a web browser, type the URL `http://<host>:<port>/solutions/`, where:
- `<host>` is the host IP address or DNS hostname of the host on which the JBoss application server is set up.
 - `<port>` is the value that appears in the output after starting the JBoss server.

- Step 2** Press **Enter**.
- The Smart+Connected Spaces Login page appears.

- Step 3** Enter the username and password for the Smart+Connected Spaces 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 User Guide*.

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

Accessing the Web Calendar

After performing all installation tasks, you can access the Smart+Connected Spaces web calendar.

To access the Smart+Connected Spaces web calendar, perform the following steps:

-
- Step 1** In a web browser, type the URL `http://<host>:<port>/calendar/`, where:
- `<host>` is the host IP address or DNS hostname of the host on which the JBoss application server is set up
 - `<port>` is the value that appears in the output after starting the JBoss server.

- Step 2** Press **Enter**.
- The Smart+Connected Spaces Login page appears.

- Step 3** Enter the username and password for the Smart+Connected Spaces web calendar, and click **Login**.

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 User Guide*.

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

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

Accessing the Kiosk Web Portal

After performing all the installation tasks, you can access the Smart+Connected Spaces kiosk web portal.

To access the Smart+Connected Spaces kiosk web portal, perform the following steps:

-
- Step 1** In a web browser, type the URL `http://<host>:<port>/spaces/` where:
- `<host>` is the host IP address or DNS hostname of the host on which the JBoss application server is set up
 - `<port>` is the value that appears in the output after starting the JBoss server.
- Step 2** Press **Enter**.
- The Smart+Connected Spaces kiosk web portal login page appears.
- Step 3** Enter the username and password for the Smart+Connected Spaces kiosk web portal, and click **Login**.
- 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 User Guide*.
- For more information on how to use the Smart+Connected Spaces features, see the *Cisco Smart+Connected Spaces User Guide*.
-

Accessing the Personalized Spaces Portal

After performing all the installation tasks, you can access the Smart+Connected Personalized Spaces web portal.

To access the Smart+Connected Personalized Spaces web portal, perform the following steps:

In a web browser, type the URL `http://<host>:<port>/ipsapp` where

- `<host>` is the host IP address or DNS hostname of the host on which the JBoss application server is set up.
 - `<port>` is the value that appears in the output after starting the JBoss server.
- Step 4** Press **Enter**.
- The Smart+Connected Personalized Spaces web portal login page appears.
- Step 5** Enter the username and password for the Smart+Connected Spaces kiosk web portal, and click **Login**.
- 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 User Guide*.
- For more information on how to use the Smart+Connected Personalized Spaces features, see the *Cisco Smart+Connected Spaces User Guide*.
-

Send documentation comments to scc-docfeedback@cisco.com



Configuring the Smart+Connected Spaces

This chapter describes the configuration tasks that you need to perform after installing the Cisco Smart+Connected Spaces (Smart+Connected Spaces) application.

- [Configuring Services in CUCM, page 3-1](#)
- [Assigning Roles \(Groups\) to the Application User, page 3-2](#)
- [Managing Users, page 3-3](#)
- [Configuring Audio Notification to IP Phone, page 3-9](#)
- [Configuring Locations, page 3-10](#)
- [Configuring Devices, page 3-14](#)
- [Configuring Room Types, page 3-23](#)
- [Configuring Adapters, page 3-24](#)
- [Setting up Data Collection, page 3-35](#)
- [Integrating CUCM and InformaCast, page 3-36](#)
- [Integrating Jabber with Smart+Connected Spaces, page 3-36](#)
- [Importing SSL Certificates, page 3-37](#)
- [Changing the JBoss Port, page 3-37](#)
- [Configuring the Property Files, page 3-38](#)
- [Changing the Theme of the Room Booking Portal, page 3-48](#)
- [Customizing the Branding Images of the Workspaces Portal, page 3-48](#)

Configuring Services in CUCM

The Cisco Unified Communications Manager (CUCM) administrator must configure the service URL in CUCM to make the service appear on the IP phone.

To configure the services in CUCM, perform the following steps:

-
- Step 1** In the browser, type the CUCM URL.
 - Step 2** Click **Cisco Unified Communications Manager**.
The Cisco Unified CM Administration home page appears.
 - Step 3** Enter the CUCM administrator's username and password, and click **Login**.

Send documentation comments to scc-docfeedback@cisco.com

Step 4 Click **Device > Device Settings > Phone Services**.

Step 5 Click **Add New**.

To add a new service, perform the following steps:

- a. Enter the service name in the Service Name field, For example, S+CC service.
- b. Enter the service description in the Service Description field.
- c. Enter the service URL in the format given below:

```
http://<host IP address>:<port>/solutions/ip-phone-comm.ip
```
- 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** check box.

Step 6 Click **Save**.

Step 7 Click **Device > Phone**.

The Find and List Phones page appears

Step 8 From the “Find Phone where” drop-down list, choose **Device Name**.

Step 9 From the drop-down list that is adjacent to the “Find Phone where” drop-down list, choose contains.

Step 10 Enter the MAC address of the IP phone for which you want to subscribe the service.

Step 11 Click **Find**, and select the IP phone.

The Phone Configuration page appears.

**Note**

Ensure that the Web Access drop-down list displays an enabled value.

Step 12 From the Related Links drop-down list, choose **Subscribe/Unsubscribe Services**, and click **Go**.

Step 13 Select the service name that you have provided in Step 5 a.

Step 14 Click **Next**.

Step 15 Click **Subscribe**.

Step 16 Click **Reset** in the Phone Configuration page.

A device reset dialog box appears.

Step 17 Click **Reset**.

Step 18 The configured service name appears under Services in the IP Phone

Assigning Roles (Groups) to the Application User

The Smart+Connected Spaces application requires an application user to be created in CUCM for pushing the audio broadcast and text messages to the Cisco IP phone.

The application user needs the following privileges minimally to allow the Smart+Connected MS application 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.

Send documentation comments to scc-docfeedback@cisco.com

- 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 the configuration information 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 following 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** Click **User Management > Application User**.
The Find and List Application Users page appears.
- Step 5** Click **Add New**.
The Application User Configuration page appears. Create the application user and assign the required roles that provide the user the above mentioned privileges.
-

Managing Users

Users

Users access the Smart+Connected Spaces to perform various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user is associated with one or more roles and each role is assigned a certain set of permissions. These roles and permissions define the tasks that a user can perform in the Smart+Connected Spaces. You can additionally assign one or more locations to each role so that the user can perform tasks at the assigned locations only.

When you install the Smart+Connected Spaces, a superadmin user (super administrator) is created by default. The superadmin user has permissions across all features and tasks.

The superadmin creates other users by adding them to the Smart+Connected Spaces application and by assigning roles and permissions to them. The other users can log in to the Smart+Connected Spaces and perform tasks based on the roles and permissions that are assigned. For information on how to add users and assign roles and permissions to them, see the [“Creating and Configuring Users” section on page 3-4](#).

All user details (such as username, first name, last name, title, email address, company, designation, and password details) are stored in the Smart+Connected Spaces database.

The Smart+Connected Spaces provides you with the following options to add users to the application database:

Send documentation comments to scc-docfeedback@cisco.com

- Creating users by manually adding details for each user.
- Importing multiple users by retrieving user details from a file (ifcXML).

After adding user details to the Smart+Connected Spaces, you can perform the following tasks:

- Assign roles and locations.

Export user details to an ifcXML file to use in other applications, if required.

Creating and Configuring Users

You can manually add user details for each user or import multiple user details from either the LDAP directory or a file (ifcXML).

To import multiple user details from the LDAP directory or a file, see [“Importing Multiple Users” section on page 3-5](#).

To add user details for each user, perform the following steps:

Step 1 Log in to the SDP application.

Step 2 Choose **Users and Roles > Create a User**.

The Create User page appears.

Step 3 Enter the following user details:

- In the Username text box, enter a unique username. The name cannot include blank spaces, can include special characters, can be alphanumeric, and contain up to 50 characters.
- In the First Name text box, enter the first name of the user.
- In the Last Name text box, enter the last name of the user.
- In the Email text box, enter the email address of the user.
- In the Title text box, enter the designation of the user.
- In the Company text box, enter the company name of the user.
- In the Password and Confirm Password text boxes, enter the user password. The password contains characters from at least three of the four character groups that are uppercase (A-Z), lowercase (a-z), number (0-9), and all special characters.

The Password and Confirm Password text boxes are displayed if you have configured the LDAP directory in a writable mode.

Alternatively, enter the username and click **Find** to fetch the user details from LDAP.



Note

- Check the **User Authentication from LDAP** check box to authenticate the user from LDAP.
- The user must be configured in LDAP and the SDP must be able to communicate with LDAP.

Step 4 In the Assign Roles and Locations area, click **Assign New Role**.

The Select Roles for the Users dialog box appears. The Available Roles column lists the roles that have been added to the Smart+Connected Spaces and are in an active state.

Step 5 In the Available Roles column, select a role, and click **Add** to move the role to the Selected Roles column.

To add multiple roles, press **Shift - Ctrl**, choose the roles, and click **Add**.

Send documentation comments to scc-docfeedback@cisco.com

To remove the selected role from the Selected Roles column, click **Remove**.



Note For the Smart+Connected Spaces user, the roles (superadmin, scpsuser, or proxyuser) must be assigned.

Step 6 Click **Assign and Close**.

The selected role is assigned to the added user along with the associated permissions and locations

Step 7 In the Assigned Locations column of the Assign Roles and Locations area, click **Assign Locations** next to the role to which you want to assign the location.

The Assign Locations dialog box appears with a location hierarchy. The location hierarchy lists the locations for which you have been assigned permissions.



Note If the user is not associated with any location or a location has not been added to the application, the location hierarchy is not displayed.

Step 8 In the location hierarchy, select a location that you want to associate to the role.

You can use shortcut tools to search and select a location in the location hierarchy. For more information on the shortcut tools, see [“Configuring Locations” section on page 3-10](#).

Step 9 Click **Assign**.

The selected location is assigned to the specified role.

Step 10 Click **Save**.

The user details are saved, and are listed in the List of Users area.

Importing Multiple Users

You can add multiple users to the Smart+Connected Spaces by importing the following user details from an ifcXML2x4:

- Username
- First and last name
- Email address
- Title
- Job description

User details are invalid if the username, or the first and last name of the user are not specified in the file. These user details are not imported during the import process. However, the import process continues for the remaining user details.

To import multiple users from an ifcXML2x4 file, perform the following steps:

Step 1 Log in to the SDP application.

Step 2 Click the **Users and Roles** tab.

Send documentation comments to scc-docfeedback@cisco.com

The Users page appears. The List of Users area displays the users that have been added in to the Smart+Connected Spaces.

Step 3 Click **Import Users** button to launch the import Users Wizard.

The Specify Source screen appears.

Step 4 In the XML file text box, browse for and select the file that contains the user details that you want to import.

Step 5 In the Import Options area, select one of the following radio buttons:

- **Overwrite these records**—Select if you want to overwrite the existing user details with the new details.

The other user details for which the data is not available in the file are not overwritten or deleted.

- **Skip these records**—Select if you do not want to overwrite the existing user details.

The new user details are added to the Smart+Connected Spaces.

Step 6 Click **Import**.

The Completed Import screen appears with information on the imported (updated or skipped) user details and error logs if an error occurs during the process.

Step 7 Click **Finish** to complete the import process.

Viewing User Details

After the users are imported from the file, the added user details are listed in the List of Users area of the Users page.

You can view detailed information about the existing users, such as username, email address, title, roles and locations that are assigned, and so on.

To view user details, perform the following steps:

Step 1 Log in to the SDP application.

Step 2 Click the **Users and Roles** tab.

The Users page appears. The List of Users area displays the users that have been added to the Smart+Connected Spaces.

Step 3 Search for a user based on the username, first name, or last name:

- a. In the User Name, First Name, or Last Name text box, type a keyword.
- b. Press **Enter**.

The List of Users area displays the following user details:

- User Name—Name of the user.
- First Name—First name of the user.
- Last Name—Last name of the user.
- Last Login—Last time when the user logged in to the Smart+Connected Spaces. The Last Login field is blank for the newly added users.
- Updated By—User who last updated the user details.

Send documentation comments to scc-docfeedback@cisco.com

- Updated On—Time at which the user details were last updated.

Step 4 To view detailed information about a user, click a username.

The View User page appears with the following detailed user information:

- User Name—Name of the user.
- First Name—First name of the user.
- Last Name—Last name of the user.
- Email—Email address of the user.
- Title—Designation of the user.
- Company—Company name of the user.
- Assigned Roles and Locations—Roles and locations that are assigned to the user.



Note If you have added any custom attributes to the application during the LDAP configuration, the specified user details are additionally listed in the View User page.

If you want to modify the existing user details, see the [“Editing User Details” section on page 3-7](#)

Editing User Details

After adding a user, you can modify the existing username, title, designation, assigned role, or associated location details.

To modify the existing user details, perform the following steps:

Step 1 Log in to the SDP application.

Step 2 Click the **Users and Roles** tab.

The Users page appears. The List of Users area displays the users that have been added to the Smart+Connected Spaces.

Step 3 In the User Name column, select the username check box of the user that you want to modify, and click .

Alternatively, click a username that you want to edit, and in the View User page, click  **Edit**.

The Edit User page appears.

Step 4 Modify the following details as necessary:

- In the Username text box, enter a unique username. The name cannot include blank spaces, can include special characters, can be alphanumeric, and contain up to 50 characters.
- In the First Name text box, enter the first name of the user.
- In the Last Name text box, enter the last name of the user.
- In the Email text box, enter the email address of the user.
- In the Title text box, enter the designation of the user.
- In the Company text box, enter the company name of the user.

Step 5 To assign new roles or unassign the associated roles, click **Assign New Role**.

Send documentation comments to scc-docfeedback@cisco.com

Step 6 To assign new locations or unassign the associated locations, click **View/Edit Locations**.

Step 7 Click **Save**.

The user details are modified, and are listed in the List of Users area. If you want to view the updated user details, see the “[Viewing User Details](#)” section on page 3-6.

Exporting User Details

You can export multiple user details from the Smart+Connected Spaces to an ifcXML2x4 file. When you export user details, a file is automatically stored in the local file system with the details. By exporting user details, you can quickly collate multiple user details from the Smart+Connected Spaces and use it in other applications, if required.

The following user details are exported from the Smart+Connected Spaces to the ifcXML2x4 file:

- Username
- First and last name
- Email address
- Title
- Job description

To export user details to an ifcXML2x4 file, perform the following steps:

Step 1 Log in to the SDP application.

Step 2 Click the **Users and Roles** tab.

The Users page appears. The List of Users area displays the users that have been added to the Smart+Connected Spaces.

Step 3 Do one of the following to launch the Export Users wizard:

- To export all users, click **Export All Users**.
- To export specific users, select the check boxes of the users that you want to export, and click **Export Selected**.
- To export a single user, choose the user that you want to export, and click .

The Export users from SDP screen appears.

Step 4 Click **Export**.

The Completed Export screen appears with a message stating that the user details are successfully exported from Smart+Connected Spaces. The ifcExport.xml file is automatically created with a list of user details.

Step 5 Save the exported file on your computer.

The Completed Export screen appears.

Click **Finish** to complete the exporting process.

Send documentation comments to scc-docfeedback@cisco.com

Deleting Users

You can delete users that you have added to the Smart+Connected Spaces.

To delete users, perform the following steps:

-
- Step 1** Log in to the SDP location.
- Step 2** Click the **Users and Roles** tab.
- The Users page appears. The List of Users area displays the users that have been added to the Smart+Connected Spaces.
- Step 3** In the User Name column, select the username check box of the user that you want to modify, and click .
- The Edit User page appears.
- Step 4** Under Assigned Roles, click a role and then click .
- Step 5** Repeat [Step 4](#) to remove all the roles that are assigned to the user.
- Step 6** Do one of the following:
- To delete a single user, choose a user that you want to delete, and click .
 - To delete multiple users, select the specific check boxes of the users that you want to delete, and click **Delete**.

The user details are deleted, and are not recoverable.



Note If you try to delete user(s) without removing the roles assigned to the user, you get an error message.

Configuring Audio Notification to IP Phone

The CUCM administrator needs to configure the audio notification feature to allow the Emergency Notification (EN) messages to be pushed to the IP phone.

To configure audio notification to IP phone, perform the following steps:

-
- Step 1** Create an application user in Call Manager so that the solution can push the Emergency Notification (EN) content to IP Phone.
- To create an application user in the Call Manager, perform the following steps:
- a. In a browser, type the CUCM URL.
 - b. Click **Cisco Unified Communications Manager**.
The Cisco Unified CM Administration home page appears.
 - c. Enter the CUCM administrator's username and password for the Call Manager, and click **Login**.
 - d. Navigate to **User Management > Application User**.
 - e. Click **Add New**.

Send documentation comments to scc-docfeedback@cisco.com

The Application User Configuration page appears.

- f. Enter the user ID in User ID field.
- g. Enter the password in the Password field.
- h. Enter the confirmed password in the Confirm Password field.
- i. From the BLF Presence Group drop-down list, choose Standard Presence group.
- j. In Device Information, move the desired devices from Available Devices to Controlled Devices.
- k. Move the desired Available Profiles to CTI Controlled Device Profiles.
- l. Under Permissions Information, click **Add to Access Control Group**.
- m. Check the **Standard CTI Enabled** checkbox in the Access Control Group list, and click **Add Selected**.
- n. Click **Save**.

The roles and permission for the new user appear.

- Step 2** For pushing audio to IP phone as part of EN, you have to make a change in the server on which the Smart+Connected Spaces application is deployed. Change the `/etc/hosts` file by moving the assigned IP address of the machine before the local loopback address.

For example,

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



Note The IP phones, application server, and CUCM must be on a multicast network. To verify if the application server is multi-cast run `/sbin/ifconfig` in the application server. The **MULTICAST** keyword appears in the output.

Configuring Locations

A location is a physical space that helps you define a spacial structure in a city, organization, complex, industry, and so on. For example, the various locations for an organization can be country, city, building, campus, wing, floor, room, and so on.

- [Adding Locations, page 3-10](#)
- [Editing Locations, page 3-13](#)
- [Deleting Locations, page 3-13](#)

Adding Locations

You can add multiple locations to the SDP application and create a location hierarchy for a city, an enterprise and so on. You can create location hierarchies beginning with the default root location that is defined during installation of the SDP application. You can also modify the name of the default root location, if required.

Send documentation comments to scc-docfeedback@cisco.com

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.

For certain location types, additional properties should be added.

Table 3-1 Location Type and Properties

| Location Type | Property | Value Description | Sample Data |
|---|-------------|---|-------------|
| Country, State, and City | Timezone | Timezone of the location. | Location1 |
| Building, Floor, Campus, Office, Quiet Room, Cubicle, and Telepresence Room | MessageId | The ID of an emergency notification message in InformaCast. | 1160 |
| | RecipientId | The ID of the group of recipients in InformaCast to which the emergency notification messages will be sent. | 9 |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-1 Location Type and Properties (continued)

| Location Type | Property | Value Description | Sample Data |
|---|---------------------------|--|---|
| Building and Floor | multicastipaddress | The IP address used to send the multicast message. | 224.0.1.43 |
| | multicastport | The port used to send the multicast message. | 31250 |
| Building | Latitude | Latitude of the building. | 10 |
| | Longitude | Longitude of the building. | 25 |
| | Address1 | Address of the building. | |
| | Address2 | Alternative address of the building. | |
| | Postal Zip Code | Pin code of the building. | 560001 |
| Campus | Room Facility Admin | Email ID of the room facility administrator or the distribution list that comprises the emails IDs of the facility team members. | campus_admingroup @ abcde.com |
| | Equipment Facility Admin | Email ID of the equipment facility administrator or the distribution list that comprises the emails IDs of the facility team members. | eqpmnt_administrator @ abcde.com |
| Floor | MaxAllowedBookingDuration | Duration in minutes for the maximum time for which a workspace can be booked. The default is 8 hours, | 480 |
| Conference Room, Telepresence Room, Office, Quiet Room, and Cubicle | Reservable | Whether the meeting room/workspace can be reserved. | Check/uncheck the Reservable check box. |
| Conference Room, and Telepresence Room | Room Size | The seating capacity of the room. | 15 |
| | Private Subject | If you enable this property, the subject displays 'Booked By <organizer name>' on the IP phone and signage instead of displaying the actual subject. | Yes |
| | Private Attendees | If you enable this property, the attendee list is not displayed on the signage. | Yes |
| | Floor Code | Not mandatory. | – |
| | Location Code | Not mandatory. | – |
| | Alias Name | The alias name of the conference room in exchange. | Room1 |
| | Email ID | The email ID of the conference room. | room1@abcde.com |
| Conference Room | confRoomId | The alias of the conference room ID in exchange. | Room1 |
| Telepresence Room | Telepresence Room Id | The alias of the Cisco TelePresence room ID in exchange. | TP Room1 |
| | sip URL | The Call set up using the Session Initiation Protocol (SIP) | 2930@abcde.com |

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

Editing Locations

After adding a location to the location hierarchy, you can modify the location name and location properties.

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:
- 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.
- For more information on how to select a location, perform [Step 1](#) through [Step 3](#) in [Adding Locations, page 3-10](#).
- 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.
- Step 4** Click **Save** to save the location details.
- The modified details are updated and displayed in the location hierarchy.
-

Deleting Locations

To delete a location, perform the following steps:

-
- Step 1** On the Locations page, select a location that you want to delete.
- 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.
- For more information on how to select a location, perform [Step 1](#) through [Step 3](#) in [Adding Locations, page 3-10](#).
- Step 2** In the right pane, click .

Send documentation comments to 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

You need to configure devices to avail the building system services for the location, such as, light settings, blinds, dimmer, and audio video controller through the Smart+Connected Spaces application. You need to use the SDP interface to access the Devices module.

The devices type definitions, such as, lights, blinds, dimmer, and audio video controller are available as part of SDP seed data that is added when SQL scripts are executed.

- [Adding Devices, page 3-14](#)
- [Deleting Devices, page 3-22](#)
- [Setting up Crestron Controller for the Projector, page 3-23](#)

Adding Devices

The following devices are supported by the Smart+Connected Spaces application:

- Cisco IP Phones
- Blinds
- Lights
- Audio Video Controller
- Dimmer
- Light Occupancy Sensor
- ThermoFuser
- VRV
- VAV
- Energy Meter
- Gas Meter
- Water Meter
- Digital Media Player (DMP)
- Cisco Interactive Experience Client (IEC)

You can add any of these devices to the selected location in the location hierarchy 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 3-2](#) lists the device properties of the devices that have been added by the Smart+Connected Spaces scripts.

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

Table 3-2 Device Properties and Values

| Device | Model | Device Property | Value Description | Sample Data |
|--------------|---|--|--|--|
| IP Phone | CP-7975G | MAC Address | MAC Address of the IP phone. | 0019305D73EF |
| | CP-9971 Non-Touch CP-9951 and CP-8945 | 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 username. | examd |
| | | Application_Password | The Call Manager application user password. | examd |
| Mobility | Model name | mobilityaddress | MAC address of the IP phone | SEP0021CCBA8B34 |
| Blinds | Generic | Open Value | Value to be set on open path to open the blinds. | 1 |
| | | Close Value | Value to be set on close path to close the blinds. | 0 |
| | | Stop Value | Value to be set on stop path to stop the blinds. | 2 |
| | | Open Path | Node path in the BMS gateway for opening the blinds. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conference_Room/Blinds/BO/Blind_Open_Close/ |
| | | Stop Path | Node path in the BMS gateway for stopping the blinds when the blinds are opening or closing. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conference_Room/Blinds/BO/Blind_Stop/ |
| | | Close Path | Node path in the BMS gateway for closing the blinds. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conference_Room/Blinds/BO/Blind_Open_Close/ |
| | Blinds Scene | Blinds URL | Node path in the BMS gateway for setting the blinds scenes. The scene may correspond to opening or closing the blinds. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conference_Room/Blinds/BO/Blind_Scene/ |
| Blinds Value | | Value to be set on blinds URL to open or close the blinds. | 0 | |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-2 Device Properties and Values (continued)

| Device | Model | Device Property | Value Description | Sample Data |
|------------------------|--------------------------|-----------------------------|---|--|
| Lights | Generic | On Value | Value to be set on On/Off URL to switch on the lights. | true |
| | | Off Value | Value to be set on On/Off URL to switch off the lights. | false |
| | | On/Off URL | Node path in the BMS gateway for switching On/Off the lights. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_HA/HallMark/BGL10/Floor_01/Conference_Room/Light_Switch/BO/Lights_ON_OFF/ |
| Audio Video Controller | Generic | Projector Screen Open Join | Join value to be sent to the Crestron Controller to bring down the projector screen. | 35 |
| | | Projector Screen Stop Join | Join value to be sent to the Crestron Controller to stop the projector screen while bringing down or moving up. | 36 |
| | | Projector Screen Close Join | Join value to be sent to the Crestron Controller to move up the projector screen. | 37 |
| | | Projector On Join | Join value to be sent to the Crestron Controller to switch on the projector. | 25 |
| | | Projector Off Join | Join value to be sent to the Crestron Controller to switch off the projector. | 26 |
| | | Signal Type | Crestron Controller signal type. Currently only digital is supported. | digital |
| | | Slot | Crestron Controller slot. | 1 |
| | | IP Address | IP address of the Crestron Controller. | 72.163.202.35 |
| | | Port | Port of the Crestron Controller. Default port is 41794. | 41794 |
| | | IP ID | IP ID of the Crestron Controller. | 3 |
| Dimmer | Generic | Min Value | Minimum luminosity value. | 0 |
| | | Max Value | Maximum luminosity value. | 100 |
| | | Dim URL | Node path in the BMS gateway for setting 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 | Dim 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/ |
| | | Dimmer Values | Scene value to be set on the BMS gateway. | 2 |

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

Table 3-2 **Device Properties and Values (continued)**

| Device | Model | Device Property | Value Description | Sample Data |
|------------------------|----------------|-------------------------|--|---|
| Light Occupancy Sensor | Generic Sensor | Sensor URL | Node path in the BMS gateway to enable or disable the sensor. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conference_Room/Light_Occ_Sensor/BV/OnOff_Status_Override/ |
| | | On Value | Value to be set on Sensor URL to switch on the sensor. | true |
| | | Off Value | Value to be set on Sensor URL to switch off the sensor. | false |
| | | Sensor Occupancy URL | Node path in the BMS gateway to sense the occupancy of the location. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_01/Conference_Room/Light_Occ_Sensor/BI/Occupancy_Status/ |
| | | Occupied Value | Value on the sensor whenever occupancy is detected. | true |
| | | Unoccupied Value | Value on the sensor whenever occupancy is idle for more than specified time. | false |
| ThermoFuser | Generic | Current Temperature URL | Node path in the BMS gateway for reading back the current temperature. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_SEC/HallMark/BGL10/Floor_01/Conference_Room/Thermofuser/nvoSpaceTemp/ |
| | | Booking Status URL | Node path in the BMS gateway to set the current booking status of the conference room. If booking status is set to booked value, occupancy status is automatically set to occupied mode. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_SEC/HallMark/BGL10/Floor_01/Conference_Room/Thermofuser/nviOccCmd/ |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-2 **Device Properties and Values (continued)**

| Device | Model | Device Property | Value Description | Sample Data |
|--------|-------|--------------------------|--|--|
| | | Room Temperature URL | Node path in the BMS gateway for reading back the current room temperature. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_SEC/HallMark/BGL10/Floor_01/Conference_Room/Thermofuser/nciSetPnts_UnOccCool/ |
| | | Temperature Offset URL | Node path in the BMS gateway for setting the offset temperature. When the offset URL is provided, the value provided by the end user, is treated as a difference from the default setpoint value. For example, when the default setpoint is set as 21 degrees and the user expectation is 20 degrees, the offset value of -1 is applied with the appropriate selection in the UI. The value set as Temperature Offset URL impacts the control setpoint, to be either increased or decreased from the preset setpoint, equal to the value set as the offset. The effective setpoint is used as the reference requirement to control the temperature needs. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_SEC/HallMark/BGL10/Floor_01/Conference_Room/Thermofuser/nviSetPtOffset/ |
| | | Temperature Setpoint URL | Node path in the BMS gateway for configuring and reading back the current setpoint temperature. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_SEC/HallMark/BGL10/Floor_01/Conference_Room/Thermofuser/nvoEffectSetPt/ |

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

Table 3-2 **Device Properties and Values (continued)**

| Device | Model | Device Property | Value Description | Sample Data |
|--------|---------|--------------------------|---|---|
| | | Occupied Value | Value to be set on occupancy status URL to move the device to occupied mode. | 0 |
| | | Unoccupied Value | Value to be set on occupancy status URL to move the device to unoccupied mode. | 1 |
| | | Standby Value | Value to be set on occupancy status URL to move the device to standby mode. | 2 |
| | | Min Temperature Value | Minimum temperature to which the room temperature can be set. | 18 |
| | | Max Temperature Value | Maximum value of the room temperature that can be set. | 28 |
| | | Temperature Unit | Unit of temperature. | C or F |
| | | Reserved Value | Value to be set on booking status URL for occupancy. | 1 |
| | | Unreserved Value | Value to be set on booking status URL for unoccupancy. | 0 |
| | | Occupancy Status URL | Node path in the BMS gateway for reading back the status for occupancy. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/Thermofuser/OccUnocc_Sts/ |
| | | Occupied Temperature URL | Node path in the BMS gateway for reading back the occupied setpoint values. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/Thermofuser/RoomTemp_OccSetpt/ |
| VRV | Generic | Current Temperature URL | Node path in the BMS gateway for reading back the current temperature. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/AV/RoomTemp_OccSetpt/ |
| | | Temperature Setpoint URL | 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/VRV/AV/SpaceTemp_Setpt/ |
| | | Min Temperature Value | Minimum temperature to which the room temperature can be set. | 18 |
| | | Max Temperature Value | Maximum temperature of the room temperature that can be set. | 28 |
| | | Temperature Unit | Unit of temperature. | C or F |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-2 Device Properties and Values (continued)

| Device | Model | Device Property | Value Description | Sample Data |
|--------------|---------|--------------------------|---|--|
| VAV | Generic | Current Temperature URL | Node path in the BMS gateway for reading back 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 reading back the status for occupancy. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/BI/OccUnocc_Sts/ |
| | | Occupied Temperature URL | Node path in the BMS gateway for reading back the occupied setpoint value. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/VAV/AV/RoomTemp_OccSetpt/ |
| | | Min Temperature Value | Minimum temperature to which the room temperature can be set. | 18 |
| | | Max Temperature Value | Maximum value of the room temperature that can be set. | 28 |
| | | Temperature Unit | 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 un occupied mode. | false |
| | | Temperature Setpoint URL | 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/ |
| Energy Meter | Generic | EnergyinKWH | Node path in the BMS gateway which provides the energy reading in KWH. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_BIM/HallMark/BGL10/Floor_Ground/PMS/AV/KWH |
| Gas Meter | Generic | gasConsumed | Node path in the BMS gateway which provides the gas consumption. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_API/HallMark/BGL10/Basement/Metering/AI/Gas_Consumed |
| Water Meter | Generic | waterConsumed | Node path in the BMS gateway which provides the water consumption. | /config/Drivers/NiagaraNetwork/aliases/India_Bangalore_API/HallMark/BGL10/Basement/Metering/AI/Water_Consumed |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-2 Device Properties and Values (continued)

| Device | Model | Device Property | Value Description | Sample Data |
|-------------|---------|-----------------|---|-----------------------|
| DMP 4400 | Generic | Username | User ID for logging in to the DMP. | admin |
| | | Touch | Touchscreen configuration in the Touch Details area: <ul style="list-style-type: none"> If the DMP has been configured with a signage that supports touchscreen overlay, select the Touch check box. If the DMP has been configured with a non-touch signage, keep the Touch checkbox unselected. | – |
| | | URL | The DMP URL. | https://10.77.78.80 |
| | | Password | User password for logging in to the DMP. | Cisco123 |
| | | MAC Address | The DMP MAC address. | 00:0f:44:02:7b:48 |
| | | Locale | Locale for the DMP to use. | en_US |
| IEC | Generic | Username | User ID for logging in to the IEC. | admin123 |
| | | Touch | Touchscreen configuration in the Touch Details area: <ul style="list-style-type: none"> If the IEC has been configured with a signage that supports touchscreen overlay, select the Touch check box. If the IEC has been configured with a non-touch signage, keep the Touch checkbox unselected. | – |
| | | URL | The IEC URL. | https://10.222.187.80 |
| | | Password | User password for logging in to the IEC. | Cisco321 |
| | | MAC Address | The IEC MAC address. | 00:0d:54:04:8c:53 |
| | | Locale | Locale for the IEC to use. | en_US |

To add devices to the SDP application, perform the following steps:

-
- Step 1** Log in to the SDP application.
- The List of Devices page appears. For more information on how to log in to the SDP application, see the *Cisco Service Delivery Platform User Guide*.
- Step 2** Click the **Devices** tab.
- The Devices page appears. The left pane displays the location hierarchy, and the right pane displays the List of Devices 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:
 3. Click  in the shortcut tools.
 4. In the Search field, enter a location keyword, and click .

Send documentation comments to scc-docfeedback@cisco.com

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 the location hierarchy:

1. Click  next to a parent location.

If the  is not displayed next to a parent location, the location does not have any child location.

2. Click a location for which you want to add the child location.

Step 4 In the right pane, click **Add a Device**.

The Add Device page appears. The Parent Location field displays the selected parent location with which you want to associate the device.

Step 5 Enter the following details:

- Device Category—Category under which you want to organize the device.
- Manufacturer—Manufacturer name of the device.
- Model—Model details of the device.
- Device Name—Name of the device.

Step 6 Click **Save**.

The newly added device is associated to the selected location.

Deleting Devices

To delete an device from the SDP application, perform the following steps:

Step 1 In the Devices page, select a location for which you want to modify the device details.

For more information on how to select a location, perform [Step 3](#) in the “[Adding Devices](#)” section on [page 3-14](#).

All devices that have been associated with the selected location are displayed.

Step 2 Do one of the following:

- To delete a single device, choose a device that you want to delete, and click .
- To delete multiple devices, select the specific check boxes of the devices that you want to delete, and click **Delete**.

The device is removed from the SDP application.

Send documentation comments to scc-docfeedback@cisco.com

Setting up Crestron Controller for the Projector

To set up Crestron Controller for the projector, you must have Windows 2008 R2 server machine or Windows 7 that has IIS 7.5 with .NET Framework 3.5 or above.

To set up the Crestron Controller, perform the following steps:

-
- Step 1** From the Linux machine, copy the Crestron Controller ZIP file located in `<MS_HOME>/pkg-properties/crestron` to a Windows machine
- Step 2** Unzip the `crestroncontroller.zip` files using any archive utility.
- Step 3** Run the `inetmgr` command. The IIS manager server console appears.
- Step 4** Right-click the default web site and choose create a new virtual directory.
- Step 5** Enter the alias as **crestron**. In the physical path, choose the Crestron Controller folder that is unzipped.
- Step 6** Right-click the `crestron` folder under Default Web Site, choose Convert to Application, and click **OK**. The application is created.
- Step 7** Enter the URL in a browser in the following format:

```
http://localhost/crestron/Home.aspx?deviceIp=<deviceIP of the Crestron Controller>
&ipId=<ipID of the Crestron controller>&port=<port of the Crestron Controller>&slot=<slot
of the Crestron Controller>&type=digital&join=<join value of the Crestron Controller>
```

- `deviceIP`—The IP ID of the Crestron Controller.
- `port`—Port of the Crestron Controller.
- `slot`—Slot of the Crestron Controller.
- `join`—Value depends on the action performed on the Crestron Controller.

For example:

```
http://localhost/crestron/Home.aspx?deviceIp=65.100.54.20&ipId=1&port=41794&slot=1&signal
Type=digital&join=62
```

A message appears indicating that the Crestron Controller is successfully set up.

Configuring Room Types

By default, the Office and Cubicle location types are configured as workspaces in the Smart+Connected Spaces 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 3-3](#) displays the `LOC_TYPE_ID`, which is the location type ID mapping in the `SSP_LOCATION_TYPE` table that is available in SDP.

Table 3-3 Room Types Properties

| Location Type ID (LOC_TYPE_ID) | Name (LOC_TYPE_NAME) |
|--------------------------------|----------------------|
| 15 | Cubicle |
| 23 | Office |

Send documentation comments to scc-docfeedback@cisco.com

Configuring Adapters

- [Adapter Description, page 3-24](#)
- [Configuring Adapter Properties, page 3-25](#)
- [Configuring Adapters to a Location, page 3-33](#)

Adapter Description

Table 3-4 lists the adapters that you must configure and the purpose these adapters serve for the functioning of the Smart+Connected Spaces application.

Table 3-4 **Adapter Description**

| Adapter | Description |
|----------------------|--|
| ObixBean | Configure this adapter to interface with the Tridium building management system. |
| AudioVideoBean | Configure this adapter to interface with Crestron Controller for projector and projector screen control. |
| 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 the Cisco JTAPI for sending emergency notifications. |
| DMMBean | Configure this adapter to interface with Digital Media Manager (DMM). |
| DMPBean | Configure this adapter to interface with the digital media players. |
| InformaCastBean | Configure this adapter to interface with Singlewire InformaCast for sending emergency notifications. |
| MediatorBean | Configure this adapter to interface with Cisco Network Building Mediator (NBM). |
| MobilityBean | Configure this adapter to interface with Call Manager for providing Extension Mobility. |
| WebCtrlBean | Configure this adapter to interface with WebCTRL, the building automation system by Automated Logic Corporation (ALC). |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-4 Adapter Description

| Adapter | Description |
|---------------------------|---|
| CPAMAccessManagerProvider | Configure this adapter to interface with Cisco Physical Access Manager (CPAM) for verifying user check-in. |
| IECBean | Configure this adapter to interface with the Cisco Interactive Experience Client for managing the display on signage.  Note The IECBean has no configurable property. |
| JabberBean | Configure this adapter to interface with Cisco Jabber for providing the list of the users' checked-in Jabber contacts. |
| TMSBean | Configure this adapter to interface with the Cisco TelePresence Management Suite for booking the TelePresence rooms. |



Note

You must configure either the IPPhoneOperationBean or the InformaCastBean adapter depending on whether you want to use Cisco JTAPI or Singlewire InformaCast for sending emergency notifications.

Configuring Adapter Properties

You need to configure adapter properties for the available adapters. Adapter configuration needs to be performed in the database by inserting data into the SDP_ADAPTER_PROPERTIES table.

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 provides information on the properties of the adapters, which can be used to come up with the SQL scripts that are then to be run against the database.

Table 3-5 Adapter Properties - Details

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|---|--|---|---------------------------|
| com.cisco.cre.ssp.adapter.obix.ObixBean | username | The Obix username | admin |
| | password | The Obix password | pAsswOrd |
| | url | The Obix URL | http : // 10.76.99.4/obix |
| | obixUrl | The Obix URL | http :// 10.76.99.4/obix |
| | obixTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to and read data from the Obix Bean adapter.  Note All the timeout values mentioned in this table are number values that need to be entered in the PROPERTY_NUM_VAL column. | 60000 |
| com.cisco.cre.ssp.adapter.audiovideo.AudioVideoBean | appPath | The path of the crestron application. | /crestron/Home.aspx |
| | hostname | The IP address of the host on which the Smart+Connected Spaces Crestron .NET component is setup on IIS. | 10.106.12.13 |
| | portNumber | The IIS port of the host on which the Smart+Connected Spaces Crestron .NET component is setup. | 80 |
| | audiovideoConnectionTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to the AudioVideoBean adapter. | 60000 |
| | audiovideoReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the AudioVideoBean adapter. | 60000 |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|--|---|---|---|
| com.cisco.cre.ssp.adapter.exchange.bean.ExchangeBean | exch_udpserverip | The Spaces 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:// <IP address of the exchange server>/autodiscovery/autodiscover.xml |
| | 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 Spaces application server listen port. | 7001 |
| | exchConnectionTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to the ExchangeBean adapter. | 60000 |
| | exchReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the ExchangeBean adapter. | 60000 |
| | impersonationConnectingSID | Represents the impersonation account when using a ExchangeImpersonation SOAP header. | PrincipalName or PrimarySmtpAddress |
| | callbackprotocol | The protocol used by an exchange server to send notifications. | http or https |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|--|---|--|---|
| com.cisco.cre.ssp.adapter.remedy.RemedyBean | password | The Remedy user's password | WPRcreIT4 |
| | userName | The Remedy user's username. | 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:// <IP address of the Remedy server>/arsys/servlet/RemedyIncidentWrapper |
| | hostName | The Remedy server IP Address/DNS hostname. | alli-stg-01.cisco.com |
| | portNumber | The Remedy Server port. | 80 |
| | remedyConnectionTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to the RemedyBean adapter. | 60000 |
| remedyReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the RemedyBean adapter. | 60000 | |
| com.cisco.cre.ssp.adapter.email.bean.EmailBean | toAddress | The address to which the e-mail needs to be sent for the case management. This is usually the facilities team helpdesk mail alias. | support @ cisco.com |
| | fromAddress | The address from which the e-mail needs to be sent for the case management. Usually, this mailbox is set up as a no-reply mailbox. | noreply-sdp @ cisco.com |
| | mail.smtp.port | The SMTP Server Port. | 25 |
| | mail.smtp.host | The IP Address/hostname of the SMTP server. | mailman.cisco.com |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|---|---|--|---|
| com.cisco.cre.ssp.adapter.ipphone.bean.IPPhoneOperationBean | password | The application user's password created in CUCM. For more information on the application password, see the “Assigning Roles (Groups) to the Application User” section on page 3-2. | ccmadmin |
| | username | The application username created in CUCM. For more information on the application username, see the “Assigning Roles (Groups) to the Application User” section on page 3-2. | Cisco @ 123 |
| | serviceuri | The uri of the Call Manager configured. | https:// <IP address of the Call Manager server>/realtimeservice/services/RisPort70 |
| | appusername | The application username created in CUCM. For more information on the application username, see the “Assigning Roles (Groups) to the Application User” section on page 3-2. | cisco |
| | apppassword | The application user's password created in CUCM. For more information on the application password, see the “Assigning Roles (Groups) to the Application User” section on page 3-2. | cisco |
| | audiourl | The audio message URL to inform the user about his checkout time. | http://10.0.0.0:17170/ipsapp/audio/audio_ipphone.wav |
| | message | The text message to inform the user about his checkout time. | You have 5 minutes to check out. |
| | ipphoneConnectionTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to connect to the IPPhoneOperationBean adapter. | 60000 |
| | ipphoneReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the IPPhoneOperationBean adapter. | 60000 |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|--|--|--|---|
| com.cisco.cre.ssp.adapter.dmm.DMMBean | dmm_url | The DMM URL. | https://<IP address of the DMM server>:<port on which the DMM server is running> |
| | dmm_username | The DMM username. | superuser |
| | dmm_domain | The domain of DMM. | scc-qa-dmm-1.cisco.com |
| | dmm_password | The DMM password. | Cisco_123 |
| | dmmConnectionTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to the DMMBean adapter. | 60000 |
| | dmmReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the DMMBean adapter. | 60000 |
| com.cisco.cre.ssp.adapter.ipphone.bean.InformaCastBean | uri | InformaCast URL | https://<IP address>:port of InformaCast server>/InformaCast/services/MessageServiceV2?wsdl |
| | username | InfomaCast username | admin |
| | password | InfomaCast password | admin |
| | informacastConnectionTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to the InformaCastBean adapter. | 60000 |
| | informacastReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the InformaCastBean adapter. | 60000 |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|---|---|---|--|
| com.cisco.cre.ssp.adapter.MediatorBean | username | The Cisco NMB username | admin |
| | password | The Cisco NMB password | password |
| | url | The Cisco NMB URL | <IP address of the Cisco NMB server> |
| | mediatorurl | The Cisco NMB URL | <IP address of the Cisco NMB server> |
| | mediatorConnectionTimeout | The maximum duration (in millisecond) for which the Spaces application tries to connect to the MediatorBean adapter. | 60000 |
| | mediatorReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the MediatorBean adapter. | 60000 |
| com.cisco.cre.ssp.adapter.mobility.MobilityBean | mobilityurl | The extension mobility URL | https://<IP address>:8443/emservice/EMServiceServlet |
| | mobappcertificate | Application password to access the extension mobility feature in CUCM. | Abbxv |
| | mobappid | Application ID to access the extension mobility feature in CUCM. | Abbxv |
| | mobappConnectionTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to connect to the MobilityBean adapter. | 60000 |
| | mobappReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the MobilityBean adapter. | 60000 |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|--|---|--|--|
| com.cisco.cre.ssp.adapter.webctrl.bean.WebCtrlBean | url | The WebCTRL URL. | <IP address of the WebCTRL server> |
| | port | Port on which the WebCTRL server is running. | 80 |
| | username | The username of the WebCTRL user. | user1 |
| | password | The password of the WebCTRL user. | pwRd1 |
| | webCtrlConnectionTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to connect to the WebCtrlBean adapter. | 60000 |
| | webCtrlReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the WebCtrlBean adapter. | 60000 |
| com.cisco.cre.ssp.adapter.accessmanager.cpam.CPAMAccessManagerProvider | cpamurl | The CPAM URL. | "http://<IP address of the CPAM server>/acws/services/psimws?wsdl" |
| | username | The username of the CPAM user. | user1 |
| | password | The password of the CPAM user. | pswRd1 |
| | cpamConnectionTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to connect to the CPAMAccessManagerProvider adapter. | 60000 |
| | cpamReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the CPAMAccessManagerProvider adapter. | 60000 |

Send documentation comments to scc-docfeedback@cisco.com

Table 3-5 Adapter Properties - Details (continued)

| Adapter (SDP_ADAPTER_DEFN) | Defined Adapter Property (SDP_ADAPTER_PROP_DEFN) | Adapter Property (SDP_ADAPTER_PROPERTIES) | Sample Value |
|--|---|---|--|
| com.cisco.cre.ssp.adapter.jabber.bean.JabberBean | jabberurl | The Cisco Jabber URL. | https://<IP address:port of the CUPS server>/EPASSoap/service/v70a |
| | username | The username of the Cisco Jabber user. | user1 |
| | password | The password of the Cisco Jabber user. | pswRd1 |
| | presenceserviceurl | The Cisco Unified Presence Server URL. | http://<IP address:port of the CUPS server>/presence-service/soap |
| | jabberConnectionTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to connect to the JabberBean adapter. | 60000 |
| | jabberReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the JabberBean adapter. | 60000 |
| com.cisco.cre.ssp.adapter.tms.TMSBean | username | The username of the Cisco TMS. | user1 |
| | password | The password of the Cisco TMS. | pswRd1 |
| | apiversion | The TMS application version. | |
| | bookingurl | The TP room booking URL. | http://10.106.9.158/tms/external/booking/remotesetup/remotesetupservice.asmx |
| | endpointurl | The TP room endpoint URL. | http://10.106.9.158/tms/external/booking/bookingService.asmx |
| | tmsConnectionTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to connect to the TMSBean adapter. | 10000 |
| | tmsReadTimeout | The maximum duration (in milliseconds) for which the Spaces application tries to read data from the TMSBean adapter. | 10000 |

Configuring Adapters to a Location

The adapters are configured to the specific location by mapping an adapter instance ID with the corresponding location in the SDP_ADAPTER_LOCATION_LINK table. When an adapter instance is associated to a location, the adapter instances are automatically applied to all the child locations for that location.

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

For a sample configuration for the ObixBean mapped to the location ID 10011, see the “Sample Adapter Configurations” section on page 3-34.

Sample Adapter Configurations

SDP_ADAPTER_DEFN table

This configuration is part of the seed data.

Table 3-6 *SDP_ADAPTER_DEFN table - Adapter Definition Mapped to an Adapter Definition ID*

| ADAPTER_DEFN_ID | ADAPTER | ADAPTER_JAR_LOCATION | VERSION | CREATED_BY | CREATED_DT | UPDATED_BY | UPDATED_DT | TENANT_ID |
|-----------------|---|----------------------|----------|------------|------------|------------|------------|-----------|
| 10 | com.cisco.cre.ssp.adapter.obix.ObixBean | – | version1 | superadmin | 27-JUN-12 | superadmin | 27-JUN-12 | 0 |

SDP_ADAPTER_INSTANCE

Table 3-7 *SDP_ADAPTER_INSTANCE - Adapter Definition ID Mapped to an Adapter Instance ID*

| 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 one or more locations. When an adapter is associated to a location, the adapter instances are automatically applied to all the child locations for that location.

Table 3-8 *SDP_ADAPTER_LOCATION_LINK Table - Adapter Instance ID Configured to the Preferred Location*

| 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 how to configure adapters, see the *Cisco Service Delivery Platform Installation Guide*.

If you change the values in these tables, you must restart the application to enable the changes.



Note

The IPPhoneOperationBean and the InformaCastBean adapters cannot point to the same location or the child location of either of these adapters in the sdp_adapter_location_link table.

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

Setting up Data Collection

To collect data from a Building Management System (BMS), you need to provide information on data points and the corresponding metadata in the SSP_DEVICE_PROPERTY_METADATA table. The device components are controlled by metadata and the metadata units defined in the SSP_DEVICE_PROPERTY_METADATA table.

Every device added in the SDP has a set of properties. Each property has a unique property id. If you need historic trending for these properties, you must configure the metadata for the properties in the SSP_DEVICE_PROPERTY_METADATA table.

Table 3-9 Metadata Properties

| Property | Purpose |
|-------------------|---|
| METADATA_ID | Primary key field of the table. |
| PROPERTY_VALUE_ID | Used to derive the id from the SSP_DEVICE_PROPERTY table which is unique across all the devices. It should be added in the SSP_DEVICE_PROPERTY_METADATA table. |
| TRENDABLE | If the trendable property is set to one, the data collector collects data for the property at the specified trend frequency. |
| TREND_FREQUENCY | Used to set the rate of data collection. Unit of measurement is minutes. The minimum value that can be provided is one minute. |
| UNIT_CONFIG | Unit of the data stored in the collection table in the database. |
| UNIT_MEASURED | Used to set the value of the unit of the data measured in BMS gateway. For example, water is measured in cubic meters. |
| MONITORABLE | Not applicable for the Smart+Connected Spaces application. Therefore, the value must be set to zero. |
| CUMULATIVE | Not applicable for the Smart+Connected Spaces application. Therefore, the value must be set to zero. |
| SCHEDULABLE | Not applicable for the Smart+Connected Spaces application. Therefore, the value must be set to zero. |
| CONTROLLABLE | Not applicable for the Smart+Connected Spaces application. Therefore, the value must be set to zero. |
| REPORTABLE | Not applicable for the Smart+Connected Spaces application. Therefore, the value must be set to zero. |
| ALARMABLE | Not applicable for the Smart+Connected Spaces application. Therefore, the value must be set to zero. |
| IS_NUMERIC | For a string property, the value is zero and the data gets collected in SSP_DATA_COLL_VAR table. For a numeric property, the value is one and the data gets collected in SSP_DATA_COLL table. |
| THRESHOLD | The threshold value is set only when it is cumulative and is based on UNIT_CONFIG value. After the threshold value is reached, the energy meter reading is reset. |

Send documentation comments to scc-docfeedback@cisco.com

Integrating CUCM and InformaCast

InformaCast is an emergency notification solution by Singlewire, that can broadcast audio stream, text messages, and notifications to multiple Cisco IP phones simultaneously as a group. InformaCast can broadcast either a live, recorded, or a scheduled message on your IP network with a single click from your computer or through API calls.

To use InformaCast in a telephony environment, you have to integrate Cisco Unified Communications Manager (CUCM) and InformaCast. Also ensure that you:

- Integrate Cisco Unified Communications Manager (CUCM) and InformaCast.
- Set up a multicast network as the InformaCast broadcast works on multicast network.



Note

You must verify that the InformaCast version and the CUCM version are compatible before you begin to integrate them.

For more information on how to configure and integrate the Cisco Unified Communications Manager (CUCM) and InformaCast, refer to the InformaCast help documentation and Singlewire online knowledge base.

Integrating Jabber with Smart+Connected Spaces

To allow the Smart+Connected Spaces to use Jabber, ensure that the LDAP, Cisco Unified Communications Manager, and CUPS are set up in the same domain and perform the following tasks in the Cisco Unified CM IM and Presence Administration:

-
- Step 1** Create an application user by navigating to the Application User Configuration page. Refer to the Cisco Unified CM IM and Presence Configuration Guide or the Cisco Unified CM IM and Presence Administration online help to understand how an application user is added. Click the following link to view the list of guides:
- <http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html>
- Step 2** Assign the following groups to the application user that you have created:
- Admin-3rd Party API
 - Admin-CUMA
- Step 3** Import LDAP users into the Cisco Unified Communications Manager database. For information on how to import Active Directory users, refer to the following link:
- <http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-71/112880-cucm-8x-ldap.html>
- Step 4** Configure the following settings for the end users by navigating to the End User Configuration page:
- a. Check the **Home Cluster** and **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** check boxes.
 - b. Assign the following groups and roles:
 - Group
 - Standard CCM End Users

Send documentation comments to scc-docfeedback@cisco.com

Roles

- Standard CCM End Users
- Standard CCMUSER Administration

Importing SSL Certificates

You must import the SSL certificates for the Cisco Unified Communications Manager (CUCM). You may also require to import the SSL certificates for the Cisco Digital Media Player (DMP), Cisco Interactive Experience Client (IEC), and Light Weight Directory Access Protocol (LDAP).

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

To import the 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, and <Alias Name> is the unique alias name.



Note In case of a separate keystore for the local certificates, change the keystore and storepass values in the above command.

For example:

```
./keytool -import -alias CM -file /home/scc-qa/CM115.cer -keystore
```



Note If you have installed the JDK using an RPM bundle, then you need access as a root user or a user with sudo permissions 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.

Changing the JBoss Port

In a non-cluster setup, the Smart+Connected Spaces application is deployed on a single node of a virtual machine and the database resides in a different virtual machine (VM). In a colocated setup, both the solution and the database reside on the same VM. You must change the following default port values that the application listens to, in order to avoid port conflicts:

Send documentation comments to scc-docfeedback@cisco.com

- 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.

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

Step 1 Open the following file:

`$JBOSS_HOME//domain/configuration/domain.xml`

Step 2 Search for 'socket-binding-group name = full-sockets', search for 'http port = 8080', and then change the port number with a value that is not in use, for example, 7159.

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

```
<socket-binding-group name="full-sockets"
  default-interface="public">
  <socket-binding name="ajp" port="8009"/>
  <socket-binding name="http" port="7159"/>
  <socket-binding name="https" port="8443"/>
  <socket-binding name="jacorb" interface="unsecure" port="3528"/>
  <socket-binding name="jacorb-ssl" interface="unsecure" port="3529"/>
  <socket-binding name="messaging" port="5445"/>
  <socket-binding name="messaging-group" port="0"
multicast-address="{jboss.messaging.group.address:231.7.7.7}"
multicast-port="{jboss.messaging.group.port:9876}"/>
  <socket-binding name="messaging-throughput" port="5455"/><socket-binding
name="remoting" port="1199"/>
</socket-binding-group>
```



Note

- While changing the default port values, ensure that you do not change any other port number apart from the 'Http' and 'Port' values of 'socket binding group name = full-sockets'.
- All of the necessary property files need to be updated with the modified port number.

Step 3 Save the file.

Configuring the Property Files

The automated installer creates the required property files with the default values. If you do not want to use the default values, you can configure the property files manually.

- [Configuring the Property Files for Non-Clustered Setup, page 3-38](#)
- [Changing the Theme of the Room Booking Portal, page 3-48](#)

Configuring the Property Files for Non-Clustered Setup

In case you want to update the application.properties, dc.properties, LDAP.properties, logging.properties, and cleWebexAdapterConfig-MC.properties files, perform the following steps:

Step 1 Open a terminal and navigate to `<SPACES_INSTALL_DIRECTORY>/pkg-properties`, where `<SPACES_INSTALL_DIRECTORY>` is the location at which the Smart+Connected Spaces application is installed.

Send documentation comments to scc-docfeedback@cisco.com

Step 2 Update the application.properties file:

a. Modify the properties as follows:

| | |
|---------------------------|---|
| energysavings_batch_limit | Size of groups in which the total conference rooms will be divided for the energy savings to be performed in batches. You can change the default value as per your requirement. |
| minutes | Time slots displayed on IP phones for booking meetings. The minimum limit is 30. |
| IB_JMSPROVIDER_URL | <i>remote://<Spaces Appserver IP Address or hostname>:<Spaces Appserver port number></i> For example, IB_JMSPROVIDER_URL=remote://10.0.0.0:4547 |
| IB_userName | <i><Spaces JBoss profile admin userid></i> For example, IB_userName=superadmin |
| IB_password | <i><Spaces JBoss profile admin password></i> For example, IB_password=superadmin |
| SDP_JMSPROVIDER_URL | <i>remote://<SDP Appserver IP Address or hostname>:<SDP Appserver port number></i> For example, SDP_JMSPROVIDER_URL=remote://10.0.0.0:4447 |
| SDP_userName | <i><SDP JBoss profile admin userid></i> For example, SDP_userName=superadmin |
| SDP_password | <i><SDP JBoss profile admin password></i> For example, SDP_password=superadmin |
| emission_factor | Carbon emission factor per 1 kWh For example, 0.00068956d |
| carbon_unit | Unit for measuring the carbon emission. |
| flighthr_Co2E | Number of flight hours saved and the reduction in carbon emission due to TelePresence usage. |
| pageSize | Number of saved drafts displayed per view in the Smart+Connected Spaces user portal. |
| working_hours | Number of working hours for a day in the enterprise. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|--|---|
| REMINDERS: | Number of minutes before the meeting when reminders will be send to all the invitees. |
| <ul style="list-style-type: none"> • showReminder1 • showReminder2 • showReminder3 • showReminder4 | |
| skin_name | <p><i><Name of the skin folder for the Spaces user portal></i></p> <p>For example, skin_name=red</p> |
| maps_theme | Color of the theme that appears for the kiosk interface. The default color is grey. You can change it to blue. |
| ms_serviceurl | <p>http://<MS Appserver IP Address or hostname>:<MS Appserver port number>/services/webcalendarservices/confDetails</p> <p>For example,</p> <p>http://10.0.0.0:8180/services/webcalendarservices/confDetails</p> |
| ps_serviceurl | <p>http://<PS Appserver IP Address or hostname>:<PS Appserver port number>/ipsapp</p> <p>For example, http://10.0.0.0:8180/ipsapp/services</p> |
| availablesoon | <p>Time in minutes to change the status of the workspaces and rooms to be available soon.</p> <p>For example, 25</p> |
| | <p> Note The default availablesoon time is 60 minutes. You can change it as per your requirement. The status color changes to yellow for the soon-to-be-available conference/TP rooms and workspaces for this duration.</p> |
| cronTriggerExpression | <p>Time at which the LDAP user details will be synchronized with the Smart+Connected Spaces application.</p> <p>For example, 0 04 13 * * ?</p> |
| | <p> Note The default cronTriggerExpression time is 12 am. You can change it as per your requirement.</p> |
| user_preference_required | <p>Show/hide the 'Do not publish my location' check box in the kiosk web portal.</p> <p>For example, 'yes' if you want to display the check box.</p> |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|--------------------------|--|
| server_type | Type of the application server used. All of the server parameters are specified based on this property. For example, JBoss |
| display_jabber_tab | Determines whether to display the Cisco Jabber tab. |
| usersubscription | Determines whether to display the option to subscribe all of the users in the LDAP. |
| triggertimeforautocancel | The trigger time (in milliseconds) to trigger an auto cancel. |
| 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 the autocancelflag is negative and the booking period is for X hours, then the auto cancelling process occurs after X hours. |
| autocancel | The auto cancel time in minutes. Automatic cancellation of the reservation happens when the user does not check in before the trigger time. |
| gracetimeforcheckin | Allows you to check in to a workspace prior to the reserved time. The grace time is in minutes. |
| advancebookingstatus | Allows you to book a workspace in advance if the value is true. |
| advancebookingmaxday | Represents the maximum number of days for which a booking in advance is allowed. |
| repeatbookingstatus | Allows you to book for multiple days if the value is true. This is dependent on the advance booking status. |
| repeatbookingmaxday | Defines the maximum number of days for which you can book for multiple days. This is dependent on the advancebookingmaxday property. |
| iecDefaultURL | Defines the path for displaying the Smart Spaces application Sign Out page. |
| signageWelcomePage | Defines the path for displaying the Smart Spaces application Welcome page. |
| signageLayoutPage | Defines the path for displaying the user's layout content. |
| iecRefreshInterval | Defines the duration by which the content gets refreshed. |
| minbookingduration | Defines the duration by which the workspace can be available. This duration is in minutes. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|----------------------------|---|
| hostname | Hostname of the Smart Spaces server for the Digital Media Player (DMP). |
| port | Port number of the Smart Spaces server. |
| appURL | Defines the application URL for the IEC device to display the layout content. |
| Adapter1 | Defines the adapter type for lights. |
| Adapter2 | Defines the adapter type for blinds. |
| Adapter3 | Defines the adapter type for dimmers. |
| Adapter29 | Defines the adapter type for air conditioners. |
| wholeDayBookingStartHour | Defines the start hour time for the whole day booking (in 24 hour format). |
| wholeDayBookingStartMinute | Defines the start minute time for the whole day booking. |
| wholeDayBookingEndHour | Defines the end hour time for the whole day booking (in 24 hour format). |
| wholeDayBookingEndMinute | Defines the end minute time for the whole day booking. |
| IP_PHONE_DATE_FORMAT | Defines the format of the date as supported by the CUCM. |
| mail.transport.protocol | The SMTP protocol used for sending and receiving an email. |
| mail.transport.host | Host name of the mail server. |
| mail.transport.port | Port number of the mail server. |
| system_admin_address | Email ID of the system administrator. |
| admin_address | Email ID of the administrator. |
| event_subject | Subject of an email. |
| event_body | Body of an email. |
| from_address | Email ID of a person or group. |
| reply_to_address | Email ID of a person or group. |
| to_address | Email ID of a person or group. |
| reservation_subject | Subject line of the meeting room reservation event. |
| shared.file | Defines the path of the person details properties file. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|-----------------------------|---|
| domain | The Jabber SDK domain name. |
| unsecureAllowed | Determines whether HTTP or HTTPS protocol is to be used for Jabber. |
| httpsBindingURL | IP address of the Presence server. |
| application.realm.username | Username to be provided when installing the application. |
| application.realm.password | Password to be provided when installing the application. |
| image_path | Defines the path of the logo images. |
| autodiscovery_exceptions | List of autodiscover exceptions. |
| dmp_access_sec | Multiple call from DMP to Smart Spaces application. |
| user_id_length | Defines the maximum length of the user ID. |
| meetings_fetch_for_max_days | Defines the maximum number of days for which the meeting details can be obtained from the Smart Spaces application. |

b. Save and close the file.

Step 3 Update the dc.properties file:

a. Modify the properties as follows:

| | |
|--------------------------------------|--|
| datacollection.useTridiumWatch | To use Tridium as a watch, set the value as True. If the value is false, Tridium will be history based. |
| datacollection.scheduler.interval | Interval in minutes for history based data collection. |
| datacollection.batch.size | Number of data collection points from which data is gathered at a time. |
| datacollection.unitxml.path= | <SPACES _INSTALL_DIRECTORY>/pkg-properties/datacollection/unit.xml For example, datacollection.unitxml.path=/home/scc-qa/pkg-properties/datacollection/unit.xml |
| datacollection.jms.jndi | JNDI for the data collection JMS. |
| datacollection.jms.connectionfactory | Connection factory for the data collection JMS. |
| datacollection.jms.initialContext | Class name for the JMS initial context. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|--|---|
| datacollection.jms.providerUrl | <i>remote://<Spaces Appserver IP Address or hostname>:<MS Appserver port number></i> For example, datacollection.jms.providerUrl=remote://10.0.0.0:4547 |
| datacollection.jms.securityPrincipal | <i><Spaces JBoss admin console user name></i> For example, datacollection.jms.securityPrincipal=superadmin |
| datacollection.jms.securityCredentials | <i><Spaces JBoss admin console password></i> For example, datacollection.jms.securityCredentials=superadmin |
| datacollection.data.precision | Data precision for the data collected by the BMS. For example, 0.00 |
| application.realm.username | Application user name for the JBoss server. For example, application.realm.username=admin. |
| application.realm.password | Application user password for the JBoss server. For example, application.realm.password=Cisco_123. |

b. Save and close the file.

Step 4 Update the LDAP.properties file:

a. Modify the properties as follows:

| | |
|----------------------------------|---|
| 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. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|------------------------------------|---|
| 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. |
| 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 whether 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.employeeype | The attribute to identify whether the nature of the user's employment is permanent or contractual. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|-----------------------------|--|
| ldap.user.worktype | The attribute to identify whether the worker is assigned a location, or is a mobile worker. |
| ldap.user.publishmobile | This attribute indicates whether the user's mobile number is displayed or not. The value should be set to yes for the user's mobile number to display. |
| ldap.user.publishpager | This attribute indicates whether the user's pager number is displayed or not. The value should be set to yes for the user's pager number to display. |
| 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 whether the user's location is displayed or not. The value should be set to yes for the user's location to display. |
| 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. |

Send documentation comments to scc-docfeedback@cisco.com

| | |
|-------------------------------|---|
| ldapBase | The base DN to be used for doing an LDAP search. |
| ldapUserName (Mandatory) | The bind username in case of a non-anonymous bind. |
| ldapMaxReturnSize (Mandatory) | The maximum number of users whose details are fetched in one batch from the LDAP. |
| ldap.user.isroom (Mandatory) | The attribute to identify whether the resource is a user or a room. |
| ldap.bind.root | The base DC to be used for doing an LDAP search. |
| cron.run.time | The attribute to identify the run time of the LDAP profile file. |
| ldap.search.zulupattern | The string pattern to use for doing an LDAP search. |



Note You can modify only the mandatory properties listed in the table. Modify the non-mandatory properties if required.

b. Save and close the file.

Step 5 Update the cleWebexAdapterConfig-MC.properties file:

a. Modify the properties as follows:

| | |
|----------------------|---|
| WEBEX_SITE_ID | For example, WEBEX_SITE_ID=98765432 |
| WEBEX_SITE_NAME | For example, WEBEX_SITE_NAME=abcorp |
| WEBEX_PARTNER_ID | For example, WEBEX_PARTNER_ID=123ci |
| WEBEX_XML_SERVER_URL | WEBEX_XML_SERVER_URL=https://abcorp/WBXService/XMLService |
| WEBEX_USER | For example, WEBEX_USER=genuser |



Note Ensure that the permission to create WebEx sessions is provided to all the WEBEX_USER values. This enables the users to avail the WebEx meeting feature while accessing the Smart+Connected Spaces portal for room booking (web calendar).

| | |
|----------------|--|
| WEBEX_PASSWORD | For example, WEBEX_PASSWORD=Hilly!23 |
| TOLL | For example: US TOLL = +1-415-655-0001 |

b. You can retain the default values for the other properties in the cleWebexAdapterConfig-MC.properties file.

Send documentation comments to scc-docfeedback@cisco.com

- c. Save and close the file.

Changing the Theme of the Room Booking Portal

You can change the skin of the user interface for the Spaces portal for room booking, so that the users can view the changed skin instead of the default skin. To activate a skin, you need to update the value of the key "skin_name" in the application.properties file. For example, skin_name=red



Note

The value should be a valid skin folder name. It is necessary that you restart the application to enable the changes.

Customizing the Branding Images of the Workspaces Portal

The branding images include the logo and the login screen. You can customize the user interface of the Smart+Connected Spaces portal for workspaces and offices by changing one or both of these images.

To customize the branding images, perform the following steps:

Step 1 Open the **SmartSpaces.ear** file, and then open the **ipsapp.war** file using any archive utility.

Step 2 Navigate to the images directory, and replace the login and the logo images.

[Table 3-10](#) displays the specifications of the branding images.

Table 3-10 Branding Image Specification

| Image Type | File Name | Width | Height |
|------------------|---------------------|------------|------------|
| Logo | cicso_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 3-10](#).



Note

You must re-deploy the SmartSpaces.ear file to enable changes to the branding images.