CHAPTER 2

Installing the Smart+Connected MS

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

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

After successfully installing the Smart+Connected MS application, you can configure the application by performing tasks that are listed in Chapter 3, "Configuring the Smart+Connected MS Application".

Prerequisites

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 is 1521.
  - 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.

- 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

Verifying Network Configurations

Verify the following network configurations:

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

Installing on a Colocated or Non-Cluster Server Setup

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

1. Installing the Application, page 2-3
2. Configuring the Database, page 2-4
3. Creating JBoss Profile, page 2-7
4. Setting Up Port, page 2-9
5. Setting Up Security Configuration, page 2-9
6. Setting Up Java Messaging Service (JMS), page 2-12
7. Setting Up Library, page 2-16
8. Setting Up Quartz, page 2-16
9. Configuring Logging, page 2-16
10. Configuring the Properties Files, page 2-17
11. Setting up Run Parameters, page 2-28
12. Setting up Apache Jackrabbit, page 2-29
13. Importing SSL Certificates, page 2-30
14. Starting the JBoss Server, page 2-31
15. Assigning Roles and Locations to the IB User, page 2-31
16. Creating and Assigning Webcalendar Roles, page 2-32
17. Accessing the Application and Verifying the Installation, page 2-33
18. Accessing the Web Calendar, page 2-33
19. Accessing the Kiosk Web Portal, page 2-34

Installing the Application

The Smart+Connected MS installation package consists of an executable file (install.bin) that is located on the product DVD.

Before you begin the installation, do the following:

- Copy the installer file to a local directory.
- Ensure that the <*JAVA_HOME*> environment variable is set to the location at which the JDK is installed and the PATH environment variable includes the <*JAVA_HOME*>/bin folder.

To install the application, perform the following steps:

Step 1 From the product DVD, run the installer:

a. In a terminal session, navigate to the directory that contains the installer and give execute permission to the install.bin file.

b. Enter the following command:

```
chmod u+x install.bin
```

c. Enter the following command:

```
./install.bin
```

Alternatively, use the installer that is available in the e-delivery package.

The Smart Plus Connected Communities - Introduction screen appears.

Step 2 Click **Next**.

The License Agreement screen appear.

Step 3 Choose **I accept the terms of the License Agreement**, and click **Next**.

The Choose Install Folder screen appears.

Step 4 Click **Choose** to select the directory where you want the applications to be installed. Alternatively, you can enter the path manually.

Note The location where you install the Smart+Connected MS application is referred as <*MS_INSTALL_DIRECTORY*> in this guide.

Step 5 (Optional) Click **Restore Default Folder** if you want to revert to the default directory.

Step 6 Click **Next**.

The Pre-Installation Summary screen appears.

Step 7 Click **Install**.

After the installation is complete, the Install Complete screen appears.

Step 8 Click **Done** to complete the installation process.

Step 9 Navigate to the directory that you had selected during installation, and verify that the following directories have been created:

- pkg-apps
- pkg-clientsamples
- pkg-jackrabbit
- pkg-jars

- pkg-jbosswsjars
- pkg-properties
- pkg-scripts
- pkg-templates

Configuring the Database

Requirements

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

- Ensure that Oracle is installed on your database server, and is ready for use.

  This document does not include information on how to set up the Oracle database. For more information, see the Oracle documentation.
- Ensure that you have provided the 'ALL' privilege to the Oracle database.
- Ensure that the following SDP database SQL scripts are already executed:
  - setup-sdp-base.sql
  - setup-sdp-types.sql

  For more information on how to execute the SDP database SQL scripts, see the "Executing Database Scripts" section on page 2-6.

About Database Scripts

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

SDP Database Scripts

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

<*SDP_INSTALL_DIRECTORY*>/sdp/

Table 2-1 SDP Database Script - Details

Script	Description
`clean-sdp-objects.sql`	Cleans all SDP-related objects from the user schema if an instance of SDP was running earlier. Executing this script is not necessary if you are installing the SDP for the first time.
`setup-sdp-base.sql`	• Creates the tables, constraints, sequences, and indexes. • Loads only the basic data that is required to bootstrap the application. • Enables the local database authentication. • Creates a user with the default username/password as superadmin/superadmin. • Adds the locations that are defined in the seed data. • Grants access rights to the locations to SuperAdmin (super administrator).
`setup-sdp-types.sql`	Loads the device types and device properties data.

MS Application Database Scripts

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

<*MS_INSTALL_DIRECTORY*>pkg-scripts

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

Table 2-2 Smart+Connected MS Database Script - Details

Script	Description
clean-Smart_Connected_Meeting_Spaces_and_Digital_Signage-objects.sql	Cleans all the Smart+Connected MS related objects from the user schema. Executing this script is not necessary if you are installing the application for the first time.
clean-common-objects.sql	Cleans all the Smart+Connected MS and the Cisco Smart+Connected Personalized Spaces (Smart+Connected PS) related objects from the user schema. Executing this script is not necessary if you have not installed either of the two applications earlier. **Note** Run this script only once as part of either the Smart+Connected MS or the Smart+Connected PS installation.
setup-common-base.sql	• Creates the tables, constraints, sequences, and indexes that are common to the Smart+Connected MS and Smart+Connected PS applications. • Loads the basic data that is required to bootstrap the applications. **Note** To install the MS and PS applications, run the clean-common-objects.sql and setup-common-base.sql scripts, followed by the PS scripts, and finally the MS scripts.
setup-Smart_Connected_Meeting_Spaces_and_Digital_Signage-base.sql	• Creates the tables, constraints, sequences, and indexes. • Loads the basic data that is required to bootstrap the application.
setup-Smart_Connected_Meeting_Spaces_and_Digital_Signage-base_ko.sql	• Creates the tables, constraints, sequences, and indexes. • Loads the basic data that is required to bootstrap the application in Korean.

Executing Database Scripts

To execute the Smart+Connected MS database scripts, perform the following steps:

Step 1 From the application install directory, copy the pkg-scripts folder to a location on the database machine.

You can access the pkg-scripts folder from the following location:

<*MS_INSTALL_DIRECTORY*>/pkg-scripts, where <*MS_INSTALL_DIRECTORY*> is the location at which the Smart+Connected MS & DS application is installed.

Step 2 Navigate to the <*MS_INSTALL_DIRECTORY*>/pkg-scripts folder on the database machine.

Step 3 Connect to SQL*Plus:

a. In a terminal session, enter **sqlplus**.

b. Press **Enter**.

Step 4 Enter the database username and password.

Step 5 For an English setup, enter

`@<MS_INSTALL_DIRECTORY>/pkg-scripts/setup-Smart_Connected_Meeting_Spaces_and_Digital_Signage-base.SQL`

For a Korean setup, enter

`@<MS_INSTALL_DIRECTORY>/pkg-scripts/setup-Smart_Connected_Meeting_Spaces_and_Digital_Signage-base_ko.SQL`

Step 6 Press **Enter**.

The database objects are created in your schema for the Smart+Connected MS application.

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

Creating JBoss Profile

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

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

Step 1 Download jboss-6.0.0.Final.zip.

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

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

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

Step 3 Open the terminal and set the *$JBOSS_HOME* and *$JAVA_HOME* environment variables by entering the following commands:

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

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

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

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

```
cd $JBOSS_HOME/server
```

Step 5 Copy the 'default' directory with the name 'solutions' by entering the following command:

```
cp -R default solutions
```

The 'solutions' directory is created under the $*JBOSS_HOME*/server directory. The 'solutions' directory is used as the Smart+Connected MS & DS application profile.

Step 6 Copy the Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear file, which is available in <*MS_INSTALL_DIRECTORY*>/pkg-apps, to the *$JBOSS_HOME*/server/solutions/deploy directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-apps/Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear $JBOSS_HOME/server/solutions/deploy
```

Step 7 Create a datasource file so that the Smart+Connected MS & DS application communicates with the database machine:

a. Create the oracle-ds.xml file under the 'solutions/deploy' folder and the SDP application with the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<local-tx-datasource>
<jndi-name>jdbc/scc</jndi-name>
<connection-url>jdbc:oracle:thin:@IPaddress:1521/DBName</connection-url>
<driver-class>oracle.jdbc.OracleDriver</driver-class>
<user-name>DBusername</user-name>
<password>DBpassword</password>
<min-pool-size>10</min-pool-size>
<max-pool-size>50</max-pool-size>
</local-tx-datasource>
</datasources>
```

b. Replace the following text with their actual values in the text that you had added in Step 7 a.:

- 'IPaddress' with the database server IP address or DNS hostname
- 'DBName' with the database name
- '1521' with the database port number if changed during the Oracle installation
- 'DBusername' with the database schema username
- 'DBpassword' with the database schema password

c. Save the file.

Step 8 Update the run.conf file to increase the memory:

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

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

Replace with the following text:

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

b. Save the file.

Setting Up Port

In a non-cluster setup, the Smart+Connected MS 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:

- 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 MS application, perform the following steps:

Step 1 Open the following file:

$JBOSS_HOME/server/solutions/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml

Step 2 Search for the port number 8080 that has the ‘bindingName’ value as ‘HttpConnector’ and replace with a port number that is not in use, for example 7159.

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

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">
  <property name="serviceName">jboss.web:service=WebServer</property>
  <property name="bindingName">HttpConnector</property>
  <property name="port">7159</property>
  <property name="description">JBoss Web HTTP connector socket; also drives the values
for the HTTPS and AJP sockets</property>
</bean>
```

Step 3 Search for the port number 1099 that has the 'bindingName' value as 'Port' and replace with a port number 1199.

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

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">
  <property name="serviceName">jboss:service=Naming</property>
  <property name="bindingName">Port</property>
  <property name="port">1199</property>
  <property name="description">The listening socket for the Naming service</property>
</bean>
```

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

Step 4 Save the file.

Setting Up Security Configuration

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

- JBoss 6 uses the HornetQ JMS engine for enterprise grade messaging. For the application to avail the Jboss messaging feature, making changes to the queue configuration file is not enough. To avoid possible authentication related errors, you would need to disable JMS security in both the Smart+Connected MS application and the SDP server.

- To authenticate the LDAP users of the Smart+Connected MS & DS application.

To set up security configuration, perform the following steps:

Step 1 To disable the JMS message security for the SDP server:

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

Where, <*SDP_PROFILE_DIR*> is the SDP JBoss profile directory

b. In the hornetq-configuration.xml file, add the following after the </security-settings> end tag to disable the JMS message security:

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

Note The value of the JMS message security is set to 'true' by default.

c. Save the file.

The JMS message security is now set to false.

Step 2 To disable the JMS message security for the Smart+Connected MS & DS application:

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

b. Save the file.

The JMS message security is now set to false.

Step 3 To enable the LDAP authentication for the application users:

a. In the *$JBOSS_HOME*/server/solutions/conf/login-config.xml file, search for the following text:

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

b. Add the following text after the preceding text:

```
<application-policy name="SDP">
<authentication>
  <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
    flag="sufficient">
    <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.SDPDataSourceLoginMod
ule</module-option>
    <module-option name="jndiName">java:jdbc/scc</module-option>
    <module-option name="debug">true</module-option>
  </login-module>
  <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
    flag="sufficient">
    <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.ldap.SDPLdapLoginModu
le</module-option>
    <module-option name="jndiName">java:jdbc/scc</module-option>
```

```
    <module-option
name="initialContextFactory">com.sun.jndi.ldap.LdapCtxFactory</module-option>
            <module-option
name="connectionURL">ldap://ldap.example.com:389</module-option>
            <module-option
name="connectionUsername">uid=name1,ou=people,ou=com</module-option>
            <module-option name="connectionPassword">password123</module-option>
            <module-option name="authentication">simple</module-option>
            <module-option
name="userBase">ou=active,ou=employees,ou=people,o=example.com</module-option>
            <module-option
name="userSearchMatching">sAMAccountName={0}</module-option>
            <module-option name="userSearchSubtree">true</module-option>
            <module-option name="debug">true</module-option>
</authentication>
</application-policy>

<application-policy name="SDP-REPORTING">
 <authentication>
   <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
     flag="sufficient">
     <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.SDPDataSourceLoginMod
ule</module-option>
     <module-option name="jndiName">java:jdbc/scc</module-option>
     <module-option name="debug">true</module-option>
   </login-module>
   <login-module code="com.cisco.sdp.core.security.authn.module.ProxyLoginModule"
     flag="sufficient">
     <module-option
name="loginModuleClass">com.cisco.sdp.core.security.authn.module.ldap.SDPLdapLoginModu
le</module-option>
     <module-option name="jndiName">java:jdbc/scc</module-option>
     <module-option
name="initialContextFactory">com.sun.jndi.ldap.LdapCtxFactory</module-option>
             <module-option
name="connectionURL">ldap://ldap.example.com:389</module-option>
             <module-option
name="connectionUsername">uid=name1,ou=people,ou=com</module-option>
             <module-option name="connectionPassword">password1</module-option>
             <module-option name="authentication">simple</module-option>
             <module-option
name="userBase">ou=active,ou=employees,ou=people,o=example.com</module-option>
             <module-option
name="userSearchMatching">sAMAccountName={0}</module-option>
             <module-option name="userSearchSubtree">true</module-option>
             <module-option name="debug">true</module-option>
   </login-module>
   <login-module code="org.jboss.security.ClientLoginModule" flag="required"
></login-module>
 </authentication>
</application-policy>
```

c. Replace the following LDAP server and LDAP user details with their actual values in the text that you added in Step 3 b.:

   - connectionURL
   - connectionUsername
   - connectionPassword
   - authentication
   - userBase

- userSearchMatching
- userSearchSubtree

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

d. Save the file.

The LDAP configuration is complete.

The JMS message security is now set to false.

Setting Up Java Messaging Service (JMS)

The Smart+Connected MS application uses Java Messaging Service (JMS) for asynchronous tasks. You need to set up JMS.

Creating a Connection Factory

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

Creating a Connection Factory in the SDP

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

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

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

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

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

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

Step 3 Replace '/ConnectionFactory' with '/SDPXAConnectionFactory' as follows:

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

Step 4 Save the file.

The connection factory is created in the SDP.

Creating a Connection Factory in the Smart+Connected MS

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

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

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

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

Step 3 Replace '/ConnectionFactory' with 'SDPXAConnectionFactory' as follows:

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

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

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

Step 5 Replace '/ConnectionFactory' with 'SDPXAConnectionFactory' as follows:

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

Step 6 Add the below text before the <queue name="DLQ"> tag:

```
<connection-factory name="sspConnectionFactory">
      <connectors>
         <connector-ref connector-name="in-vm"/>
      </connectors>
```

```
        <entries>
           <entry name="/sspConnectionFactory"/>
           <entry name="/XAConnectionFactory"/>
        </entries>
     </connection-factory>

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

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

Step 7 Save the file.

Creating an Event Topic

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

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

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

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

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

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

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

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

Step 4 Save the file.

An event topic is created in the SDP server.

Configuring an Event Topic

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

Step 1 In a file browser, navigate to *$JBOSS_HOME*/bin, and open the run.sh file for the SDP profile.

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

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

Step 3 Add the following command line to the text that you have searched for:

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

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

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

Step 4 Save the file.

Creating Queues

You need to create queues in the Smart+Connected MS application server.

To create queues, perform the following steps in the Smart+Connected MS application server:

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

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

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

Step 3 After the preceding text, add the following text:

```
 <queue name="insertUsageQueue">
   <entry name="/jms/insertUsageQueue"/>
 </queue>

 <queue name="callbackExchangeQueue">
   <entry name="/jms/callbackExchangeQueue"/>
 </queue>

<queue name="emailCaseManagementQueue">
   <entry name="/jms/emailCaseManagementQueue"/>
 </queue>

<queue name="dataCollectionQueue">
   <entry name="/jms/dataCollectionQueue"/>
 </queue>

<queue name="emailPoisonQueue">
   <entry name="/jms/emailPoisonQueue"/>
</queue>
```

Step 4 Save the file.

The JMS queues for the Smart+Connected MS application are created.

Setting Up Library

JBoss requires the Oracle library for connecting to the Oracle database. To set up the library, copy the following jar files to the *$JBOSS_HOME*/server/solutions/lib folder:

- ojdbc14.jar—Available at the <*MS_INSTALL_DIRECTORY*>/pkg-jars location on the server where the Smart+Connected MS has been installed.
- sdp-authmodules.jar—Available at the <*SDP_INSTALL_DIRECTORY*>/sdp/bin/jars location on the server where the SDP has been installed.
- datacollection.jar—Available at the <*MS_INSTALL_DIRECTORY*>/pkg-jars location on the server where the Smart+Connected MS has been installed.

Note For cluster deployment, copy the jar files to the *$JBOSS_HOME*/server/all/lib folder on the Node 1 and Node 2 servers.

Setting Up Quartz

The Smart+Connected MS application uses Quartz the enterprise scheduler. To set up Quartz, remove the quartz-ra.rar under the *$JBOSS_HOME*/server/solutions/deploy folder to make the use of Quartz from the ear.

Note For cluster deployment, the folder path is *$JBOSS_HOME*/server/all/deploy.

Configuring Logging

For the application to log the information and error messages to the correct log files, you need to configure the logging.properties file. To configure logging in the JBoss server, perform the following steps:

Step 1 Create the 'SCMS_Log' folder in the <*MS_INSTALL_DIRECTORY*>, and provide the read and write permissions to the users who run the JBoss profile for the Smart+Connected MS application.

Step 2 Navigate to the $JBOSS_HOME/server/solutions/deploy directory, and open the ‘jboss-logging.xml’ file in a text editor.

Step 3 Below the existing ‘periodic-rotating-file-handler’ tag, add the following text:

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

For example:

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

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

Step 4 Search for the following text:

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

Replace the text as follows:

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

Step 5 Save the ‘jboss-logging.xml’ file.

Logging is configured for the Smart+Connected MS application.

Configuring the Properties Files

Updating the Properties Files

To update the application.properties, dc.properties, LDAP.properties, logging.properties, ehcacheconfig, and cleWebexAdapterConfig-MC.properties files, perform the following steps:

Step 1 Copy the properties files from <*MS_INSTALL_DIRECTORY*> to a local directory.

a. Create a folder with a name 'ms_config' under the directory in which the Smart+Connected MS application is set up, and assign the read and write permissions.

b. Open a terminal and navigate to <*MS_INSTALL_DIRECTORY*>/pkg-properties, where <*MS_INSTALL_DIRECTORY*> is the location at which the Smart+Connected MS application is installed.

c. Copy the application.properties.sample file to the <*MS_INSTALL_DIRECTORY*>/ms_config directory with the target file name as application.properties.

For example: cp application.properties.sample <*MS_INSTALL_DIRECTORY*>/ms_config/application.properties

d. Copy the directory datacollection to the <*MS_INSTALL_DIRECTORY*>/ms_config location.

For example: cp -r datacollection <*MS_INSTALL_DIRECTORY*>/ms_config

e. Copy the LDAP.properties.sample file to the <*MS_INSTALL_DIRECTORY*>/ms_config location with the target file name as LDAP.properties.

For example: cp LDAP.properties.sample <*MS_INSTALL_DIRECTORY*>/ms_config/LDAP.properties

f. Copy the logging.properties.sample file to the location <*MS_INSTALL_DIRECTORY*>/ms_config with the target file name as logging.properties.

For example: cp logging.properties.sample <*MS_INSTALL_DIRECTORY*>/ms_config/logging.properties

g. Copy the ehcacheconfig.xml file to the <*MS_INSTALL_DIRECTORY*>/ms_config location.

For example: cp ehcacheconfig.xml<*MS_INSTALL_DIRECTORY*>/ms_config

h. Copy the cleWebexAdapterConfig-MC.properties.sample file to the location <*MS_INSTALL_DIRECTORY*>/ms_config with the target file name as cleWebexAdapterConfig-MC.properties.

For example: cp cleWebexAdapterConfig-MC.properties.sample<*MS_INSTALL_DIRECTORY*>/ms_config/

cleWebexAdapterConfig-MC.properties

Note You do not need to modify the properties in the timezone.properties and quartz files. You can use the default values provided for the properties in these files.

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	jnp**://**<*MS Appserver IP Address or hostname*>:<*MS Appserver port number*> For example, IB_JMSPROVIDER_URL=jnp://10.65.111.54:1199
IB_userName	MS JBoss profile admin userid. For example, IB_userName=admin
IB_password	MS JBoss profile admin password. For example, IB_password=admin
SDP_JMSPROVIDER_URL	jnp://<*SDP APP server IP Address or hostname*>:<*SDP Appserver port number*> For example, SDP_JMSPROVIDER_URL=jnp://10.65.111.54:1099
SDP_userName	SDP JBoss profile admin user ID. For example, SDP_userName=admin
SDP_password	SDP JBoss profile admin password. For example, SDP_password=admin
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 MS user portal.
working_hours	Number of working hours for a day in the enterprise.
REMINDERS: • showReminder1 • showReminder2 • showReminder3 • showReminder4	Number of minutes before the meeting when reminders will be send to all the invitees.
skin_name	Name of the skin folder for the MS user portal. For example, skin_name=red
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	http://*<MS Appserver IP Address or hostname>:<MS Appserver port number>/services/webcalendarservices/confDetails* For example, http://10.104.18.196:7010/services/webcalendarservices/confDetails
ps_serviceurl	http://*<PS Appserver IP Address or hostname>:<PS Appserver port number>/ipsapp* For example, http://10.104.18.196:8000/ipsapp
availablesoon	Time in minutes to change the status of the workspaces and rooms to available soon. For example, 25

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 worskpaces for this duration.

cronTriggerExpression	Time at which the LDAP user details will be synchronized with the Smart+Connected MS application. For example, 0 04 13 * * ?

Note The default cronTriggerExpression time is 12 am. You can change it as per your requirement.

user_preference_required	Show/hide the 'Do not publish my location' check box in the kiosk web portal. For example, ‘yes’ if you want to display the check box.

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	*<MS_INSTALL_DIRECTORY>*/ms_config/datacollection/unit.xml For example, datacollection.unitxml.path=/home/scc-qa/ms_config/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.
datacollection.jms.providerUrl	jnp**://**<*MS Appserver IP Address or hostname*>:<*MS Appserver port number*> For example, datacollection.jms.providerUrl=jnp://10.65.111.54:1199
datacollection.jms.securityPrincipal	MS JBoss admin console user name. For example, datacollection.jms.securityPrincipal=admin
datacollection.jms.securityCredentials	MS JBoss admin console password. For example, datacollection.jms.securityCredentials=admin
datacollection.data.precision	Data precision for the data collected by the BMS. For example, 0.00

b. Save and close the file.

Step 4 Update the LDAP.properties file:

a. Modify the properties as follows:

Table 2-3 LDAP Properties

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

Table 2-3 LDAP Properties (Continued)

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

Table 2-3 LDAP Properties (Continued)

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

Table 2-3 LDAP Properties (Continued)

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

Note You can modify only the mandatory properties listed in Table 2-3. Modify the non-mandatory properties if required.

b. Save and close the file.

Step 5 Modify the logging.properties file to update the directory in which the Smart+Connected MS log file needs to be generated:

a. Create the 'ms_log' folder under <*MS_INSTALL_DIRECTORY*> directory, and provide the read and write access.

b. Search for the line starting with `java.util.logging.FileHander.pattern` and replace it as follows:

```
java.util.logging.FileHandler.pattern=<MS_INSTALL_DIRECTORY>/ms_log/MS-%u.log
```

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

c. Save and close the file.

Step 6 Modify the ehcacheconfig.xml file to identify the cache configurations:

a. Search for the following text:

```
<cacheManagerPeerProviderFactory
class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
properties="peerDiscovery=manual,
rmiUrls=//<MS server IP address or hostname>:<Any free port that is above 1024. For
example, 4001>/sampleCache11|=//<MS server IP address or hostname>:4001/sampleCache12">
```

b. Replace with:

```
<cacheManagerPeerProviderFactory
class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
properties="peerDiscovery=manual,
rmiUrls=//<MS managed server IP address or hostname>:4001/ipphone.cache|//<MS managed
server IP address or hostname>:4001/subscription.cache|//<MS managed server IP address or
hostname>:4001/locationproperty.cache|//<MS managed server IP address or
hostname>:4001/timezone.cache|//<MS managed server IP address or
hostname>:4001/equipment.cache|//<MS managed server IP address or
hostname>:4001/iec.cache"/>
```

Step 7 Update the cleWebexAdapterConfig-MC.properties file:

a. Modify the mandatory properties as follows:

WEBEX_SITE_ID	For example, 98765432
WEBEX_SITE_NAME	For example, abcorp
WEBEX_PARTNER_ID	For example, 123ci
WEBEX_XML_SERVER_URL	For example, https://abcorp/WBXService/XMLService
WEBEX_USER	For example, WEBEX_USER=genuser
WEBEX_PASSWORD	For example, WEBEX_PASSWORD=Hilly!23
WEBEX_TIMEZONE	For example, EST

b. You can retain the default values for the following properties:

- WEBEX_ADMIN_USER
- WEBEX_ADMIN_PASSWORD
- TEMPLATE_PATH
- AUTH_TEMPLATE_NAME
- CREATE_USER_TEMPLATE_NAME
- UPDATE_USER_TEMPLATE_NAME
- RESET_PASSWORD_TEMPLATE_NAME
- DELETE_USER_TEMPLATE_NAME
- USER_MAPPING_TEMPLATE_NAME
- GET_USER_TEMPLATE_NAME
- CREATE_CONF_TEMPLATE_NAME
- UPDATE_CONF_TEMPLATE_NAME
- GET_CONF_SESSION_KEYS_TEMPLATE_NAME
- GET_CONF_TEMPLATE_NAME
- DELETE_CONF_TEMPLATE_NAME
- CONF_MAPPING_TEMPLATE_NAME
- GET_HOST_URL_TEMPLATE_NAME
- GET_JOIN_URL_TEMPLATE_NAME
- GET_RECORDING_URL_TEMPLATE_NAME
- GET_RECORDING_URL_SESSION_TEMPLATE_NAME
- DELETE_RECORDING_TEMPLATE_NAME
- CREATE_CONF_ATTENDEE_TEMPLATE_NAME
- SERVREASON
- SERVRESULT

- TICKET
- SUCCESS
- WEBEXID_ALREADY_EXISTS
- SESSIONKEY
- HOSTURL
- JOINURL
- CONFID
- OWNER
- SUBJECT
- CONFSTARTTIME
- CONFSTARTTIMEZONE
- DURATION
- PRESENTERS
- ATTENDEES
- PARTICIPANT_ID
- PARTICIPANT_EMAIL
- OCCURENCES
- BODY
- ROLE
- DAYINWEEK
- DAY_IN_MONTH
- MONTH_IN_YEAR
- WEEK_IN_MONTH
- DAY
- EPSESSION
- EPSESSIONKEY
- SERVTOTAL
- SERVRETURNED
- STREAM_URL
- CONF_STATUS
- USER_FIRSTNAME
- USER_LASTNAME
- USER_WEBEXID
- USER_EMAIL
- USER_REG_DATE
- USER_TYPE
- USER_PASSWORD
- USER_ACCOUNT_ID

- RECORDING_ID
- RECORDING_NAME
- RECORDING_CREATE_TIME
- RECORDING_STREAM_URL
- RECORDING_DOWNLOAD_URL
- RECORDING_CONFERENCE_ID
- RECORDING_TIMEZONE_ID
- RECORDING_HOST_ID
- RECORDING_DURATION

c. Save and close the file.

Setting up Webex

To configure the WebEx setup for the Smart+Connected MS user portal, perform the following steps:

Step 1 Navigate to the WebEx properties file in the Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear using the following path:

<*MS_INSTALL_DIRECTORY*>/pkg-apps/calendar.war/WEB-INF/classes/cleWebexAdapterConfig-MC.properties

Step 2 Replace the cleWebexAdapterConfig-MC.properties file in the ear with the cleWebexAdapterConfig-MC.properties file you updated in the "Updating the Properties Files" section on page 2-17.

Setting up Data Collection

To collect data from a Building Management System (BMS), you need to provide information on the 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 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 2-4 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.

Table 2-4 Metadata Properties (Continued)

Property	Purpose
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 MS application. Therefore, the value must be set to zero.
CUMULATIVE	Not applicable for the Smart+Connected MS application. Therefore, the value must be set to zero.
SCHEDULABLE	Not applicable for the Smart+Connected MS application. Therefore, the value must be set to zero.
CONTROLLABLE	Not applicable for the Smart+Connected MS application. Therefore, the value must be set to zero.
REPORTABLE	Not applicable for the Smart+Connected MS application. Therefore, the value must be set to zero.
ALARMABLE	Not applicable for the Smart+Connected MS 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.

Setting up Run Parameters

To set up run parameters, perform the following steps:

Step 1 Navigate to *$JBOSS_HOME*/bin, copy the ‘run.sh’ file, and create a file with the name ‘run_solutions.sh’.

Step 2 Configure the properties (quartz, data collection, application, LDAP, ehcacheconfig, timezone):

a. In the run_solutions.sh file, search for the following text:

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

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

```
-Dorg.quartz.properties=<path of the quartz.properties file>/quartz.properties
-DDataCollectionPropertyFilePath=<path of the dc.properties file>/dc.properties
-Dapplication.properties.filepath=<path of the application.properties
file>/application.properties
```

```
-Dcom.cisco.sdp.ldap.configfilepath=<path of the LDAP.properties file>/LDAP.properties
-Dib.cache.config=<path of the ehcacheconfig.xml file>/ehcacheconfig.xml
-Dtimezone.properties.filepath=<path of the
timezone.propertiesfile>/timezone.properties
```

For example:

```
-Dorg.quartz.properties=/home/scc-qa/ms_config/quartz.properties
-DDataCollectionPropertyFilePath=/home/scc-qa/ms_config/dc.properties
-Dapplication.properties.filepath=/home/scc-qa/ms_config/application.properties
-Dcom.cisco.sdp.ldap.configfilepath=/home/scc-qa/ms_config/LDAP.properties
-Dib.cache.config=/home/scc-qa/ms_config/ehcacheconfig.xml
-Dtimezone.properties.filepath=/home/scc-qa/ms_config/timezone.properties
```

Step 3 After adding the command line, the text is displayed as follows:

```
set JAVA_OPTS=-Dprogram.name=%PROGNAME% -
DANTLR_USE_DIRECT_CLASS_LOADING=true -
Dorg.quartz.properties=<MS_INSTALL_DIRECTORY>/ms_config/quartz.properties -
DDataCollectionPropertyFilePath=<MS_INSTALL_DIRECTORY>/ms_config/dc.properties -
Dapplication.properties.filepath=<MS_INSTALL_DIRECTORY>/ms_config/application.properti
es -
Dcom.cisco.sdp.ldap.configfilepath=<MS_INSTALL_DIRECTORY>/ms_config/LDAP.properties
Dib.cache.config=<MS_INSTALL_DIRECTORY>/ms_config/ehcacheconfig.xml
Dtimezone.properties.filepath=<MS_INSTALL_DIRECTORY>/ms_config/timezone.properties
-Dsdp.event.config.mode=global -Xms256m -Xmx1024m
-XX:MaxPermSize=512m -Dorg.jboss.resolver.warning=true
Dsun.rmi.dgc.client.gcInterval=3600000 -
Dsun.rmi.dgc.server.gcInterval=3600000
%JAVA_OPTS%
```

Step 4 Save and close the run_solutions.sh file.

Setting up Apache Jackrabbit

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

To set up Jackrabbit, perform the following steps:

Step 1 Copy the jackrabbit-jca-2.2.12.rar file that is available in <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to *$JBOSS_HOME*/server/<*server_name*>/deploy directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-jackrabbit/jackrabbit-jca-2.2.12.rar
$JBOSS_HOME/server/<server_name>/deploy
```

Step 2 Copy the jcr-2.0.jar file that is available in <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to *$JBOSS_HOME*/common/lib directory by entering the following command:

```
Cp <MS_INSTALL_DIRECTORY>/pkg-jackrabbit/jcr-2.0.jar $JBOSS_HOME/common/lib
```

Step 3 Copy the jcr-ds.xml file that is available in <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to *$JBOSS_HOME*/server/<*server_name*>/deploy directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-jackrabbit/jcr-ds.xml
$JBOSS_HOME/server/<server_name>/deploy
```

Importing SSL Certificates

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

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

To import SSL certificates, perform the following steps:

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

Step 2 Enter the following command:

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

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

For example:

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

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

A message prompts you to trust this certificate.

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

The certificates are imported.

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

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

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

```
set JAVA_OPTS=-Dprogram.name=%PROGNAME% -
DANTLR_USE_DIRECT_CLASS_LOADING=true -
Dorg.quartz.properties=<MS_INSTALL_DIRECTORY>/ms_config/quartz.properties -
DDataCollectionPropertyFilePath=<MS_INSTALL_DIRECTORY>/ms_config/dc.properties -
Dapplication.properties.filepath=<MS_INSTALL_DIRECTORY>/ms_config/application.properti
es -
Dcom.cisco.sdp.ldap.configfilepath=<MS_INSTALL_DIRECTORY>/ms_config/LDAP.properties
Dib.cache.config=<MS_INSTALL_DIRECTORY>/ms_config/ehcacheconfig.xml
Dtimezone.properties.filepath=<MS_INSTALL_DIRECTORY>/ms_config/timezone.properties
-Dsdp.event.config.mode=global -Xms256m
-Xmx1024 -XX:MaxPermSize=512m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000 -
Dsun.rmi.dgc.server.gcInterval=3600000
-Djavax.net.ssl.trustStore=/usr/java/default/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit"
 %JAVA_OPTS%
```

Step 5 Save the run_solutions.sh file.

Starting the JBoss Server

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

Step 1 Ensure that:

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

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

```
./run_solutions.sh -c solutions -Djboss.service.binding.set=ports-01 -b 0.0.0.0
```

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

```
2012-11-20 11:41:31,360 INFO  [org.apache.coyote.http11.Http11Protocol] (Thread-2)
Starting Coyote HTTP/1.1 on http-0.0.0.0-7259
```

The port value that appears in the output is the value obtained by adding the HttpConnector port value (which you had set up in "Setting Up Port" section on page 2-9) and the "ports-01" offset value in the bindings-jboss-beans.xml file (which is 100 by default).

Assigning Roles and Locations to the IB User

To access the Smart+Connected MS application, you need to assign roles and locations to the 'IBUser'. 'IBUser' is the default user that is created with the seed data.

You can assign roles and locations by performing the following tasks in the SDP:

- Assigning the InfoBundle Manager role to 'IBUser'.
- Assigning specific locations to the InfoBundle Manager role.

To assign roles and locations to 'IBUser' in the SDP, perform the following steps:

Step 1 Log in into the SDP application.

For more information on how to log in to the SDP application, see the *Cisco Service Delivery Platform Administrator Guide*.

Step 2 To assign the InfoBundle Manager role to 'IBUser', do the following:

a. Click the **Users & Roles** tab.

The List of Users area displays the 'IBUser'.

b. In the User Name column, click 'IBUser', and in the View User page, click **Edit**.

The Edit User page appears.

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

   The Select Roles for the Users dialog box appears. The Available Roles box lists the InfoBundle Manager role.

d. In the Available Roles column, select the InfoBundle Manager role, and click **Add**.

e. Click **Assign and Close**.

   The InfoBundle Manager role is assigned to 'IBUser' along with the associated permissions.

f. Click **Save**.

Step 3 To assign specific locations to the InfoBundle Manager role, do the following:

a. Ensure that the locations that you want to assign to the InfoBundle Manager role is already added in SDP.

b. In the Assigned Locations column of the Assign Roles and Locations area, click **Assign Locations** next to the InfoBundle Manager role.

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

c. In the location hierarchy, select a location that you want to associate to the InfoBundle Manager.

   You can use shortcut tools to search and select a location in the location hierarchy.

d. Click **Assign**.

   The selected location is assigned to the InfoBundle Manager.

e. Click **Save**.

Creating and Assigning Webcalendar Roles

To create users and assign Webcalendar User roles, perform the following steps:

Step 1 Log in into the SDP application.

For more information on how to log in to the SDP application, see the *Cisco Service Delivery Platform User Guide*.

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

The Create User page appears.

Step 3 Enter the user details and click **Save**.

For more information on how to create users, see the *Cisco Service Delivery Platform User Guide*.

Step 4 To assign the Webcalendar User role, do the following:

a. Click the **Users & Roles** tab.

   The List of Users area displays all the users.

b. In the User Name column, click the specific user, and in the View User page, click **Edit**.

   The Edit User page appears.

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

   The Select Roles for the Users dialog box appears. The Available Roles box lists the Webcalendar User role.

d. In the Available Roles column, select the Webcalendar User role, and click **Add**.

e. Click **Assign and Close**.

The Webcalendar User role is assigned along with the associated permissions.

f. Click **Save**.

Accessing the Application and Verifying the Installation

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

Step 1 In a web browser, type the application server URL, http://<*host*>:<*port*>/solutions.

Where <*host*> is the IP address or DNS hostname of the host on which the JBoss application server is set up and <*port*> is the value that appears in the output after starting the JBoss server.

Note The 'port' value is obtained by adding the HttpConnector port value (which you had set up in "Setting Up Port" section on page 2-9) and the "ports-01" offset value in the bindings-jboss-beans.xml file (which is 100 by default).

Step 2 Press **Enter**.

The Smart+Connected MS login page appears.

Step 3 Enter the username and password for the Smart+Connected MS 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 MS features, see the *Cisco Smart+Connected Meeting Spaces User Guide*.

Accessing the Web Calendar

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

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

Step 1 In a web browser, type the URL http://<*host*>:<*port*>/calendar/.

Where <*host*> is the IP address or DNS hostname of the host on which the JBoss application server is set up and <*port*> is the value that appears in the output after starting the JBoss server.

Step 2 Press **Enter**.

The Smart+Connected MS web calendar login page appears.

Step 3 Enter the username and password for the Smart+Connected MS 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 MS features, see the *Cisco Smart+Connected Meeting Spaces User Guide*.

Accessing the Kiosk Web Portal

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

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

Step 1 In a web browser, type the URL http://<*host*>:<*port*>/spaces/.

Where <*host*> is the IP address or DNS hostname of the host on which the JBoss application server is set up and <*port*> is the value that appears in the output after starting the JBoss server.

Step 2 Press **Enter**.

The Smart+Connected MS kiosk web portal login page appears.

Step 3 Enter the username and password for the Smart+Connected MS 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 MS features, see the *Cisco Smart+Connected Spaces User Guide*.

Installing on a Cluster Server Setup

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

1. About Clustering, page 2-35
1. Installing the Application, page 2-36
2. Configuring Audio Notification to the Cisco IP Phone, page 2-36
3. Configuring the Database, page 2-36
4. Configuring the JBoss Profile, page 2-37
5. Setting up Port, page 2-38
6. Setting up Security Configuration, page 2-38
7. Setting up Java Messaging Service (JMS), page 2-38
8. Setting up Library, page 2-38
9. Setting up Quartz, page 2-38

About Clustering

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

An example of clustered deployment in a distributed environment is explained below. It has the following constituents:

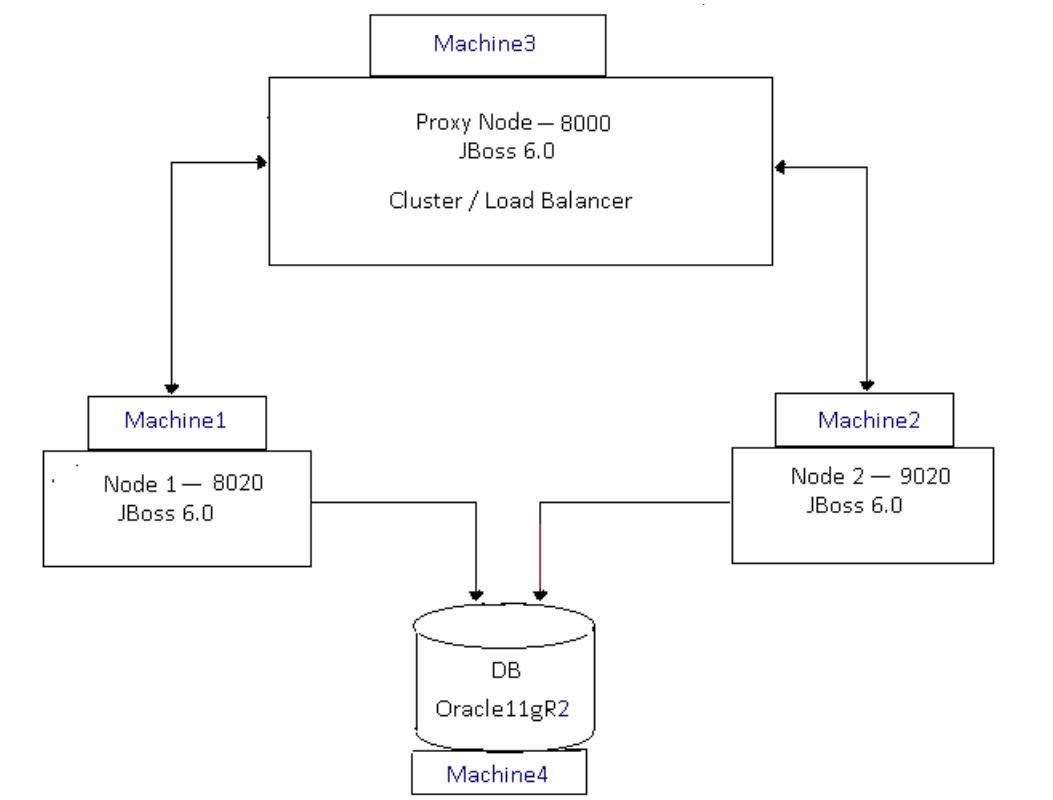
- Database is non-clustered.
- Application servers are clustered.
- Three virtual machines host the application servers.
- One virtual machine hosts the administrative server and a proxy server. This proxy server acts as a software load balancer.
- Application is deployed on two machines—Machine 1 and Machine 2—that has two managed servers.

You can modify this setup based on your requirement, such as the number of managed servers, port numbers, and so on.

An example of cluster setup is as follows:

- Machine 1: JBoss Managed Server 1 (JBoss 6.0)
- Machine 2: JBoss Managed Server 2 (JBoss 6.0)
- Machine 3: JBoss Admin Server and HTTP Proxy Server (JBoss 6.0)
- Machine 4: Database Server (Oracle Database 11gR2)

Figure 2-1 Example of a Clustering Setup



Installing the Application

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

For information on how to install the Smart+Connected MS application, see the "Installing the Application" section on page 2-3.

Configuring Audio Notification to the Cisco IP Phone

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

For information on how to configure audio notification to the Cisco IP phone, see the in "Configuring Audio Notification to IP Phone" section on page 3-3 in Chapter 3, "Configuring the Smart+Connected MS Application".

Configuring the Database

For information on how to configure the database, see the "Configuring the Database" section on page 2-4.

Configuring the JBoss Profile

You need to configure the JBoss profile on the Node 1 and Node 2 servers for a cluster deployment.

To configure the JBoss profile, perform the following steps on both the Node 1 and Node 2 servers:

Step 1 Download the jboss-6.0.0.Final.zip file.

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

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

Step 2 Create a folder named 'jboss', and unzip the jboss-6.0.0.Final.zip file into it.

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

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

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

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

Step 4 Copy the Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear file, available in <*MS_INSTALL_DIRECTORY*>pkg-apps, to the *$JBOSS_HOME*/server/all/deploy directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-apps/
Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear $JBOSS_HOME/server/all/deploy
```

Step 5 Create a datasource file so that the Smart+Connected MS application communicates with the database machine:

a. Create the oracle-ds.xml file under the 'all/deploy' folder with the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<local-tx-datasource>
<jndi-name>jdbc/scc</jndi-name>
<connection-url>jdbc:oracle:thin@IPaddress:1521/schemaName</connection-url>
<driver-class>oracle.jdbc.OracleDriver</driver-class>
<user-name>DBusername</user-name>
<password>DBpassword</password>
<min-pool-size>10</min-pool-size>
<max-pool-size>50</max-pool-size>
</local-tx-datasource>
</datasources>
```

b. Replace the following text with their actual values in the text that you had added in Step 5 a.:

- 'IPaddress' with the database server IP address or DNS hostname
- 'schemaName' with the database name
- '1521' with the database port number, if changed during the Oracle installation
- 'DBusername' with the database schema username
- 'DBpassword' with the database schema password

c. Save the file.

Step 6 Update the run.conf file to increase the memory:

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

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

Replace with the following text:

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

b. Save the file.

Setting up Port

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

For more information on how to set up the port, see the "Setting Up Port" section on page 2-9.

Setting up Security Configuration

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

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

For more information on how to set up security configuration on the Node 1 and Node 2 servers, see the "Setting Up Security Configuration" section on page 2-9.

Setting up Java Messaging Service (JMS)

For more information on how to set up JMS on the Node 1 and Node 2 servers, see the "Setting Up Java Messaging Service (JMS)" section on page 2-12.

Setting up Library

For more information on setting up library, see the "Setting Up Library" section on page 2-16.

Setting up Quartz

For more information on how to set up Quartz, see the "Setting Up Quartz" section on page 2-16.

Configuring Logging

For more information on how to configure logging on the Node 1 and Node 2 servers, see the "Configuring Logging" section on page 2-16.

Configuring the Cluster Server Setup

Installing mod_cluster on the Proxy Node

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

To install mod_cluster on the proxy node, perform the following steps:

Step 1 Create a directory in your local system where you want to install the mod_cluster binary bundle.

Step 2 Download the Linux 64-bit mod_cluster 1.1.0 bundle.

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

`http://www.jboss.org/mod_cluster/downloads.html`

Step 3 Save and untar the mod_cluster binary bundle in the directory that you had created in Step 1.

The directory where you have extracted the mod_cluster bundle is referred as *<MOD_CLUSTER_HOME>*.

Step 4 Navigate to the *<MOD_CLUSTER_HOME>*/opt/jboss/httpd/sbin folder and run the “installhome.sh” file.

The httpd now runs on port “8000”.

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

a. Navigate to the following location:

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

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

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

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

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

d. Save the file.

Note By default, mod_cluster communicates only with the server instances that run on localhost. Step 5 should be performed to allow mod_cluster to communicate with the proxy.

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

a. Navigate to the following location:

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

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

```
<IfModulemanager_module>
  Listen 127.0.0.1:6666
ManagerBalancerNamemycluster
<VirtualHost 127.0.0.1:6666>
<Directory />
     Order deny,allow
     Allow from all
</Directory>

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

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

</VirtualHost>
</IfModule>
```

c. Replace the directory access of the Manager Module in the <Location /mod_cluster_manager> element as follows:

```
<Location /mod_cluster_manager>
SetHandlermod_cluster-manager
       Order deny,allow
       Allow from all
</Location>
```

After replacing, the text is displayed as follows:

```
<IfModulemanager_module>
  Listen 127.0.0.1:6666
ManagerBalancerNamemycluster
<VirtualHost 127.0.0.1:6666>
<Directory />
     Order deny,allow
     Allow from all
</Directory>

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

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

</VirtualHost>
</IfModule>
```

d. Save and close the file.

Configuring Cluster on Nodes

To ensure high availability, you must configure cluster on the nodes. To configure cluster on nodes, perform the following steps on the Node 1 and Node 2 servers:

Step 1 Update the server.xml file:

a. Navigate to the *$JBOSS_HOME*/server/solutions/deploy/jbossweb.sar folder, and open the server.xml file.

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

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

c. Add jvmRoute to the Engine "jboss.web". For example:

- For Node 1:

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

- For Node 2:

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

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

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

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

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

1. Search for the following text:

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

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

f. Save the server.xml file.

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

a. In a file browser, navigate to the $*JBOSS_HOME*/server/solutions/deploy/mod_cluster.sar/META_INF folder.

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

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

c. Add proxies in the proxyList property as follows:

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

Note In the proxyList property format, the "address:port" refers to the host IP address and port where the proxy is running. The port number is 8000 that you had configured in Step 4 in the "Installing mod_cluster on the Proxy Node" section on page 2-39.

d. Save the mod_cluster-jboss-beans.xml file.

Configuring the Properties Files

Updating the Properties Files

To update the application.properties, dc.properties, LDAP.properties, logging.properties, cleWebexAdapterConfig-MC.properties, and ehcacheconfig.xml files, perform the following steps:

Step 1 Copy the properties files from <*MS_INSTALL_DIRECTORY*> to a local directory.

a. Create a folder with the name 'ms_config' under the directory in which the Smart+Connected MS & DS application is set up, and assign the read and write permissions.

b. Open a terminal and navigate to <*MS_INSTALL_DIRECTORY*>/pkg-properties, where <*MS_INSTALL_DIRECTORY*> is the location at which the Smart+Connected MS & DS application is installed.

c. Copy the application.properties.sample file to the <*MS_INSTALL_DIRECTORY*>/ms_config directory with the target file name as application.properties.

For example: cp application.properties.sample <*MS_INSTALL_DIRECTORY*>/ms_config/application.properties

d. Navigate to <*MS_INSTALL_DIRECTORY*>/pkg-properties/ and copy the directory datacollection to the <*MS_INSTALL_DIRECTORY*>/ms_config location.

For example: cp -r datacollection <*MS_INSTALL_DIRECTORY*>/ms_config

e. Copy the LDAP.properties.sample file to the <*MS_INSTALL_DIRECTORY*>/ms_config location with the target file name as LDAP.properties.

For example: cp LDAP.properties.sample <*MS_INSTALL_DIRECTORY*>/ms_config/LDAP.properties

f. Navigate to <*MS_INSTALL_DIRECTORY*>/pkg-properties/logging and copy the logging.properties.sample file to the location <*MS_INSTALL_DIRECTORY*>/ms_config with the target file name as logging.properties.

For example: cp logging.properties.sample <*MS_INSTALL_DIRECTORY*>/ms_config/logging.properties

g. Navigate to <*MS_INSTALL_DIRECTORY*>/pkg-properties and copy the cleWebexAdapterConfig-MC.properties.sample file to the location <*MS_INSTALL_DIRECTORY*>/ms_config with the target file name as cleWebexAdapterConfig-MC.properties.

For example: cp cleWebexAdapterConfig-MC.properties.sample<*MS_INSTALL_DIRECTORY*>/ms_config/cleWebexAdapterConfig-MC.properties

h. Navigate to <MS_INSTALL_DIRECTORY>/pkg-properties/ and copy the ehcacheconfig.xml file to the <*MS_INSTALL_DIRECTORY*>/ms_config location.

For example: cp ehcacheconfig.xml<*MS_INSTALL_DIRECTORY*>/ms_config

Note You do not need to modify the properties in the timezone.properties and quartz files. You can use the default values provided for the properties in these files.

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	jnp://<*MS managed server IP Address or hostname*>:<*MS managed server port number*> For example, • For managed server 1: IB_JMSPROVIDER_URL=jnp://10.65.111.54:8020 • For managed server 2: IB_JMSPROVIDER_URL=jnp://10.65.111.55:9020
IB_userName	MS JBoss profile admin userid For example, IB_userName=admin
IB_password	MS JBoss profile admin password For example, IB_password=admin
SDP_JMSPROVIDER_URL	jnp://<*SDP APP server IP Address or hostname*>:<*SDP Appserver port number*> For example, SDP_JMSPROVIDER_URL=jnp://10.65.111.56:7001
SDP_userName	SDP JBoss profile admin userid For example, SDP_userName=admin
SDP_password	SDP JBoss profile admin password For example, SDP_password=admin

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 MS user portal.
working_hours	Number of working hours for a day in the enterprise.
REMINDERS: • showReminder1 • showReminder2 • showReminder3 • showReminder4	Number of minutes before the meeting when reminders will be send to all the invitees.
skin_name	Name of the skin folder for the MS user portal For example, skin_name=red
maps_theme	Color of the theme for the floor maps displayed on the kiosk. The default color is grey. You can change it to blue.
ms_serviceurl	http://*<MS managed server IP Address or hostname>:<MS managed server port number>*/services/webcalendarservices/confDetails For example, • For managed server 1: ms_serviceurl=http://10.65.111.54:8020/services/webcalendarservices/confDetails For managed server 2: ms_serviceurl=http://10.65.111.55:9020/services/webcalendarservices/confDetails
ps_serviceurl	http://*<PS Appserver IP Address or hostname>:<PS Appserver port number>/ipsapp* • For managed server 1: ps_serviceurl=http://10.104.18.195:8000/ipsapp • For managed server 2: ps_serviceurl=http://10.104.18.196:9000/ipsapp

availablesoon	Time in minutes to change the status of the workspaces and rooms to available soon. For example, 25

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.

cronTriggerExpression	The time at which the LDAP user details will be synchronized with the Smart+Connected MS application. For example, 0 04 13 * * ?

Note The default cronTriggerExpression time is 12 am. You can change it as per your requirement.

user_preference_required	Show/hide the 'Do not publish my location' check box in the kiosk web portal. For example, yes

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	*<MS_INSTALL_DIRECTORY>*/ms_config/datacollection/unit.xml For example, datacollection.unitxml.path=/home/scc-qa/ms_config/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.

datacollection.jms.providerUrl	jnp://<*MS managed server IP Address or hostname*>:<*MSmanaged server port number*> For example, • For Managed Server1: datacollection.jms.providerUrl=jnp://10.65.111.54:8020 • For Managed Server2: datacollection.jms.providerUrl=jnp://10.65.111.55:9020
datacollection.jms.securityPrincipal	MS JBoss admin console user name For example, datacollection.jms.securityPrincipal=admin
datacollection.jms.securityCredentials	MS JBoss admin console password For example, datacollection.jms.securityCredentials=admin
datacollection.data.precision	Data precision for the data collected by the BMS. For example, 0.00

b. Save and close the file.

Step 4 Update the LDAP.properties file. For more information, see Step 4 in the "Updating the Properties Files" section on page 2-17.

Step 5 Modify the logging.properties file to update the directory in which the MS application log file needs to be generated. For more information, see Step 5 in the "Updating the Properties Files" section on page 2-17.

Step 6 Modify the ehcacheconfig.xml file to identify the cache configurations:

a. Search for the following text:

```
<cacheManagerPeerProviderFactory
class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
properties="peerDiscovery=manual,
rmiUrls=//server1:4001/sampleCache11|=//server2:4001/sampleCache12">
```

b. Replace with:

```
<cacheManagerPeerProviderFactory
class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
properties="peerDiscovery=manual,
rmiUrls=//<MS managed server IP address or hostname>:40001/ipphone.cache|//<MS managed
server IP address or hostname>:4001/subscription.cache|//<MS managed server IP address or
hostname>:4001/locationproperty.cache|//<MS managed server IP address or
hostname>:4001/timezone.cache|//<MS managed server IP address or
hostname>:4001/equipment.cache|//<MS managed server IP address or
hostname>:4001/iec.cache"/>
```

For example:

- For Managed Server1:

  MS managed server IP address or hostname=Managed Server2 IP Address or hostname
- For Managed Server2:

  MS managed server IP address or hostname=Managed Server1 IP Address or hostname

Step 7 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
WEBEX_PASSWORD	For example, WEBEX_PASSWORD=Hilly!23
WEBEX_TIMEZONE	For example, EST

b. You can retain the default values for the other properties in the cleWebexAdapterConfig-MC.properties file. For more information, see the Step 7 b. in the "Updating the Properties Files" section on page 2-17.

c. Save and close the file.

Setting up WebEx

To configure the WebEx setup for the Smart+Connected MS user portal, perform the following steps:

Step 1 Navigate to the WebEx properties file in the Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear using the following path:

<*MS_INSTALL_DIRECTORY*>/pkg-apps/calendar.war/WEB-INF/classes/cleWebexAdapterConfig-MC.properties

Step 2 Replace the cleWebexAdapterConfig-MC.properties file in the ear with the cleWebexAdapterConfig-MC.properties file you updated in the "Configuring the Properties Files" section on page 2-42.

Setting up Data Collection

You must set up data collection to gather the data which the Green Advisor module in Smart+Connected MS uses to display reports. For information on how to set up data collection, see the "Setting up Data Collection" section on page 2-27.

Setting Up Apache Jackrabbit

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

To set up Jackrabbit, perform the following steps:

Step 1 Copy the jackrabbit-jca-2.2.12.rar file that is available in <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to the *$JBOSS_HOME*/server/<*server_name*>/deploy directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-jackrabbit/jackrabbit-jca-2.2.12.rar
$JBOSS_HOME/server/<server_name>/deploy
```

Step 2 Copy the jcr-2.0.jar file that is available in <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to *$JBOSS_HOME*/common/lib directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-jackrabbit/jcr-2.0.jar $JBOSS_HOME/common/lib
```

Step 3 Copy the jcr-ds.xml file that is available in <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to *$JBOSS_HOME*/server/<*server_name*>/deploy directory by entering the following command:

```
cp <MS_INSTALL_DIRECTORY>/pkg-jackrabbit/jcr-ds.xml
$JBOSS_HOME/server/<server_name>/deploy
```

Step 4 Repeat Step 1 through Step 3 on the Node 2 server.

Configuring the Jackrabbit Repository

You need to configure the Jackrabbit repository for the application to use the Jackrabbit content management system. To configure the Jackrabbit repository, provide the DB host IP address, DB port number (default 1521), DB schema name, MS schema username, and MS schema password.

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

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

Step 2 Search for the below text:

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

Replace with:

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

Step 3 Search for the below text:

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

Replace with:

```
 <DataStore class="org.apache.jackrabbit.core.data.db.DbDataStore">
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>/<db
schemaName>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="databaseType" value="oracle"/>
<param name="driver" value="oracle.jdbc.driver.OracleDriver"/>
<param name="minRecordLength" value="1024"/>
<param name="copyWhenReading" value="true"/>
<param name="tablePrefix" value=""/>
<param name="schemaObjectPrefix" value="D_1_"/>
<param name="schemaCheckEnabled" value="true"/>
 </DataStore>
```

Step 4 Search for the below text:

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

Replace with:

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

Step 5 Search for the below text:

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

Replace with:

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

Step 6 Add the following text at the end of the preceding text:

```
 <Cluster id ="node1" syncDelay = "1000">
        <Journal class="org.apache.jackrabbit.core.journal.DatabaseJournal">
        <param name="driver" value="oracle.jdbc.driver.OracleDriver"/>
        <param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port
 number>/<db schemaName>"/>
        <param name="schema" value="oracle"/>
        <param name="user" value="<schema username>"/>
```

```
        <param name="password" value="<schema password>3"/>
        <param name="schemaObjectPrefix" value="C_1_"/>
        </Journal>
</Cluster>
```

Note Change the cluster ID accordingly for each node. For example, “node1” for the Node 1 server, “node2” for the Node 2 server, so on.

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

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

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

Step 9 Start the proxy on the proxy node and JBoss on the Node 1 and Node 2 servers, and verify that 13 new tables and two new sequences have been created in the database.

These tables and sequences have names starting with c_1_, d_1_, f_1_, v_1_, w_1_, and so on.

Importing SSL Certificates

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

For information on how to import SSL certificates on the Node 1 and Node 2 servers, see the “Importing SSL Certificates” section on page 2-30.

Assigning Roles and Locations to IBUser

To access the Smart+Connected MS application, you need to assign roles and locations to the ‘IBUser’. ‘IBUser’ is the default user that is created with the seed data.

For more information on how to assign roles and locations to ‘IBUser’, see the “Assigning Roles and Locations to the IB User” section on page 2-31.

Creating and Assigning Webcalendar Roles

For more information on how to create and assign webcalendar roles, see the Creating and Assigning Webcalendar Roles, page 2-32.

Starting the Cluster and Proxy

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

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

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

b. Using a terminal session, navigate to the *$JBOSS_HOME*/bin directory.

c. Enter the following command to start each node in the cluster:

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

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

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

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

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

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

b. Enter the following command to start the proxy:

```
./apachectl start
```

c. Click **Enter**.

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

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

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

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

b. Enter the following command to stop the proxy:

```
./apachectl stop
```

c. Click **Enter**.

Accessing the Application

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

Step 1 In a web browser, type the URL http://<*proxy IP address*>:<*proxy port*>/solutions.

Where <proxy IP address> is the host IP address or DNS hostname of the proxy server and <proxy port> refers to the port number (default 8000) that you defined for the proxy server in Step 4 in the "Installing mod_cluster on the Proxy Node" section on page 2-39.

Step 2 Press **Enter**.

The Smart+Connected MS login page appears.

Step 3 Enter the username and password for the Smart+Connected MS 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 MS features, see the *Cisco Smart+Connected Meeting Spaces User Guide*.

Accessing the Web Calendar

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

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

Step 1 In a web browser, type the URL http://<*proxy IP address*>:<*proxy port*> /calendar.

Where 'proxy ip address' is the host IP address or DNS hostname of proxy server and port refers to the port number (default 8000) that you have defined for the proxy server in Step 4 in the "Installing mod_cluster on the Proxy Node" section on page 2-39.

Step 2 Press **Enter**.

The Smart+Connected MS login page appears.

Step 3 Enter the username and password for the Smart+Connected MS 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 MS features, see the *Cisco Smart+Connected Meeting Spaces User Guide*.

Accessing the Kiosk Web Portal

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

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

Step 1 In a web browser, type the URL http://<*proxy IP address*>:<*port*>/spaces/.

Where 'proxy ip address' is the host IP address or DNS hostname of proxy server and port refers to the port number (default 8000) that you have defined for the proxy server in Step 4 in the "Installing mod_cluster on the Proxy Node" section on page 2-39.

Step 2 Press **Enter**.

The Smart+Connected MS kiosk web portal login page appears.

Step 3 Enter the username and password for the Smart+Connected MS 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 MS features, see the *Cisco Smart+Connected Spaces User Guide*.