Installing the Smart+Connected MS & DS on WebLogic

This chapter describes how to install the Cisco Smart+Connected Meeting Spaces & Cisco Smart+Connected Digital Signage (Smart+Connected MS & DS) application by using the Oracle database and WebLogic application server.

After successfully installing the Smart+Connected MS & DS application, you can configure the application by performing tasks that are listed in Chapter 3, "Configuring the Smart+Connected MS & DS 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
  - Database schema username
  - Database schema password
  - SSH credentials

    These credentials are required to access the machine. This account needs to be able to run SQLPlus.
- Application Server details:

- Location of the WebLogic directory, if the WebLogic Server has been pre-installed. If not, then you require the preferred path to set up the WebLogic server.
- SSH credentials

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

Verifying Network Configurations

Verify the following network configuration:

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

Installing on a Colocated or Non-Cluster Server Setup

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

1. Installing the Application, page 2-2
2. Configuring the Database, page 2-3
3. Creating a WebLogic 11g Domain, page 2-7
4. Extending the WebLogic 11g Domain, page 2-8
5. Configuring the Property Files, page 2-9
6. Starting the WebLogic Server, page 2-11
7. Deploying the Apache Jackrabbit and the Smart+Connected MS & DS Application, page 2-12
8. Importing SSL Certificates, page 2-12
9. Restarting the WebLogic Server, page 2-13
10. Assigning Roles and Locations to IBUser, page 2-14
11. Accessing the Smart+Connected MS & DS Application, page 2-15
12. Accessing the Web Calendar, page 2-16

Installing the Application

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

Before you begin the installation, do the following:

- Copy the WebLogic installer file (install.bin) from the WebLogic folder 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 appears.

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 & DS 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-properties
- pkg-scripts
- pkg-templates

Configuring the Database

You must configure a database for the Smart+Connected MS & DS environment.

- Requirements, page 2-4
- About the Database Scripts, page 2-4

Requirements

Before configuring the database, ensure that the following requirements are met:

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

  This document does not include information on how to set up the Oracle database. For more information, see the Oracle documentation.
- A database user is created with the following grants:
  - connect
  - create table
  - create procedure
  - create sequence
  - create trigger
  - create view
  - create job

  For more information on how to create users and provide grants, see the Oracle documentation.
- The following SDP database SQL scripts have been executed:
  - setup-sdp-base.sql
  - setup-sdp-types.sql

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

  <SDP_INSTALL_DIRECTORY>/sdp/

  For more information on how to execute the SDP database scripts, see the *Cisco Service Delivery Platform Installation Guide*.

About the Database Scripts

SDP Database Scripts

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 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 for the locations to the SuperAdmin (super administrator).
setup-sdp-types.sql	Loads the device types and device properties data.

Application Database Scripts

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

Script	Description
clean-Smart_Connected_Meeting_Spaces_and_Digital_Signage-objects.sql	Cleans all Smart+Connected MS & DS related objects from the user schema. Executing this script is not necessary if you are installing the application for the first time.
setup-Smart_Connected_Meeting_Spaces_and_Digital_Signage-base.sql	• Creates 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 tables, constraints, sequences, and indexes. • Loads the basic data that is required to bootstrap the application in Korean.

Executing Database Scripts

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

Ensure that you have the 'read' permission to run the scripts. You can execute the SQL scripts by using SQL *Plus or SQL Developer. After the database scripts have been executed, the necessary objects are created in the database schema.

To execute the database scripts by using the SQL *Plus, 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 & DS 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.

Configuring the Non-Touch IP Phones

By default, the Smart+Connected MS & DS application supports touchscreen IP phones. To enable text-based menu display on non-touchscreen IP phones, you must configure the non-touchscreen IP phones.

To configure the non-touch IP phones, enter the following details in the SSP_MOBILE table, which is available in the database schema you created earlier:

- HEADER_NAME—x-CiscoIPPhoneModelName
- HEADER_VALUE—Model Name
- SCREEN_MODE—Menu

These values are case-sensitive.

```
INSERT INTO SSP_MOBILE (MOBILE_DEVICE_ID, MOBILE_DEVICE_NAME, BROWSER_NAME,HEADER_NAME,
HEADER_VALUE, SCREEN_MODE,IMAGE_PATH, CREATED_BY, CREATED_DT, UPDATED_BY,UPDATED_DT,
TENANT_ID) VALUES (1,'Cisco IP Phone','All','x-CiscoIPPhoneModelName','CP-
9951','Menu',null,'superadmin',SYSDATE,'superadmin',SYSDATE,0);
COMMIT;
```

Creating a WebLogic 11g Domain

You must create a WebLogic domain where the Smart+Connected MS & DS application will be deployed. To create a WebLogic domain, perform the following steps:

Step 1 Launch the WebLogic Configuration wizard:

a. Navigate to <*BEA_HOME*>/wlserver_10.3/common/bin directory, where <*BEA_HOME*> is the location at which WebLogic is installed.

b. Run the **config.sh** file.

The Configuration wizard appears.

Step 2 Choose Create a new WebLogic domain and click **Next**.

The Select Domain Source screen appears.

Step 3 Choose **Generate a domain configured automatically to support the following products**, and click **Next**.

The Specify Domain Name and Location screen appears. Specify the domain and location for the domain.

Step 4 Enter a domain name in the Domain Name field. For example, MSDS.

Step 5 Browse for or enter the path where you want to save the domain and then click **Next**.

Note It is recommended that you create the domain at the default location.

The Configure Administrator User Name and Password screen appears.

Step 6 Enter the administrator username, password, confirm password, and description in the corresponding fields and click **Next**.

The Configure Start Mode and JDK screen appears.

Step 7 In the Select JDK and Start Mode screen, do the following:

a. Under WebLogic Domain Startup Mode, choose Production Mode.

b. Under Available JDKs, choose **Sun SDK 1.6.0_24**.

c. Click **Next**.

The Optional Configuration Screen appears.

Step 8 Select the Administration Server check box and then click **Next**.

The Configure the Administration Server screen appears.

Step 9 Enter the details and click **Next**.

Step 10 If you want to use the default port 7001, click **Next**. If you want to change the port from 7001, enter the new port number, and click **Next**.

The Configuration Summary screen appears.

Step 11 Review the details and click **Create**.

A new WebLogic domain is created.

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

Extending the WebLogic 11g Domain

After creating the WebLogic 11g domain, you must extend it by using the domain template that is provided with the MS & DS application. Ensure that you have prepared the database for the application.

To extend the Oracle WebLogic server domain using the domain template, perform the following steps:

Step 1 Navigate to <*BEA_HOME*>/wlserver_10.3/common/bin, where <*BEA_HOME*> is the location at which WebLogic is installed and run the **config.sh** command in the command mode. For example, **./configu.sh -mode=console**.

The console mode that displays options to either create or extend the WebLogic domain appears.

Step 2 Select the option to extend the WebLogic domain and press **Enter**.

Step 3 From the list of domain directories, choose the domain directory and press **Enter**.

Step 4 Select the option to choose the custom template and press **Enter**.

Step 5 Enter the path to the domain template and press **Enter**.

The path of the domain template is <MS_INSTALL_DIRECTORY>/pkg-templates/scmsdomain.jar, where <MS_INSTALL_DIRECTORY> is the location at which you have installed the Smart+Connected MS & DS application

Step 6 Select the option to modify the Data Sources and press **Enter**.

Step 7 Select the option to modify the DBMS name, enter the database SID, and press **Enter**.

Step 8 Select the option to modify the DBMS host name, enter the database host IP address or the DNS hostname, and press **Enter**.

Step 9 Select the option to modify the DBMS port number, enter the database port number (default port for Oracle is 1521), and press **Enter**.

Step 10 Select the option to modify the username, enter the schema username, and press **Enter**.

Step 11 Select the option to modify the password, enter the schema password, and press **Enter**.

Step 12 Select the option to confirm the password, enter the schema password, and press **Enter**.

Step 13 Press **Accept**.

Step 14 A confirmation message requesting you to proceed appears. Press **Yes**.

The WebLogic domain is successfully extended.

Configuring the Property Files

Updating the Properties Files

To update the application.properties, dc.properties, and logging.properties files, perform the following steps:

Step 1 Navigate to the <*BEA_HOME*>/user_projects/domains/<DOMAIN NAME>/properties folder.

Step 2 Update the application.properties file:

a. Modify the properties as follows:

IB_JMSPROVIDER_URL	t3**://**<*MS Appserver IP Address or hostname*>*:*<*MS Appserver port number*> For example, IB_JMSPROVIDER_URL=t3://10.65.111.54:8001
IB_userName	<*MS weblogic domain admin userid*> For example, IB_userName=weblogic
IB_password	<*MS weblogic domain admin password*> For example, IB_password=weblogic
SDP_JMSPROVIDER_URL	t3://<*SDP APP server IP Address or hostname*>:<*SDP Appserver port number*> For example, SDP_JMSPROVIDER_URL=t3://10.65.111.54:7001
SDP_userName	<*SDP weblogic console user name*> For example, SDP_userName=weblogic
SDP_password	<*SDP weblogic console password*> For example, SDP_password=weblogic

b. Save and close the file.

Step 3 Update the dc.properties file:

a. Modify the properties as follows:

datacollection.jms.providerUrl	t3**://**<*MS Appserver IP Address or hostname*>*:*<*MS Appserver port number*> For example, datacollection.jms.providerUrl=t3://10.65.111.54:8001
datacollection.jms.securityPrincipal	<*MS weblogic console user name*> For example, datacollection.jms.securityPrincipal=weblogic

datacollection.jms.securityCredentials	*<MS weblogic console password>* For example, datacollection.jms.securityCredentials=weblogic
datacollection.unitxml.path=	*<MS_INSTALL_DIRECTORY>*/ms_config/datacollection/unit.xml For example, datacollection.unitxml.path=/home/scc-qa/ms_config/datacollection/unit.xml

b. Save and close the file.

Step 4 Modify the logging.properties file to update the directory in which the MS & DS Application 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.

Setting up Data Collection

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

Every device added in the SDP has a unique property ID. For historic trending, reporting and policies for system generated alarms, the solution uses data collection tables and metadata table of Data Collection Schema. The collected data is mapped to the associated location and device instance.

Table 2-3 Metadata Properties

Property	Purpose
METADATA_ID	Primary key field of the table.
PROPERTY_VALUE_ID	Used to derive the id from the SSP_DEVICE_PROPERTY table which is unique across all the devices. It should be added in the SSP_DEVICE_PROPERTY_METADATA table.
TRENDABLE	If the trendable property is set to one, the data collector collects data for the property at the specified trend frequency.
TREND_FREQUENCY	Used to set the rate of data collection. Unit of measurement is minutes. The minimum value that can be provided is one minute.

Table 2-3 Metadata Properties (continued)

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

Starting the WebLogic Server

You need to start the WebLogic server after completing all the above tasks, such as installing the Smart+Connected MS & DS application, configuring the database, setting up the WebLogic domain, and so on.

To start the WebLogic server, perform the following steps:

Step 1 In a terminal session, navigate to the following location:

<*BEA_HOME*>/user_projects/domains/<*your domain*>/bin, where <*BEA_HOME*> is the location at which WebLogic is installed.

Step 2 Use the following command to start the WebLogic server:

```
./startWebLogic.sh
```

When prompted, enter the username and password that you provided while creating the domain. For example, weblogic/weblogic.

Deploying the Apache Jackrabbit and the Smart+Connected MS & DS Application

To deploy the Apache Jackrabbit and the Smart+Connected MS & DS application, perform the following steps:

Step 1 Copy the jackrabbit-jca-2.2.8.rar from <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit to solutions domain library (<*BEA_HOME*>/scms/bin/apps).

Step 2 Copy the Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear file from <*MS_INSTALL_DIRECTORY*>/pkg-apps folder, to solutions domain library (<*BEA_HOME*>/scms/bin/apps)

Note <*BEA_HOME*> is the location at which WebLogic is installed, and <*MS_INSTALL_DIRECTORY*> is the location at which the Smart+Connected MS & DS application is installed.

Step 3 Restart the WebLogic server.

For information, see the "Restarting the WebLogic Server" section on page 2-34.

Importing SSL Certificates

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

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

To import the SSL certificates, perform the following steps:

Step 1 In a terminal session, navigate to the directory <*JAVA_HOME*>/bin, where <*JAVA_HOME*> is the location at which JDK is installed.

Step 2 Execute the following command:

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

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

For example:

- CUCM—./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
- DMP—./keytool -import -alias DMP -file /home/scc-qa/DMP.cer -keystore /home/scc-qa/Desktop/jdk1.6.0_24/jre/lib/security/cacerts -storepass changeit
- IEC—./keytool -import -alias IEC -file /home/scc-qa/IEC.cer -keystore /home/scc-qa/Desktop/jdk1.6.0_24/jre/lib/security/cacerts -storepass changeit

- Exchange Server—./keytool -import -alias EXCH -file /home/scc-qa/EXCH.cer -keystore /home/scc-qa/Desktop/jdk1.6.0_24/jre/lib/security/cacerts -storepass changeit

Note If you have installed JDK 1.6 update 24 using an RPM binary bundle, you need SUDO access to add the certificate to the keystore.

A message is displayed that prompts you to trust this certificate.

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

The certificates are imported.

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

```
-Dweblogic.net.proxyAuthenticatorClassName=java.net.Authenticator
-Djavax.net.ssl.trustStore=<JAVA_HOME>/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

For example:

```
-Dweblogic.net.proxyAuthenticatorClassName=java.net.Authenticator
-Djavax.net.ssl.trustStore=/usr/java/default/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

Step 5 Restart the WebLogic server.

Restarting the WebLogic Server

You must restart the WebLogic server if you have made any changes through the WebLogic console or any configuration changes that require a restart of the server.

To restart the WebLogic server, perform the following steps:

Step 1 In a terminal session, navigate to the following location:

<*BEA_HOME*>/user_projects/domains/<*your domain*>/bin, where <*BEA_HOME*> is the location at which WebLogic is installed.

Step 2 Stop the WebLogic server using the following command:

```
./stopWebLogic.sh
```

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

```
./startWebLogic.sh
```

When prompted, enter the username and password that you provided while creating the domain. For example, weblogic/weblogic.

Assigning Roles and Locations to IBUser

To access the Smart+Connected MS & DS 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 User 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 Smart+Connected MS & DS Application

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

Step 1 In a Web browser, type the URL http://<*host*>:<*port*>/solutions/, where <*host*> is the host IP address or DNS hostname and <*port*> is the port number of the Weblogic application server.

Step 2 Press **Enter**.

The Smart+Connected MS & DS Login page appears.

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

Accessing the Web Calendar

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

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

Step 1 In a Web browser, type the URL http://<*host*>:<*port*>/calendar/, where <*host*> is the host IP address or DNS hostname and <*port*> is the port number of the WebLogic application server.

Step 2 Press **Enter**.

The Smart+Connected MS & DS Login page appears.

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

Installing on a Cluster Server Setup

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

1. Installing the Application, page 2-18
2. Configuring the Smart+Connected MS & DS Database, page 2-18
3. Configuring the JAVA File, page 2-19
4. Setting up Managed Servers, page 2-19
5. Creating WebLogic Domain for Admin/Proxy Server, page 2-26
6. Extending WebLogic Domain for Admin/Proxy Server, page 2-28
7. Starting the Administrative Server, page 2-29
8. Configuring the Cluster, page 2-29
9. Deploying Apache Jackrabbit, page 2-34
10. Deploying the Smart+Connected MS & DS Application, page 2-35
11. Starting Managed Server and Proxy Server, page 2-35
12. Starting Application/Cluster Services, page 2-36
13. Configuring the Apache Jackrabbit Repository, page 2-36
14. Importing SSL Certificates, page 2-39
15. Assigning Roles and Locations to IBUser, page 2-39
16. Accessing the Application, page 2-39
17. Accessing the Web Calendar, page 2-39

About Clustering

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

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

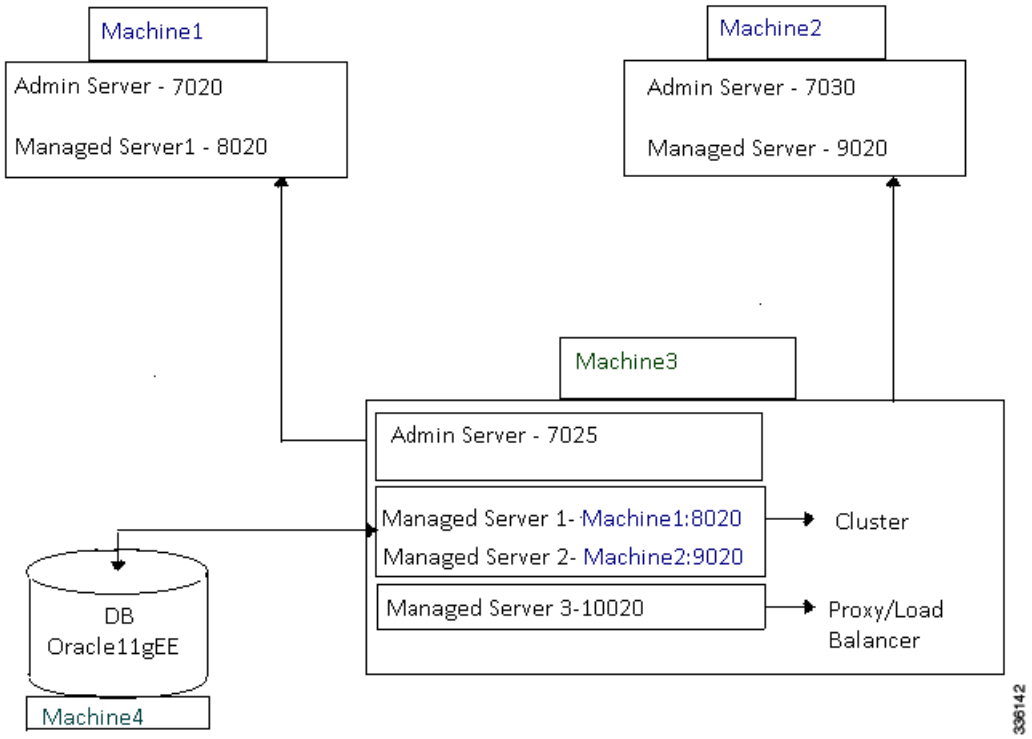
- Database is non-clustered.
- Application servers are clustered.
- Three virtual machines host the application servers.
- One of the virtual machines hosts the administrative server and a proxy server. This proxy server acts as a software load balancer.
- Application is deployed on two machines—Machine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

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

An example of cluster setup is as follows:

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

Figure 2-1 Clustering in a Distributed Setup



Installing the Application

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

Configuring the Smart+Connected MS & DS Database

For information on how to configure the Smart+Connected MS & DS database, see the "Configuring the Database" section on page 2-3.

Configuring the JAVA File

To configure the JAVA file, perform the following steps:

Step 1 Navigate to the location *$JAVA_HOME*/jre/lib/security directory and open the java.security file for editing.

Step 2 Search for the below text:

```
securerandom.source=file:/dev/urandom
```

Replace with:

```
securerandom.source=file:/dev/./urandom
```

Setting up Managed Servers

The following section explains the configuration required to set up the managed server on one host. In order to complete the setup, the same configuration must be performed on all the other managed servers.

- Creating a New WebLogic Domain for a Managed Server, page 2-19
- Extending the WebLogic Domain for a Managed Server, page 2-21
- Configuring the Property Files, page 2-22
- Configuring Jackrabbit in Managed Server, page 2-26

Creating a New WebLogic Domain for a Managed Server

To create a WebLogic domain for managed servers on the machines that are described in Figure 2-1, perform the following steps:

Step 1 Log in to the machine where you want to create a WebLogic domain.

Navigate to **<***BEA_HOME***>**/wlserver_10.3/common/bin and run the **config.sh** file, where <*BEA_HOME*> is the location at which WebLogic is installed.

The Configuration Wizard appears.

Step 2 Choose **Create a new WebLogic domain**, and click **Next**.

The Select Domain Source screen appears.

Step 3 Select **Generate a domain configured automatically to support the following products**, and click **Next**.

The Specify Domain Name and Location screen appears.Specify the domain and location for the domain.

Step 4 Enter the domain name in the Domain Name field.

Step 5 Browse for or enter the path where you want to save the domain and click **Next**.

It is recommended that you create the domain at the default location.

The Configuration Administrator Username and Password screen appears.

Step 6 Enter the administrator username, password, confirm password, and description in the corresponding fields and click **Next**.

The Configure Server Start Mode and JDK screen appears.

Step 7 In the Select JDK and Start Mode screen, do the following:

a. Under WebLogic Domain Startup Mode, choose **Production Mode**.

b. Under Available JDKs, choose **Sun SDK 1.6.0_24**.

c. Click **Next**.

The Select Optional Configuration Screen appears.

Step 8 Select the Adminstration Server, Manager Servers, Clusters and Machines, RDBMS Security Stores check boxes, and click **Next**.

The Configure the Administration Server screen appears.

Step 9 Enter the following details, and click **Next**:

- In the Listen Port field for Machine1, enter 7020.
- In the Listen address field, enter IP address of the managed server.

Note Use Listen Port 7030 for Machine 2.

The Configure Managed Server screen appears.

Step 10 To add the managed server, perform the following steps:

a. In the Configure Managed Servers screen, click **Add**.

A row for the new managed server appears.

b. In the Name field, enter the name of the managed server, for example, MS1.

Note When you configure the managed server names for Machine 1 and Machine 2, you must ensure that the managed server names are unique. For example, MS1 is for Machine 1, while MS2 is for Machine2.

c. In the Listen address field, enter the host IP address of the managed server 1.

d. In the Listen port field, enter the port number as 8020. The port 8020 is the listen port of the managed server 1.

Note Use Listen Port 9020 for Machine 2.

e. Click **Next**.

The Configure Clusters screen appears.

Step 11 Click **Next**.

The Configure Machines screen appears.

Step 12 Click **Next**.

The Configure RDBMS Security Store Database screen appears.

Step 13 Click **Next**.

The Configuration Summary screen appears.

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

A new WebLogic domain is created.

Note After creating the WebLogic domain, you can navigate to <*BEA_HOME*>/user_projects/domains and verify that the domain is created successfully. If you have specified a different location for the domain, navigate to that location to verify if the domain is created successfully.

Extending the WebLogic Domain for a Managed Server

To extend the Oracle WebLogic server domain using the domain template, perform the following steps:

Step 1 Navigate to <*BEA_HOME*>/wlserver_10.3/common/bin, where <*BEA_HOME*> is the location at which WebLogic is installed and run the **config.sh** command in the command mode. For example, **./configu.sh -mode=console**.

The console mode that displays options to either create or extend the WebLogic domain appears.

Step 2 Select the option to extend the WebLogic domain and press **Enter**.

Step 3 From the list of domain directories, choose the domain directory and press **Enter**.

Step 4 Select the option to choose the custom template and press **Enter**.

Step 5 Enter the path to the domain template and press **Enter**.

The domain template for SDP is located at: <SDP_HOME>/sdp/templates/domains/10g/sdp10gdomain.jar, where <SDP_HOME> is the location at which you have installed the SDP.

Step 6 Select the option to modify the Data Sources and press **Enter**.

Step 7 Select the option to modify the DBMS name, enter the database SID, and press **Enter**.

Step 8 Select the option to modify the DBMS host name, enter the database host IP address or the DNS hostname, and press **Enter**.

Step 9 Select the option to modify the DBMS port number, enter the database port number (default port for Oracle is 1521), and press **Enter**.

Step 10 Select the option to modify the username, enter the schema username, and press **Enter**.

Step 11 Select the option to modify the password, enter the schema password, and press **Enter**.

Step 12 Select the option to confirm the password, enter the schema password, and press **Enter**.

Step 13 Press **Accept**.

Step 14 A confirmation message requesting you to proceed appears. Press **Yes**.

The WebLogic domain is successfully extended.

Configuring the Property Files

Updating the Property Files

To update the application.properties, dc.properties, logging.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 a 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. 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

e. 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

f. 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

g. Navigate to <MS_INSTALL_DIRECTORY>/pkg-properties/ and copy the ehcacheconfig.xml

Step 2 Update the application.properties file:

a. Modify the properties as follows:

IB_JMSPROVIDER_URL	*t3://<MS managed server IP Address or hostname>:<MSmanaged server port number>* For example, • For managed server 1: IB_JMSPROVIDER_URL=t3://10.65.111.54:8020 • For managed server 2: IB_JMSPROVIDER_URL=t3://10.65.111.55:9020
IB_userName	*<MS weblogic domain admin userid>* For example, IB_userName=weblogic
IB_password	*<MS weblogic domain admin password>* For example, IB_password=weblogic
SDP_JMSPROVIDER_URL	t3://*<SDP APP server IP Address or hostname>*:*<SDP Appserver port number>* For example, SDP_JMSPROVIDER_URL=t3://10.65.111.56:7001
SDP_userName	*<SDP weblogic console user name>* For example, SDP_userName=weblogic
SDP_password	*<SDP weblogic console password>* For example, SDP_password=weblogic

b. Save and close the file.

Step 3 Update the dc.properties file:

a. Modify the properties as follows:

datacollection.jms.providerUrl	t3://<MS managed server IP Address or hostname>:<MSmanaged server port number> For example, • For Managed Server1: datacollection.jms.providerUrl=t3://10.65.111.54:8020 • For Managed Server2: datacollection.jms.providerUrl=t3://10.65.111.55:9020
datacollection.jms.securityPrincipal	*<MS weblogic console user name>* For example, datacollection.jms.securityPrincipal=weblogic

datacollection.jms.securityCredentials	*<MS weblogic console password>* For example, datacollection.jms.securityCredentials=weblogic
datacollection.unitxml.path=	*<MS_INSTALL_DIRECTORY>*/ms_config/datacollection/unit.xml For example, datacollection.unitxml.path=/home/scc-qa/ms_config/datacollection/unit.xml

b. Save and close the file.

Step 4 Modify the logging.properties file to update the directory in which the MS & DS application 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 5 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=//server2:4001/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>:40001/subscription.cache|//<MS managed server IP address or
hostname>:40001/locationproperty.cache|//<MS managed server IP address or
hostname>:40001/timezone.cache|//<MS managed server IP address or
hostname>:40001/equipment.cache|//<MS managed server IP address or
hostname>:40001/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

Setting up Data Collection

You must set up data collection to gather the data which the Green Advisor module in Smart+Connected DS uses to display reports. For information on how to set up data collection, see the "Setting up Data Collection" section on page 2-10.

Adding Configurations to the WebLogic Server

You must configure the WebLogic server for data collection.

To add the configurations to the WebLogic server, perform the following steps:

Step 1 Open the setDomainEnv.sh file using an editor. The setDomainEnv.sh file is available at: <*BEA_HOME*>/user_projects/domains/<*your domain*>, where <*BEA_HOME*> is the location at which WebLogic is installed.

Step 2 Search for the following text:

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

Step 3 Append the following statement at the end of the above text:

```
-Dcom.cisco.sdp.ldap.configfilepath=<MS_INSTALL_DIRECTORY>/ms_config/LDAP.properties
-DUseSunHttpHandler=true
-Dapplication.properties.filepath=<MS_INSTALL_DIRECTORY>/ms_config/application.properties
-Dipphone.usagemetrics=true
-DDataCollectionPropertyFilePath=<MS_INSTALL_DIRECTORY>/ms_config/datacollection/dc.proper
ties -Djava.util.logging.config.file=<MS_INSTALL_DIRECTORY>/ms_config/logging.properties
-Dweblogic.management.clearTextCredentialAccessEnabled=true
-Dorg.quartz.properties= <MS_INSTALL_DIRECTORY>/ms_config/datacollection/quartz.properties
-Dib.cache.config=<MS_INSTALL_DIRECTORY>/ms_config/ehcacheconfig.xml
-DWebexPropertyFilePath=<MS_INSTALL_DIRECTORY>/ms_config/cleWebexAdapterConfig-MC.properti
es"
```

For example:

```
JAVA_PROPERTIES="${JAVA_PROPERTIES} -da:com.sun.xml.ws...
-Dsdp.cache.config=${DOMAIN_HOME}/sdp/config/platform/cache/sdpcacheconfig.xml
-Dshared.dir=${DOMAIN_HOME}/sdp/shared -Dsdp.mt.mode=1 -Dsdp.event.config.mode=global
-Dcom.cisco.sdp.ldap.configfilepath=/home/scc-qa/ms_config/LDAP.properties
-DUseSunHttpHandler=true
-Dapplication.properties.filepath=/home/scc-qa/ms_config/application.properties
-Dipphone.usagemetrics=true
-DDataCollectionPropertyFilePath=/home/scc-qa/ms_config/datacollection/dc.properties
-Djava.util.logging.config.file=/home/scc-qa/ms_config/logging.properties
-Dweblogic.management.clearTextCredentialAccessEnabled=true"
-Dorg.quartz.properties= <MS_INSTALL_DIRECTORY>/ms_config/datacollection/quartz.properties
-Dib.cache.config=<MS_INSTALL_DIRECTORY>/ms_config/ehcacheconfig.xml
-DWebexPropertyFilePath=<MS_INSTALL_DIRECTORY>/ms_config/cleWebexAdapterConfig-MC.properti
es"
```

Step 4 Save and close the setDomainEnv.sh file.

Configuring Jackrabbit in Managed Server

To configure Jackrabbit in a managed server, perform the following steps:

Step 1 Navigate to the following location:

<*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit

Step 2 Copy jcr-2.0.jar to the directory <*BEA_HOME*>/user_projects/domains/<*Your domain*>/lib, where <*BEA_HOME*> is the location at which WebLogic is installed.

Jackrabbit is successfully configured in a managed server.

Creating WebLogic Domain for Admin/Proxy Server

You must create a WebLogic domain for the admin/proxy server so that the application can be deployed from administrative console. After the application is deployed, it can be accessed from other machines through the proxy server.

To create a WebLogic domain for admin/proxy server, perform the following steps:

Step 1 Log in to Machine 3 where you want to create the admin or proxy server.

In the file browser, navigate to <*BEA_HOME*>/wlserver_10.3/common/bin and run the **config.sh** file.

Where <*BEA_HOME*> is the location at which WebLogic is installed.

The Configuration Wizard appears.

Step 2 Choose **Create a new WebLogic domain**, and click **Next**.

The Select Domain Source screen appears.

Step 3 Select **Generate a domain configured automatically to support the following products**, and click **Next**.

The Specify Domain Name and Location screen appears.Specify the domain and location for the domain.

Step 4 Enter the domain name in the Domain Name field.

Step 5 Browse for or enter the path where you want to save the domain and click **Next**.

It is recommended that you create the domain at the default location.

The Configuration Administrator Username and Password screen appears.

Step 6 Enter the administrator username, password, confirm password, and description in the corresponding fields and click **Next**.

Step 7 In the Select JDK and Start Mode screen, do the following:

a. Under WebLogic Domain Startup Mode, choose Production Mode.

b. Under Available JDKs, choose **Sun SDK 1.6.0_24**.

c. Click **Next**.

The Select Optional Configuration Screen appears.

Step 8 Select the Adminstration Server, Manager Servers, Clusters and Machines, RDBMS Security Stores check boxes, and click **Next**.

The Configure the Administration Server screen appears.

Step 9 Enter the following details, and click **Next**:

- In the Listen Port field, enter 7025.
- In the Listen address field, enter IP address of the admin server.

The Configure Managed Server screen appears.

Step 10 To add the managed server, perform the following steps:

a. In the Configure Managed Servers screen, click **Add**.

A row for the new managed server appears.

b. In the Name field, enter the name of the managed server, for example, MS1.

c. In the Listen address field, enter the host IP address of the managed server 1.

d. In the Listen port field, enter the port number as 8020. The port 8020 is the listen port of the managed server 1.

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

A row for the new managed server appears.

f. In the Name field, enter the name of the managed server. For example, MS2.

g. In the Listen address field, enter the host IP address of the managed server 2.

h. In the Listen port field, enter the port number as 9020. The port 9020 is the listen port of the managed server 2.

i. In the Configure Managed Servers screen, click the **Add**.

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

j. In the Name field, enter the name of the managed server. For example, MS3.

k. In the Listen address field, enter the host IP address of the admin/proxy server.

l. In the Listen port field, enter the port number as 10020. The port 10020 is the listen port of the proxy server.

Step 11 Click **Next**.

The Configure Clusters screen appears.

Step 12 Click **Add** and do the following:

- Enter a name for the cluster, for example MSCluster.
- Change the multicast port to 11020.

Step 13 Click **Next**.

The Assign Servers to the Clusters screen appears.

Step 14 Move all the managed servers from the Servers pane to the Cluster pane but do not move the proxy server (MS3).

Step 15 Click **Next**.

The Create HTTP Proxy Applications screen appears.

Select the **Create HTTP proxy for cluster** <*cluster_name*> check box. Ensure that MS3 is selected in the proxy server combo box.

Step 16 Click **Next**.

The Configure machines screen appears.

Step 17 Click **Next**.

The Configure RDBMS Security Store Database screen appears.

Step 18 Select **I don't want to change anything here**, and click **Next**.

The Review WebLogic Domain screen appears.

Step 19 Review the domain and then click **Create**.

A new WebLogic domain is created.

Note After creating the WebLogic domain, you can navigate to <*BEA_HOME*>/user_projects/domains and verify that the domain is successfully created. If you have specified a different location for the domain, navigate to that location to verify that the domain is successfully created.

Extending WebLogic Domain for Admin/Proxy Server

To extend the WebLogic domain for admin/proxy server, perform the following steps:

Step 1 Navigate to <*BEA_HOME*>/wlserver_10.3/common/bin, where <*BEA_HOME*> is the location at which WebLogic is installed and run the **config.sh -mode=console** file.

The console mode that displays options to either create or extend the WebLogic domain appears.

Step 2 Select the option to xtend the WebLogic domain and press **Enter**.

Step 3 From the list of domain directories, choose the domain directory and press **Enter**. .

Step 4 Enter the path or browse to the domain template. The domain template for SDP is located at:

<*SDP_HOME*>/sdp/templates/domains/10g/sdp10gdomain.jar, where <*SDP_HOME*> is the location at which you have installed the SDP.

Step 5 Select the option to modify the Data Sources and press **Enter**.

Step 6 Select the option to modify the DBMS name, enter the database SID, and press **Enter**.

Step 7 Select the option to modify the DBMS host name, enter the database host IP address or the DNS hostname, and press **Enter**.

Step 8 Select the option to modify the DBMS port number, enter the database port number (default port for Oracle is 1521), and press **Enter**.

Step 9 Select the option to modify the username, enter the schema username, and press **Enter**.

Step 10 Select the option to modify the password, enter the schema password, and press **Enter**.

Step 11 Select the option to confirm the password, enter the schema password, and press **Enter**.

Step 12 Press **Accept**.

Step 13 A confirmation message requesting you to proceed with the update appears. Press **Yes**.

Step 14 The WebLogic domain is successfully updated.

Starting the Administrative Server

To start the admin server, see the "Starting the WebLogic Server" section on page 2-11.

Configuring the Cluster

Configuring a Replication Group

To configure a replication group, perform the following steps:

Step 1 Ensure that the administration server is up and running.

Step 2 Log in to the WebLogic Server Administration Console.

The WebLogic Server Administration Login page appears.

Step 3 Enter the user details that you had specified while creating the WebLogic domain, and click **Login**.

The WebLogic Server home page appears.

Step 4 Click **Lock & Edit**.

Step 5 In the Domain Structure pane, expand the 'Environment' node, and click **Servers**.

The Summary of Servers page appears. Ensure that all the servers are listed with the appropriate port numbers.

Step 6 In the Name column, select **MS 1**.

The Settings for Managed Server 1 page appears.

Step 7 Click **Cluster**, and enter the replication group name in the **Replication Group** field. For example, rep1

Step 8 Click **Save**.

Step 9 In the Name column, select **MS 2**.

The Settings for Managed Server 2 page appears.

Step 10 Click **Cluster**, and enter the replication group name in the **Replication Group** field. For example, rep1.

Note You must enter the same replication group name in both, MS 1 and MS 2. If you change the name, the clustering setup will not work.

Step 11 Click **Save**.

Step 12 Click **Activate Changes**.

Setting Up the Message Types

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

To change the message settings, perform the following steps:

Step 1 Log in to the WebLogic Server Administration Console.

The WebLogic Server Administration Login page appears.

Step 2 Enter the user details that you have specified during the WebLogic domain creation, and click **Login**.

The WebLogic Server home page appears.

Step 3 In the Domain Structure pane, expand the ‘Environment’ node and click **Clusters**.

The Summary of Clusters page appears.

Step 4 Under the **Name** column, select **Cluster**.

The Settings for Cluster page appears.

Step 5 Under the **Configuration** tab, click the **Messaging** tab.

Step 6 Click **Lock and Edit**.

Step 7 From the **Messaging Mode** drop-down list, choose **Unicast**, and then click **Save**.

Step 8 Click **Activate Changes**.

The message settings are now changed to unicast successfully.

Enabling the WebLogic Plug-in

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

Step 1 Log in to the WebLogic Server Administration Console.

The WebLogic Server Administration Login page appears.

Step 2 Enter the user details that you had specified while creating the WebLogic domain, and click **Login**.

The WebLogic Server home page appears.

Step 3 In the Domain Structure pane, expand the Environment node, and click **Clusters**.

The Summary of Clusters page appears.

Step 4 In the Name column, select **Cluster**.

The Settings for Cluster page appears.

Step 5 Click **Advanced**, and click **Lock & Edit**.

Step 6 Select the **WebLogic Plug-In Enabled** check box, and click **Save**.

Step 7 In the Domain Structure pane, click a domain name.

The settings for domain page appears.

Step 8 Click the **Web Applications** tab.

Step 9 Select the **Client Cert Proxy Enabled** and **WebLogic Plug-In Enabled** check boxes, and click **Save**.

Step 10 Click **Activate Changes**.

The WebLogic plug-in is successfully enabled.

Configuring Distributed JMS

To configure the distributed JMS configuration, perform the following steps:

Step 1 Log in to the WebLogic console using the administrator credentials that you provided while creating the domain.

Step 2 Click **Lock & Edit**.

Step 3 Choose **Domain Structure > Services > Messaging > JMS Servers**, and choose **New**.

Step 4 Enter the Name as sspJMSServer1, and click **Next**.

Step 5 Choose the target server as MS1 from the Target drop-down list and click **Finish**.

Step 6 Choose **Domain Structure > Services > Messaging > JMS Servers**, and choose **New**.

Step 7 Enter the name as sspJMSServer2 and click **Next**.

Step 8 Choose the target servers as MS2 from the Target drop-down list, and click **Finish**.

Step 9 Choose **Domain Structure > Services > Messaging > JMS Servers**, and choose **New**.

Step 10 Enter the Name as sspJMSServer3, and click **Next**.

Step 11 Choose the target servers as MS3 from the Target drop-down list, and click **Finish**.

Step 12 Choose **Domain Structure > Services > Messaging > JMS Modules**, and choose **New**.

Step 13 Enter the **Name** as sspJMSModule1 and click **Next**.

Step 14 Choose the cluster under Targets. Click **Next** and then click **Finish**.

Step 15 Choose **Domain Structure > Services > Messaging > JMS Modules**, and choose **New**.

Step 16 Enter the **Name** as sspJMSModule2, and click **Next**.

Step 17 Choose the target as Proxy (MS3), click **Next**, and click **Finish**.

Step 18 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1,** and click **New**.

Step 19 Choose **Connection Factory**, and click **Next**.

Step 20 Enter the Name as sspConnectionFactory1 and JNDI Name as jms/sspConnectionFactory, click **Next**, and click **Finish**.

Step 21 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**, and choose **New**.

Step 22 Choose **Distributed Queue**, and click **Next**.

Step 23 Enter the Name as insertUsageQueue1 and JNDI Name as jms/insertUsageQueue. Click **Next** and then click **Finish**.

Step 24 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**, and choose **New**.

Step 25 Choose **Distributed Queue** and click **Next**.

Step 26 Enter the Name as callbackExchangeQueue1 and JNDI Name as jms/callbackExchangeQueue. Click **Next** and then click **Finish**.

Step 27 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**, and choose **New**.

Step 28 Choose **Distributed Queue** and click **Next**.

Step 29 Enter the Name as emailCaseManagementQueue1 and JNDI Name as jms/emailCaseManagementQueue. Click **Next** and click **Finish**.

Step 30 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**, and choose **New**.

Step 31 Choose **Distributed Queue** and click **Next.**

Step 32 Enter the Name as emailPoisonQueue1 and JNDI Name as jms/emailPoisonQueue. Click **Next** and then click **Finish**.

Step 33 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**, and choose **New**.

Step 34 Choose **Connection Factory** and click **Next**.

Step 35 Enter the Name as dataCollectionConnectionFactory1 and JNDI Name as jms/dataCollectionConnectionFactory. Click **Next** and then click **Finish**.

Step 36 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**, and choose **New**.

Step 37 Choose **Distributed Queue** and click **Next**.

Step 38 Enter the Name as dataCollectionQueue1, JNDI Name as jms/dataCollectionQueue. Click **Next** and then click **Finish**.

Step 39 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 40 Choose **Connection Factory** and click **Next**.

Step 41 Enter the Name as sspConnectionFactory2 and JNDI Name as jms/sspConnectionFactory. Click **Next** and click **Finish**.

Step 42 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 43 Choose **Queue** and click **Next**.

Step 44 Enter the Name as insertUsageQueue2 and JNDI Name as jms/insertUsageQueue. Click **Next**.

Step 45 Click **Create a New Subdeployment**. Enter the Subdeployment Name as insertUsageQueueSubDeployment, and click **OK**.

Step 46 Choose **sspJMSServer3** under Targets, and click **Finish**.

Step 47 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 48 Choose **Queue**, and click **Next**.

Step 49 Enter the Name as callbackExchangeQueue2 and JNDI Name as jms/callbackExchangeQueue. Click **Next**.

Step 50 Click **Create a New Subdeployment** and enter the Subdeployment Name as callbackExchangeQueueSubDeployment. Click **OK**.

Step 51 Choose **sspJMSServer3** under Targets, and click **Finish**.

Step 52 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 53 Choose **Queue**, and click **Next**.

Step 54 Enter the Name as emailCaseManagementQueue2 and JNDI Name as jms/emailCaseManagementQueue. Click **Next**.

Step 55 Click **Create a New Subdeployment** and enter the Subdeployment Name as emailCaseManagementQueueSubdeployment. Click **OK**.

Step 56 Choose sspJMSServer3 under Targets and click **Finish**.

Step 57 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 58 Choose **Queue** and click **Next**.

Step 59 Enter the Name as emailPoisonQueue2 and JNDI Name as jms/emailPoisonQueue. Click **Next**.

Step 60 Click **Create a New Subdeployment**. Enter the Subdeployment Name as emailPoisonQueueSubdeployment and click **OK**.

Step 61 Choose sspJMSServer3 under Targets, and click **Finish**.

Step 62 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 63 Choose **Connection Factory**, and click **Next**.

Step 64 Enter the Name as dataCollectionConnectionFactory2 and JNDI Name as jms/dataCollectionConnectionFactory. Click **Next** and then click **Finish**.

Step 65 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**, and choose **New**.

Step 66 Choose **Queue**, and click **Next**.

Step 67 Enter the Name as dataCollectionQueue2 and JNDI Name as jms/dataCollectionQueue. Click **Next**.

Step 68 Click **Create a New Subdeployment** and enter the Subdeployment Name as dataCollectionQueueSubdeployment. Click **OK**.

Step 69 Choose sspJMSServer3 under Targets, and click **Finish**.

Step 70 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule1**.

Step 71 Click **emailCaseManagementQueue1**.

Step 72 Click the **Delivery Failure** tab.

Step 73 Enter the delay time between the redelivery tries in the Redelivery Delay Override field. Redelivery Delay is the interval after which another attempt to deliver the message will be made after a failed attempt.

Step 74 Enter the redelivery limit value in the Redelivery Limit field.

Step 75 Choose **Redirect** from the Expiration Policy drop-down list.

Step 76 Choose **emailPoisonQueue1** from the Error Destination drop-down list.

Step 77 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule2**.

Step 78 Click **emailCaseManagementQueue2**.

Step 79 Click the **Delivery Failure** tab.

Step 80 In the **Redelivery Delay Override** field, enter the delay time between the redelivery tries.

Redelivery Delay is the interval after which another attempt to deliver the message will be made after a failed attempt.

Step 81 In the **Redelivery Limit** field, enter the redelivery limit value.

Step 82 From the Expiration Policy drop-down list, choose **Redirect**.

Step 83 From the Error Destination drop-down list, choose **emailPoisonQueue2**.

Step 84 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule 1 > Summary of Resources > sspConnectionFactory1**.

Step 85 In the Settings for sspConnectionFactory1 page, click the **Transactions** tab.

Step 86 Select the **XA Connection Factory Enabled** check box, and click **Save**.

Step 87 Choose **Domain Structure > Services > Messaging > JMS Modules > sspJMSModule 2 > Summary of Resources > sspConnectionFactory2**.

Step 88 In the Settings for sspConnectionFactory2 page, click the **Transactions** tab.

Step 89 Select the **XA Connection Factory Enabled** check box, and click **Save**.

Step 90 Click **Activate Changes**.

Restarting the WebLogic Server

For information on how to restart the WebLogic server, see the "Restarting the WebLogic Server" section on page 2-13.

Deploying Apache Jackrabbit

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

Step 1 Log in to the WebLogic Server Administration Console.

The WebLogic home page appears.

Step 2 In the WebLogic home page, under the **Domain Structure**, click **Deployments**.

The Summary of Deployments page appears.

Step 3 Click **Lock & Edit.**

Step 4 Delete the sdpApp and the sdpreport created when you use the SDP domain extension template.

Step 5 Click **Install**.

Navigate to <*MS_INSTALL_DIRECTORY*>/pkg-jackrabbit by either selecting the current location option or by entering path in the path field, and select the jackrabbit-jca-2.2.8.rar file.

Step 6 Click **Next**.

Step 7 Install this deployment as an application, and click **Next**.

Step 8 Select the configured cluster as a target, and click **Next**.

Step 9 Click **Yes, take me to the deployment's configuration screen**, and click **Finish**.

The Configuration screen appears.

Step 10 Change the Deployment Order to 50, and click **Save**.

Step 11 Click **Activate Changes**.

Deploying the Smart+Connected MS & DS Application

To deploy the Smart+Connected MS & DS application for the cluster, perform the following steps on the administrative server:

Step 1 Log in to the WebLogic Administration Console.

The WebLogic home page appears.

Step 2 Click **Lock & Edit**.

Step 3 Click **Deployments**, and choose **Install**.

Step 4 Browse for the Smart_Connected_Meeting_Spaces_and_Digital_Signage.ear file that is available in the <*MS_INSTALL_DIRECTORY*>/pkg-apps folder, and click **Next**.

Step 5 Choose **Install this deployment as an application**, and click **Next.**

Step 6 Select the configured cluster as a target from the Select deployment targets area, click **Next**, and then click **Finish**.

Step 7 Click **Save**.

Step 8 Click **Activate Changes**.

Starting Managed Server and Proxy Server

You must start the managed server and proxy server before you begin accessing the application. To start the managed server and the proxy server, perform the following steps:

Step 1 Login to the server that hosts the WebLogic managed server/proxy.

In a terminal, navigate to the <*BEA_HOME*>/user_projects/domains/<*Your domain*>/bin directory, where <*BEA_HOME*> is the location at which WebLogic is installed.

Step 2 Run the following command to start a managed server:

```
./startManagedWebLogic.sh <name of Managed Server1> t3://<IP address/DNS hostname of admin server>:<listen port of admin server>
```

For example,

```
./startManagedWebLogic.sh MS1 t3://10.65.111.54:7025 (For managed server 1, on Machine 1)
./startManagedWebLogic.sh MS2 t3://10.65.111.54:7025 (For managed server 2, on Machine 2)
./startManagedWebLogic.sh MS3 t3://10.65.111.54:7025 (For proxy, on Machine 3)
```

Step 3 When prompted, enter the domain username and password. For example, weblogic/weblogic.

The application is deployed after the managed server is started.

Starting Application/Cluster Services

The application must be started and running in all the managed servers in the cluster to the service requests. Ensure that all the managed servers are up and running before starting the application/cluster services.

To start the application/cluster services, perform the following steps:

Step 1 Log in to the WebLogic Server Administration Console using the WebLogic domain username and password.

The WebLogic home page appears.

Step 2 In the WebLogic home page, under the Domain Structure, click **Deployments**.

The Summary of Deployments page appears.

Step 3 Click **Lock & Edit**.

Step 4 Choose all the deployments by selecting the respective check boxes.

Step 5 From the Start drop-down list, choose **Start Servicing all requests**.

Step 6 Click **Activate Changes**.

Configuring the Apache Jackrabbit Repository

Configure the Apache Jackrabbit repository by performing the following tasks:

1. Create a sample content in the Smart+Connected MS & DS application—After creating a sample content in the Smart+Connected MS & DS application, a repository structure is automatically created. You must delete the sample content later.
2. Modify the repository.xml file—After modifying the repository.xml file and restarting the managed server, the database tables that are required for Jackrabbit cluster are automatically created.

To configure the Apache Jackrabbit repository, perform the following steps:

Step 1 Ensure that only one managed server is running and all other managed servers are stopped.

Step 2 To create a sample green content, do the following:

a. Log in to the Smart+Connected MS & DS application.

For more information on how to log in to the Smart+Connected MS & DS application, see the "Accessing the Application" section on page 2-39.

The Smart+Connected MS & DS home page appears.

b. Click the **Smart+Connected MS & DS Green Advisor** tab.

The Green Fact tab appears.

c. In the Green Content area, click **Add**, and enter the following details:

- File name
- Content for the file

d. In the left pane, select a location from the location hierarchy tree to which you want to associate the content.

e. Click **Save**.

The repository structure is created in Apache Jackrabbit.

Step 3 Log in to the managed server that is up and running, navigate to the <*BEA_HOME*>/user_projects/domains/<*Your domain*> directory, and verify that the jackrabbit directory is created.

Step 4 To delete the sample green content that you had created in Step 2, do the following:

a. In the Smart+Connected MS & DS application, under the Green Content area, select the content that you had created.

b. Click **Delete**.

Step 5 In the managed server, navigate to <*BEA_HOME*>/user_projects/domains/<*Your domain*> directory and open the repository.xml file for editing.

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

Step 6 Search for the following text:

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

Replace with:

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

Step 7 Search for the following text:

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

Replace with:

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

Step 8 Search for the following text:

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

Replace with:

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

Step 9 Search for the following text:

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

Replace with:

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

Add the following text at the end of the file just above the text *</Repository>*:

```
<Cluster id ="node1" syncDelay = "1000">
<Journal class="org.apache.jackrabbit.core.journal.OracleDatabaseJournal">
<param name="driver" value="oracle.jdbc.driver.OracleDriver"/>
<param name="url" value="jdbc:oracle:thin:@<db host IP address>:<db port number>:<SID of
the db>"/>
<param name="user" value="<schema username>"/>
<param name="password" value="<schema password>"/>
<param name="schemaObjectPrefix" value="C_1_"/>
</Journal>
</Cluster>
```

Note In the above text, you must change value of the *<cluster id>* attribute for each managed server. For example: node1 for MS1, node2 for MS2 and so on.

Step 10 In the Step 6 through Step 9, replace the following strings with their actual values:

Replace *<db host IP address>* with the database server IP address

Replace *<db port number>* with the database port number

Replace *<SID of the db>* with the SID of the database

Replace *<schema username>* with the database username

Replace *<schema password>* with the database user password

Step 11 Delete the jackrabbit directory available under *<BEA_HOME>*/user_projects/domains/*<Your domain>*

Step 12 Restart the managed server.

Step 13 Repeat Step 1 through Step 12 on all the managed servers in the cluster.

Step 14 Start all the managed servers and verify that tables have been created in the database. These tables have names starting with c_1_, d_1_, f_1_, v_1_, w_1_

Importing SSL Certificates

You need to import the SSL certificates for all the managed servers. For more information on how to import the SSL certificates, see the "Importing SSL Certificates" section on page 2-12.

Assigning Roles and Locations to IBUser

To access the Smart+Connected MS & DS 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 IBUser" section on page 2-14.

Accessing the Application

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

Step 1 In the address field of a web browser, type the URL http://<*proxy ip address*>:<*proxy port*>/solutions, and press **Enter**.

The port refers to the port number that you have defined for the proxy server of the Smart+Connected MS & DS domain. The Smart+Connected MS & DS Login page appears.

Step 2 Enter the username and password for the Smart+Connected MS & DS application, and click **Login**.

Your default login credentials are:

- Username—superadmin
- Password—superadmin

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

The Smart+Connected MS & DS home page appears.

For more information on how to use the Smart+Connected MS & DS features, see the *Cisco Smart+Connected Meeting Spaces User Guide and Cisco Smart+Connected Digital Signage User Guide*.

Accessing the Web Calendar

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

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

Step 1 In a Web browser, type the 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 that you have defined for the proxy server of the Smart+Connected MS & DS domain.

Step 2 Press **Enter**.

The Smart+Connected MS & DS Login page appears.

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