Core Change Configuration and Release Management (CCRM)

HP Service Manager – HP Release Control – HP Universal CMDB

for the Windows operating system

Software Version: 9.0

Deployment and Configuration Guide

Document Release Date: July 2010
Software Release Date: July 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Acknowledgements

- This product includes software developed by Apache Software Foundation (http://www.apache.org/licenses).
- This product includes OpenLDAP code from OpenLDAP Foundation (http://www.openldap.org/foundation/).

- This product includes GNU code from Free Software Foundation, Inc. (http://www.fsf.org/).
- This product includes JiBX code from Dennis M. Sosnoski.
- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.
- This product includes the Office Look and Feels License from Robert Futrell (http://sourceforge.net/projects/officelnfs).
- This product includes JEP - Java Expression Parser code from Netaphor Software, Inc. (http://www.netaphor.com/home.asp).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

Welcome to This Guide

This guide provides information for setting up and configuring the Core Change Configuration and Release Management (CCRM) solution that provides a change management process using HP Universal CMDB, HP Service Manager, and HP Release Control.

This chapter includes:

Note: If you have any feedback or comments, please contact solutionpackagingandscp@hp.com.

How This Guide Is Organized

This guide contains the following chapters:

Chapter 1 Introduction to Core CCRM

Provides an introduction to Core CCRM integrations and briefly describes how HP Universal CMDB, HP Service Manager, and HP Release Control integrate with each other.

Chapter 2 UCMDB – Service Manager Integration Configuration

Provides information about setting up UCMDB and Service Manager in order to perform the integration.

Chapter 3 UCMDB – Release Control Integration Configuration

Provides information about setting up UCMDB and Release Control in order to perform the integration.

Chapter 4 Service Manager – Release Control Integration Configuration

Provides information about setting up Service Manager and Release Control in order to perform the integration.

Chapter 5 Solution Verification – Security Settings

Provides information for verifying the Service Manager and Release Control integration, as well as how to configure LWSSO in UCMDB, Release Control, and Service Manager (without HP Operations Orchestration).

Chapter 6 Introduction to CCRM Automation Extension

Provides an introduction to CCRM Extended Automation integrations and briefly describes how Service Manager and Operations Orchestration integrate with each other.

Chapter 7 HP Service Manager – HP Operations Orchestration Integration

Provides information about setting up Service Manager and Operations Orchestration in order to perform the integration, as well as how to configure LWSSO in Operations Orchestration and Service Manager.

Chapter 8 Solution Verification for HP Service Manager and HP Operations Orchestration

Provides information for verifying the Service Manager and Operations Orchestration integration.

Who Should Read This Guide

This guide is intended for a system implementer or system administrator who will be establishing and maintaining a connection between the HP Universal CMDB, HP Service Manager, and HP Release Control systems. This guide assumes that you have administrative access to all systems. The procedures in this guide may duplicate information available in your UCMDB, Service Manager, and Release Control documentation, but is provided here for convenience.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Part I

Core CCRM

1

Introduction to Core CCRM

This chapter includes:

Concepts

Concepts

Core CCRM – Overview

Changes to your IT infrastructure arise for the following reasons:

- proactively – to provide benefits to your organization, either through lower total cost of ownership (TCO), or by providing options that enable your business to develop.
- reactively – to resolve errors that have an impact on the level of services that are provided.

IT organizations today are plagued with numerous incidents that result from unplanned or improperly planned changes to the organization.

The Core Change Configuration and Release Management (CCRM) solution:

- provides the structure and formal workflow necessary to implement changes.
- reduces the risk of making changes by providing an accurate picture of your IT infrastructure, as well as the impact any change may have on IT services.
- enables early detection of unplanned changes.
- maintains an accurate record of the IT infrastructure.

An integration between HP Universal CMDB (UCMDB) and HP Service Manager enables you to share information about the actual state of a configuration item (CI) between your UCMDB system and a Service Manager system. Any organization that wants to implement the best practices Configuration Management and Change Management ITIL processes can use this integration to verify that CIs actually have the attribute values the organization has agreed to support.

You can use this integration to automate the creation of Service Manager change or incident records to update or rollback CIs that have unexpected attribute values. Service Manager allows you to programmatically define what actions you want to take whenever a CI's actual state does not match the expected state as defined in the CI record.

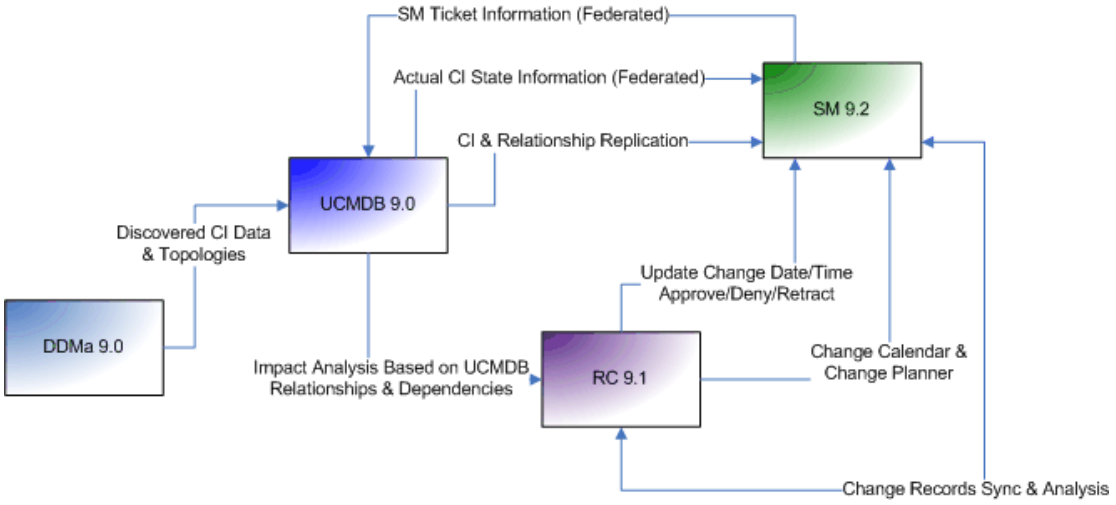
HP Release Control provides your IT organization with an advanced set of capabilities designed to assist in the proper planning and implementation of planned changes to your IT infrastructure.

Note: This guide assumes that the CCRM products are installed in the following default locations:

- **UCMDB – C:\hp\UCMDB**
- **Release Control – C:\hp\RC910**
- **Service Manager – C:\Program Files\hp\Service Manager 9.20\Server**
- **Operations Orchestration – C:\Program Files\Hewlett-Packard\Operations Orchestration**

Core CCRM 9.0 Solution Diagram

The following diagram displays the various data flows of the Core CCRM Solution.



Hardware and Software Requirements

The instructions in this document assume that products are installed in the default location; if this is not the case, you will need to make the appropriate modifications to file paths mentioned in this document.

This section also includes:

➤ "Supported Versions" on page 18

➤ "Enterprise Hardware and Software Requirements" on page 19

For HP Operations Orchestration system requirements, see:

➤ "Operations Orchestration Requirements" on page 58

Supported Versions

Product	Version	instructions
UCMDB	9.00 or later	For installation instructions, see the *HP Universal CMDB Deployment Guide*.
Service Manager	9.20 or later	For installation instructions, see *Service Manager 9.20 Installation Guide*.
Release Control	9.10 or later	For installation instructions, see the *HP Release Control Deployment Guide*.

Enterprise Hardware and Software Requirements

UCMDB Requirements

Recommendations	**Operating system** For 64-bit Windows systems, one of the following: ➤ Windows 2003 Enterprise SP2 and R2 SP2 ➤ Windows 2008 Enterprise SP2 and R2 (recommended) ➤ Red hat Linux 5 Enterprise/Advanced To fulfill the CPU requirements, one of the following: ➤ Intel Dual Core Xeon Processor 2.4 GHz or higher ➤ AMD Opteron Dual Core Processor 2.4 GHz or higher The following number of CPU Cores, depending on your deployment configuration: ➤ Small deployment: 1 CPU ➤ Standard deployment: 4 CPU ➤ Enterprise deployment: 8 CPUs Note: As HP Universal CMDB performance is dependent upon processor speed, to ensure proper HP Universal CMDB performance, it is recommended that you use the fastest possible processor speed. **Memory: Windows** One of the following: ➤ Small deployment: 4 GB RAM ➤ Standard deployment: 8 GB RAM ➤ Enterprise deployment: 16 GB RAM **Virtual memory/Memory swap file: Windows** One of the following: ➤ Small deployment: 6 GB (Supported) ➤ Standard deployment: 12 GB ➤ Enterprise deployment: 24 GB Note:. The virtual memory for Windows should be at least 1.5 times the physical memory size.

Recommendations	**Free hard disk space** ➤ Minimum 30 GB (for logs, memory dumps, and so on) **Display: Windows** ➤ Color palette setting of at least 256 colors (recommended: 32,000 colors)

Service Manager Requirements

Recommendations	**Operating System** For a Windows system, one of the following: ➤ Windows Vista SP1 or higher (recommended) or Windows XP Professional SP2 or higher ➤ Current Windows updates for your operating system ➤ 1 GB RAM minimum, based on the expected user load ➤ Local administrator account to install on the Windows server ➤ Unix **Client Tier** ➤ Windows Client ➤ Compatible Windows OS ➤ Local Administrator account ➤ 100Mb network connection to HP Service Manager (SOAP over HTTP or HTTPS) ➤ Web Clients (optional) ➤ Compatible Browser ➤ Enable Cookies ➤ Enable Java Script ➤ Enable pop-ups ➤ 100Mb network connection to HP Service Manager over a Web browser (HTTP or HTTPS) ➤ Web ➤ Applications that can connect to or communicate with HP Service Manager via Web Services API

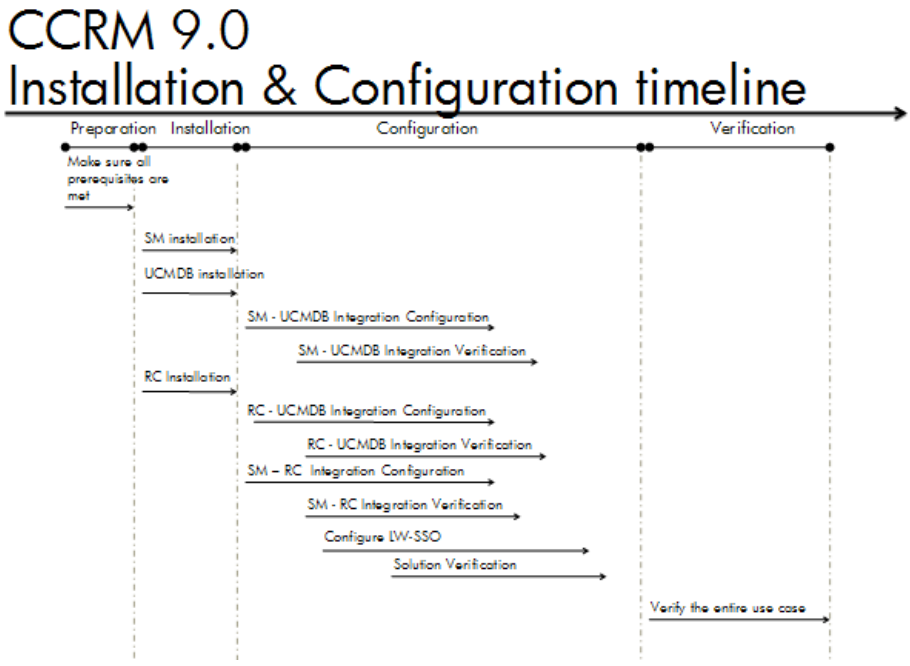
Recommendations	**Server Tier** ➤ HP Service Manager Server ➤ Local Administrator account ➤ Single HP Service Manager Instance ➤ Free communications port ➤ Default: 13080 ➤ Manages connections between clients and the Database tier **Help Server** ➤ Can reside on the same server as the Web Server using same host and a separate communications port OR compatible Web Server and free communications port ➤ HTML help as part of Windows and Web clients or as a standalone HTML page ➤ Web Server ➤ Compatible Web Server ➤ Free communications port ➤ Default: 80 ➤ HTTP or HTTPS content to Web clients ➤ Web Application Server ➤ Compatible Web Application Server ➤ Configure web.xml for connection properties ➤ Compatible JDK ➤ 100+Mb network connection to Web Server (SOAP) ➤ Offers Java applications and content for Web clients **Database Tier** ➤ One or more supported RDBMS on a separate server (RDBMS is a relational database management system for storing HP Service Manager applications and data.) ➤ 1 Gb network connections ➤ HP Service Manager Server **Web Tier (optional)** ➤ Web application server on separate server ➤ Web server on separate server ➤ Service Manager webtier-9.20.war file deployed

Release Control Requirements

Recommendations	CPU: Intel Pentium 4 RAM: 2 GB minimum Free Disk Space: 5 GB minimum **Machine** ➤ VMware ➤ Physical **Operating System** ➤ Windows 2003 Server Enterprise Edition SP2 ➤ Windows Server 2008 **Database** ➤ Microsoft SQL Sever 2005 SP2; 2005 Compatibility Mode 80; (Enterprise Editions for all) ➤ Oracle 9.2.0.8, 10.2.x, 11.1.x **HP Universal CMDB** ➤ HP Universal CMDB version 9.0x (typical CMDB installation) and above **Browser** ➤ Microsoft Internet Explorer 6.0, 7.0, 8.0. ➤ Mozilla Firefox 3.x **Flash Player Browser Plug-in** ➤ Flash Player 9 or above **Screen Resolution** ➤ Minimum 1024x768 ➤ Recommended 1280x1024 **Color Quality** ➤ Minimum of 16 bit Note: If you are logging on to the HP Release Control server through a remote connection, ensure that the Remote Desktop color display setting is set to a minimum of 16 bit.

Core CCRM Project Planning

The following diagram provides a visual display of the various tasks that must be done in order to use the Core CCRM solution.



HP Universal CMDB – Overview

HP Universal CMDB (UCMDB) enables you to manage all the CIs contained in a managed world. A managed world refers to any self-contained environment that can be described using a topology model (defined with HP's Topology Query Language (TQL)).

Integration Class Model

The integration comes with a class model that maps UCMDB CI types, relationships, and attributes to objects and attributes that Service Manager recognizes. In general, Service Manager recognizes fewer CI types than UCMDB. Service Manager manages certain UCMDB CI types, such as a TCP/IP port, as CI attributes rather than a separate CI type. The integration class model groups UCMDB CI types to match how they are managed in Service Manager.

If you want to change the CIs that your UCMDB system sends to your Service Manager system, you need to edit both the integration class model and the integration queries that support the model.

Integration TQL Queries

The integration uses a collection of TQL queries to gather CI attribute information from UCMDB and sends it to the Service Manager system. If you want to change what CI types or attributes are part of the integration, you must also edit the integration queries to support your updated CI types and attributes.

HP Service Manager – Overview

HP Service Manager stores the managed or expected state of CIs and CI relationships as attribute values in a CI record. To be part of the integration, a CI attribute in your UCMDB system must map to a managed field in the Service Manager CI record. You can add, remove, or update the managed fields that are part of the integration by tailoring the Service Manager Web services that manage the integration.

Service Manager runs according to a set of rules that define what actions you want the system to take whenever a CI's actual state does not match the expected state as defined in the CI record. You define these rules from the Discovery Event Manager (DEM) in Service Manager where you can do the following:

- Automatically update a CI record to match the attribute values listed in the actual state. (This is the default behavior.)
- Automatically create a change record to review the differences between the actual state and the managed state.
- Automatically create an incident record to review the differences between the actual state and the managed state.

HP Release Control – Overview

HP Release Control analyzes each change request in the system and provides real-time information and alerts during implementation. In addition, HP Release Control enables collaboration, feedback, and review throughout the release life cycle.

2

UCMDB – Service Manager Integration Configuration

This chapter includes:

Concepts

Tasks

Concepts

Overview

This section describes the necessary steps to configure and verify the integration between UCMDB and Service Manager (SM).

Typically, UCMDB uses one or more discovery mechanisms (feeders) to automatically detect CI attribute values. The UCMDB to Service Manager integration only uses a subset of the CI attributes available in a UCMDB system.

Tasks

Set Up UCMDB for Integration with Service Manager

This task lists the steps necessary to configure HP Universal CMDB in order to perform integration with HP Service Manager.

This task includes the following steps:

- "Prerequisites" on page 28
- "Deploy the Service Manager Integration Package" on page 29
- "Create a New Integration Point" on page 29
- "Set Up the RMI Job" on page 31
- "Set Up the Changes Job" on page 31
- "Run the Replication Jobs" on page 31

Prerequisites

See "Hardware and Software Requirements" on page 18.

Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.

Caution: Run discovery on your UCMDB server. The Service Manager server must be in the range of discovery.

Note: The package should be installed by default when UCMDB 9 is deployed. If it is not, deploy the Service Manager integration package as described in **Deploy the Service Manager Integration Package**.

Deploy the Service Manager Integration Package

1 Log on to UCMDB as an administrator.

2 Select **Administration** > **Package Manager.**

UCMDB displays a list of installed packages.

3 Click the **Deploy Packages to Server (from local disk)** button.

The Deploy Packages to Server dialog box opens.

4 Click the **Add** button and navigate to **c:/hp/UCMDB/ucmdbserver/content/basic-packages**.

5 Select the **smintegration.zip** package and click **Open**, then click **Deploy**.

6 When the installation is complete, a confirmation message appears.

Click **OK**.

Create a New Integration Point

1 Select **Data Flow Management** > **Integration Studio**.

2 In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens.

Enter the following information:

Name	Recommended Value	Description
Adapter	**<user defined>**	Select the appropriate adapter for the version of Service Manager that you are using.

Name	Recommended Value	Description
Credentials	**<user defined>**	If Service Manager credentials appear in the Credentials column, select them. If no Service Manager credentials appear, select **Generic Protocol** and click the **Add new connection details for selected protocol type** button. Enter the following information: ➤ **Description**. Enter **Service Manager**. ➤ **User Name**. Enter the Service Manager user name. The default value is **falcon**. ➤ **User Password**. Enter and confirm a password.
Hostname/IP	**<user defined>**	The name of the Service Manager server.
Integration Name	**SM Integration**	The name you give to the integration point.
Is Integration Activated	**selected**	Select this check box to create an active integration point.
Port	**<user defined>**	The port through which you access Service Manager.

3 Click **OK**.

4 On the Federation tab, select the **Incident**, **Problem**, and **RequestForChange** CI types and click the **Save Integration** button.

Set Up the RMI Job

1 Select the **Data Push** tab and click **Add**.

The Create New Job Definition dialog box opens.

2 In the **Name** field, enter **RMI**.

3 In the **Job Definition** section, select the Job Type **RMI**.

4 In the **Query Name** section, click **Add**.

The Available Queries dialog box opens.

5 Select **Integration** > **SM Sync**.

6 Select queries **businessServiceRelationsData**, **hostRelationsData**, **applicationRelationsData,** and click **OK**.

7 Select the **Allow Deletion** check box for each of the queries and click **OK**.

Set Up the Changes Job

1 Click **Add** to create the Changes adapter.

The Create New Job Definition dialog box opens.

2 In the **Name** field, enter **Changes**.

3 In the **Job Definition** section, select the Job Type **Changes**.

4 In the **Query Name** section, click **Add.**

The Available Queries dialog box opens.

5 Select **Integration** > **SM Sync.**

6 Select queries **applicationData**, **printerData**, **businessServiceData,** **hostData**, **networkData,** and click **OK**.

7 Select the **Allow Deletion** check box for each of the queries and click **OK**.

Run the Replication Jobs

1 Log on to UCMDB.

2 Select **Data Flow Management** > **Integration Studio**.

3 In the Integration Point pane, select the correct integration.

4 Select the **Data Push** tab.

The Job Definition pane appears.

Note: The Changes job must be run before the RMI job.

5 Select your job and click the **Run Full Job** button to run the replication job.

6 When the Confirm synchronizing window appears, click **Yes**.

7 Click the **Statistics** button to view the progress of the synchronization.

8 Click the **Refresh** button to view the updated synchronization status.

Note: Follow the same procedure for the RMI and Changes jobs.

Set Up Service Manager for Integration with UCMDB

This task lists the steps necessary to configure HP Service Manager, in order to perform the integration with HP Universal CMDB.

This task includes the following steps:

- "Prerequisites" on page 32
- "Add the UCMDB Connection Information to the System Information Record" on page 33

Prerequisites

See "Hardware and Software Requirements" on page 18.

Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.

Add the UCMDB Connection Information to the System Information Record

1. Log on to your Service Manager system as an administrator.
2. Select **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
3. Select the **Active Integrations** tab.
4. Select the **HP Universal CMDB** option. The form displays the UCMDB Web service URL field.
5. In the UCMDB Web service URL field, enter the URL to the HP Universal CMDB Web service API. The URL has the following format: **http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService**.
6. In the UserId dialog box, enter your UCMDB user name and password and click **Save**.

Verify UCMDB – Service Manager Integration

1. Browse to your Service Manager server.
2. Select **Configuration Management** > **Resources** > **Search CIs**.
3. 
Click the **Search** button and verify that all the CIs from UCMDB are listed in Service Manager and select the **Actual State** tab to view the CI properties in UCMDB.

3

UCMDB – Release Control Integration Configuration

This chapter includes:

Concepts

Tasks

Concepts

Overview

Release Control (RC) reviews changes to CIs, and analyzes the impact that these changes will have on the CIs and their relationships in UCMDB and Service Manager.

Tasks

This task lists the steps necessary to configure HP Universal CMDB in order to perform the integration with HP Release Control.

This task includes the following steps:

- "Prerequisites" on page 36
- "Deploy the Release Control Integration Package" on page 36

Prerequisites

See "Hardware and Software Requirements" on page 18.

Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.

Deploy the Release Control Integration Package

1 Copy the **rc_package.zip** file from **C:\hp\RC910\uCmdb\ucmdb-90\extensions** on the RC server to **c:\hp\UCMDB\UCMDBServer\content\basic_packages** on the UCMDB server.

2 Launch the CMD user interface (UI) from the UCMDB server.

3 Select **Administration** > **Package Manager**.

UCMDB displays a list of installed packages.

4 Click the **Deploy Packages to Server (from local disk)** button.

The **Deploy Packages to Server** dialog box opens.

5 Click the **Add** button and navigate to **c:\hp\UCMDB\UCMDBServer\content\basic_packages.**

6 Select the **rc_package.zip** package and click **Open**, then click **Deploy**.

7 When the installation is complete, a confirmation message appears.

Click **OK.**

Set Up Release Control for Integration with UCMDB

1. In the RC UI, select **Module** > **Administrator** > **Configuration** > **HP Universal CMDB**.

   The **HP Universal CMDB** pane appears on the right.

2. In the HP Universal CMDB version box, select the appropriate version.
3. Select **Integrations** > **HP Universal CMDB** > **Available Connections**.
4. Enter a valid CMDB server name, port, user name, and password.

5. Click the **Save** button.
6. In the **Save As Draft** dialog box, enter the adapter's draft name.
7. Click **Save**.

8. Click the **Activate** button.

4

Service Manager – Release Control Integration Configuration

This chapter includes:

Concepts

Tasks

Concepts

Overview

This chapter describes how to set up the Service Manager (SM) – Release Control (RC) integration with a common Universal Content Management Database (CMDB) to:

➤ synchronize change data from Service Manager to Release Control

➤ update a Service Manager change record from within Release Control

➤ launch the Release Control Change Calendar and Change Assessment from within Service Manager

Tasks

Set Up Service Manager for Integration with Release Control

This task lists the steps necessary to configure HP Service Manager in order to perform the integration with HP Release Control.

This task includes the following steps:

- "Prerequisites" on page 40
- "Add RC Integration Instance" on page 40

Prerequisites

See "Hardware and Software Requirements" on page 18.

Make sure you have done the following (as part of the installation):

- generate a database schema
- populate the Release Control database

Add RC Integration Instance

1. In SM UI, select **Tailoring**.
2. Select the **Integration Instance Manager** tab.
3.  Click the **Add** button and select **SMtoRC.**
4. In the Integration Template Selection pane, click **Next**.
5. In the Integration Instance Information pane, select **Run at system startup** and click **Next**.
6. In the Integration Instance Parameters pane, select the **General Parameters** tab and enter name of the RC server and its IP address in the **Name** and **Value** fields. Click **Next**.
7. In the Integration Instance fields, click **Next**.

8 In the Integration Instance Mapping table, click **Finish**.

9 In the Integration Instance Manager pane, select **SMtoRC.**

10 Select the **Enable** check box to enable the integration.

Set Up Release Control for Integration with Service Manager

1 Open a remote session with RC.

2 Click **Start** > **Run** > **cmd**.

3 Run the command: **C:\hp\RC910\bin\SdiConfigurer.bat**. The SdiConfigurer.bat batch file asks questions about your system. Answer the questions as follows:

- Select service desk type [ServiceCenter/Service Manager service desks].

  Select **(1) Service Center/Service Manager service desks**.

- Enter adapter name (notice that the name has to be unique).

  Enter **RC-SM Adapter**.

- Select Service Manager/Center version [7.10|7.11|7.2].

  Select **(5) 7.10 and above**.

- Is HP's lightweight single sign on (LWSSO) used (y/n)?

  Type **Y**, since you have enabled LWSSO for the integration.

- Enter Service Manager user name [].

  Enter your user name.

Note: This must be a user account that has access to Service Manager Web services.

➤ Enter password [].

Enter your Service Manager user's password.

➤ Enter Service Manager timezone [US/Pacific].

Note: The time zone for Release Control and Service Manager must be the same.

If you are using the default time zone, press **ENTER**. The default time zone is US/Pacific.

If you are not using the default time zone, then the time zone entered here must synchronize with the time zone used in your Service Manager adapter settings.

➤ Enter Service Manager host name [].

Enter your SM host name in fully qualified domain name (FQDN) format.

➤ Is https required in order to access wsdl? [n]

Press **ENTER** for default.

➤ Enter Service Manager port [13080].

Press **ENTER** for default.

➤ Insert the url suffix for the wsdl file [sc62server/PWS/].

Press **ENTER** for default.

The following confirmation message is displayed in the **C:\hp\RC910\bin\result** folder:

The procedure is complete. The results are located in the result folder.

4 In the RC UI, select **Module** > **Administrator** > **Configuration** > **Integration** > **Service Desk Adapter**.

5 Click the **Add configuration to configuration set** button and select **Service Desk Adapter**.

6 Navigate to **<HP Release Control installation directory>\bin\result** and open **<adapter_name>.zip**.

7 Click the adapter that you created in the previous step.

8 Click the **Save** button.

9 Click the **Activate** button to activate the adapter.

5

Solution Verification – Security Settings

This chapter includes:

Tasks

Tasks

Verify Service Manager – Release Control Integration

1. In the Service Manager user interface (UI), select **Change Management** > **Changes** > **Open New Change**.
2. Enter all necessary information in the appropriate fields and click **Save**.
3. Browse to your RC server. After 30 seconds, your change request is displayed in the calendar.

Configure LWSSO in Universal CMDB (UCMDB)

1 In the UCMDB UI, select **Administrator** > **Infrastructure Settings** in the Configuration tab, and select **Security**.

2 In the list, scroll down and fill in the following fields:

Parameter	Description
LW-SSO Domain	Network domain name (for example, HP.com)
LW-SSO enabling state	Option to enable or disable feature
LW-SSO init string	Initialization string
LW-SSO TRUSTED DNS domains	Network domain name (for example, HP.com)

3 Click **Save**.

4 Restart the UCMDB.

Configure LWSSO in Release Control

1 In RC UI, select **Module** > **Administrator** > **Configuration** > **Security**.

2 Select **HP Lightweight SSO (LWSSO)** and fill in the relevant details.

Parameter	Description
Domain	Network domain name (for example, HP.com)
Initialization String	Encryption key (minimum of six characters)
Protected Domain	Network domain name (for example, HP.com)

3 Click the **Save** button.

4 Click the **Activate** button to activate the adapter.

5 Restart the RC service after any change.

Configure LWSSO in Service Manager

IMPORTANT:

- This configuration applies only to the Apachi Tomcat Web tier.
- If OO exists in the setup, skip to Part II, "Automation Extension" on page 53.

---

1 Deploy the **SymphonyAdapter.war** file shipped with the Service Manager DVD and browse to the directory.

2 In the SymphonyAdapter\WEB-INF\classes folder, rename **lwssofmconf.xml.sample** to **lwssofmconf.xml**. Modify it as follows:

Note: Take note of bold text.

```
<lwsso-config
    xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
    <webui enabled="true">
        <web-lwsso>
            <lwsso startLWSSO="enabled">
                <domain>asiapacific.hpqcorp.net</domain>
                <crypto cipherType="symmetricBlockCipher"
                    engineName="AES" paddingModeName="CBC" keySize="256"
                    encodingMode="Base64Url" initString="HPSELSMRCVINSON"></
crypto>
                expirationPeriod>50</expirationPeriod>
            </lwsso>
            <protectedDomains>
                <url>asiapacific.hpqcorp.net</url>
            </protectedDomains>
            <roleSecurityFrameworkIntegration
                rolePrefix="ROLE_"
                fromLWSSOToSecurityFramework="both"
                fromSecurityFrameworkToLWSSO="enabled"
                caseConversion="upperCase"/>
            <groupSecurityFrameworkIntegration
                fromLWSSOToSecurityFramework="both"
                fromSecurityFrameworkToLWSSO="enabled"
                caseConversion="upperCase"/>
        </web-lwsso>
    </webui>
</lwsso-config>
```

3 Modify the **web.xml** file in the Web client deployment to enable LWSSO.

Locate and uncomment the LWSSO filter and filter-mapping elements in the **web.xml** file. It should display as follows:

```
<filter>
<filter-name>LWSSO</filter-name>
<filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
</filter>

<filter-mapping>
<filter-name>LWSSO</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

4 In the WEB-INF\classes folder of the SM Web client deployment, modify the **application-context.xml** file.

Locate the **filterChainProxy** bean element. Add the lwSsoFilter to the value element. It should display as follows:

```
<bean id="filterChainProxy" class="org.acegisecurity.util.FilterChainProxy">
<property name="filterInvocationDefinitionSource">
<value>
PATTERN_TYPE_APACHE_ANT
/images/**=#NONE#
/js/**=#NONE#
/css/**=#NONE#
/cwc/images/**=#NONE#
/cwc/js/**=#NONE#
/cwc/css/**=#NONE#
/cwc/tree/**=#NONE#
/**=httpSessionContextIntegrationFilter,lwSsoFilter,anonymousProcessingFilter
</value>
</property>
</bean>
```

5 Locate and uncomment the lwSsoFilter bean and the lwSsoIntegration bean. It should display as follows:

Note: <!-- This bean is used for HP Lightweight Single Sign-on, to integrate with other Hewlett-Packard software products. Uncomment it here and reference it in the filterChainProxy as commented above. -->

```
<bean id="lwSsoFilter"
class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
<property name="authenticationManager">
<ref bean="authenticationManager"/>
</property>
<property name="defaultRole">
<value>ROLE_PRE</value>
</property>
</bean>

<bean id="lwSsoIntegrationBean"
class="com.hp.ov.sm.client.webtier.lwsso.LwSsoIntegration"/>
```

If it is not displayed, add it.

6 In the WEB-INF\classes folder of the SM Web client deployment, add domain and crypto settings to the **lwssofmconf.xml** file. It should display as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config
xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
<webui enabled="true">
<web-lwsso>
    <lwsso startLWSSO="enabled">
        <domain>asiapacific.hpqcorp.net</domain>
        <crypto cipherType="symmetricBlockCipher"
            engineName="AES" paddingModeName="CBC" keySize="256"
            encodingMode="Base64Url" initString="HPSELSMRCVINSON"></crypto>
        <expirationPeriod>50</expirationPeriod>
    </lwsso>
    <logoutURLs>
        <url>sm/goodbye.jsp</url>
    </logoutURLs>
    <protectedDomains>
        <url>asiapacific.hpqcorp.net</url>
    </protectedDomains>
    <roleSecurityFrameworkIntegration
        rolePrefix="ROLE_"
        fromLWSSOToSecurityFramework="external"
        fromSecurityFrameworkToLWSSO="enabled"
        caseConversion="upperCase"/>
    <groupSecurityFrameworkIntegration
        fromLWSSOToSecurityFramework="external"
        fromSecurityFrameworkToLWSSO="enabled"
        caseConversion="upperCase"/>
</web-lwsso>
</webui>
</lwsso-config>
```

7 Modify the server.xml file under **Direct to <tomcat directory>\conf\server.xml**.

Open **server.xml** with a text editor.

```
<Connector port="8009"
enableLookups="false" tomcatAuthentication="false" redirectPort="8443" debug="0"
protocol="AJP/1.3" />
```

Restart your tomcat.

Configure Release Control

1 Click **Module** > **Administrator** > **Configuration** > **Security** > **HP LightweightSSO(LWSSO)**.

Change the domain, initialization string, and protected domains to the correct ones.

2 Create a RC user which has the same account and password as the one in Service Manager.

Verification Procedure with Security Enabled

To verify that your solution is working with security enabled:

1 Log in to **Service Manager** and launch the **RC Change Calendar**. Bypass the RC log-in prompt.

2 Update a **Service Manager** change from within RC.

Part II

Automation Extension

6

Introduction to CCRM Automation Extension

This chapter includes:

Concepts

Concepts

CCRM Automation Extension

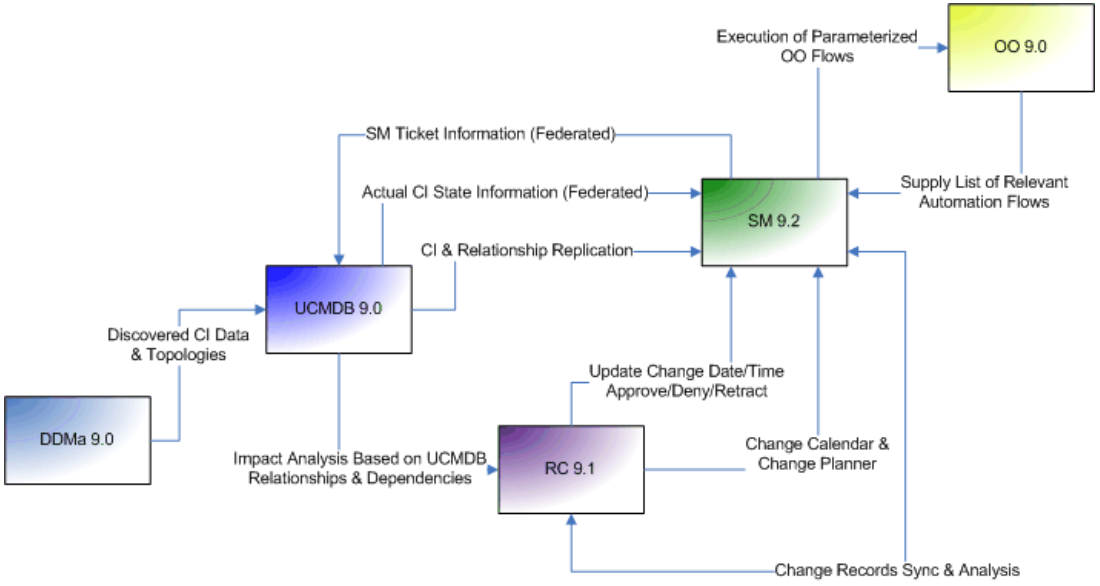
HP Operations Orchestration (OO) provides an extension to the CCRM solution that can be easily implemented. An extension module can always be added to the CCRM solution in order to cover broader functionalities and processes.

Note: This guide assumes that the CCRM Automation Extension product is installed in the following default location:

➤ **Operations Orchestration – C:\Program Files\Hewlett-Packard\Operations Orchestration**

CCRM 9.0 Solution Automation Extension Diagram

The following diagram displays the various data flows of the CCRM Solution Automation Extension.



Hardware and Software Requirements

The instructions in this document assume that products are installed in the default location; if this is not the case, you will need to make the appropriate modifications to file paths mentioned in this document.

This section also includes:

➤ "Operations Orchestration Requirements" on page 58

For core system requirements, see:

➤ "UCMDB Requirements" on page 19

➤ "Service Manager Requirements" on page 20

➤ "Release Control Requirements" on page 22

Supported Versions

Product	Version	instructions
OO	9.00 or later	For installation instructions, see the *Installing or Upgrading HP Operations Orchestration Windows, Linux, and Solaris Operating Systems Guide*.

Enterprise Hardware and Software Requirements

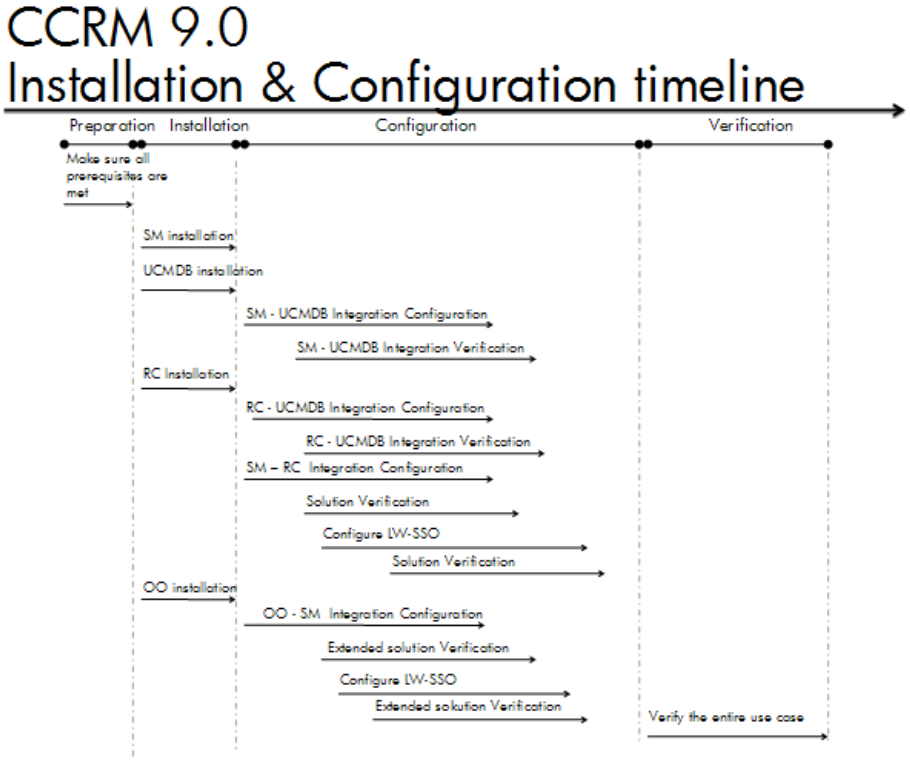
Operations Orchestration Requirements

Recommendations	For 64-bit Windows systems, OO supports the AMD64 and Intel64 servers. CPU: 3 Gigahertz (GHz) for single-processor systems or 2 GHz for multi-processor systems Memory (RAM): 3 Gigabyte (GB) **Hard-drive space** ➤ Database server: As described in your database system requirements ➤ HP OO Central server: 4 GB (This includes room for the flows and operations that are included in the installation and for their rolling backups.) ➤ When the database and Central are installed on the same machine, sum the requirements for the database and the Central servers. ➤ Add 100KB for each flow that you have created and its rolling backups. ➤ Add 10.2MB if you install HP OO Load Balancer. A Central server that is installed on a Windows operating system can now use an Oracle database. If the Oracle database is resides on an Oracle RAC, incorporate the Guide to Installing HP OO with RAC (InstallingHPOO_RACGuide.pdf) into your HP OO installation planning and procedures.

Recommendations	**Operating system** One of the following: ➤ Microsoft Windows 2003 Server (Standard, Enterprise, or Datacenter edition) Service Pack (SP) 2, 32-bit or 64-bit, with the December 2008 cumulative time zone update for Microsoft Windows operating systems applied. For information on applying the time zone update, see support.microsoft.com, Knowledge Base article 955839. ➤ Microsoft Windows 2008 R2, Server (Standard, Enterprise, or Datacenter edition) SP 2, 32-bit or 64-bit. **Runtime environments** Microsoft .NET Framework 2.0 Service Pack 1 (SP 1) and either 3.0 or 3.5 SP 1, with ASP.NET enabled for either **Important:** If you have .NET Framework 3.0 or 3.5 SP 1 installed, you must also install .NET Framework 2.0 SP 1, side by side with version 3.0 or 3.5 SP 1. **Database management system** One of the following: ➤ Microsoft SQL Server 2000 Service Pack 3a or later, SQL Server 2005 SP 3, or SQL Server 2008 SP 1. ➤ Oracle (one of the following): ➤ 10g Standard R2 ➤ 10g Enterprise R2 ➤ 11g Standard R2 ➤ 11g Enterprise R2 ➤ 11g RAC R2 ➤ Sun Microsystems MySQL 5.0.41 or 5.1.30. **Web browsers** One of the following: ➤ Microsoft Internet Explorer 6.x, 7.x, or 8.x ➤ FireFox 1.5, 2.x, or 3.x **Scriptlet language support** If you run a flow that contains a Perl scriptlet operation, ActivePerl 5.8.8.824 is required. When installing ActivePerl, select the option to add its path to the PATH environmental variable. **Flash animation support** Adobe Flash Player version 10.0

CCRM Operations Orchestration Project Planning

The following diagram provides a visual display of the various tasks that must be done in order to use the CCRM Automated Extension solution.



HP Operations Orchestration – Overview

HP Operations Orchestration (HP OO) is a system for creating automated procedures (called Ops flows or flows) and making them available to IT personnel. Ops flows are made up of operations that each perform a specific action to maintain, diagnose, and/or repair a system.

Operations Orchestration is made up of:

- The Central Web application, which provides the business-logic tier between the OO Repository database and both the Central Web client and Studio.
- The Central Web client, which is the browser-based tool that IT personnel use to execute Ops flows.
- The Remote Action Service (RAS), a service that enables you to run operations outside Central and the domain in which Central resides. With RAS, you can run operations on any system, anywhere.
- OO Studio, a standalone application in which you create new Ops flows.

7

HP Service Manager – HP Operations Orchestration Integration

This chapter includes:

Concepts

Tasks

Concepts

Overview

This section describes the necessary steps to configure and verify the integration between HP Service Manager (SM) and HP Operations Orchestration (OO).

Tasks

Set up HP Service Manager for integration with HP Operations Orchestration

This task lists the steps necessary to configure HP Service Manager in order to perform the integration with HP Operations Orchestration.

This task includes the following steps:

- "Prerequisites" on page 64
- "Integration Configuration" on page 68
- "Service Manager – Operations Orchestration Security Configuration" on page 70
- "Configure LWSSO" on page 75

Prerequisites

See "Hardware and Software Requirements" on page 18.

1. Install SM9.2—Install Apache Tomcat 6 application server and SM Web tier (for installation instructions, see the platform's installation manual).

Note: We are only referring to the Apache Tomcat application server and not to other web tiers.

---

2. Download the **SM 9 Unloads For SM9 Intregration.rar** file and extract it to your desktop. The **CCRM with OO** folder is displayed.
3. Import the SM integration unload files.

Note: If you are prompted to modify the database structure at any point in the following process, you have two options:

- Click the **SM Alters** button to enable SM to make these modifications to the database.
- Manually copy the database scripts displayed in the window and send them to your database administrator to make these modifications.

Your choice depends on your company policy and is not a matter of Best Practices.

---

a Open an http session to **SM: http://smhostname:8080/webtier-9.20/index.do** and log in as a system administrator.

b In Service Manager, enter **db** in the command box and click the **Execute** button to execute the command.

c In the Database window, select **More** > **Import/Load.**

d Click the **Browse** button next to the **File Name** field to locate the **CCRM with OO** folder you downloaded on desktop in step 2, select the **SM 9 Unloads** file and click **OK**.

e After you have selected the correct file, click **Load FG**.

f Repeat the process for the other two *.unl files.

4 Install OO Central 9.0 (for installation instructions, see the platform's installation manual).

5 Update the latest OO content install jar file in OO server for updated SM operations.

a From the **CCRM with OO** folder you downloaded on desktop in step 2, select the **OO 9 Content** file and copy it to the OO server file system.

b Run this command to install the package: **java -jar OO-9_00-ContentInstaller.jar -centralPassword <password>**.

Note: For the command to run properly, run it from OO's jre folder (version 1.6 and above). For example, C:\Program Files\Hewlett-Packard\Operations Orchestration\jre1.6\bin).

---

c Confirm the file modify date of HPserverManager.rar in C:\Program Files\HP\Operations Orchestration\RAS\Java\Default\repository.

d Confirm the HP SM actions properties in OO's studio under /Library/Integrations/Hewlett-Packard/Service Manager/.

Note: All operations must have the same version.

---

6 Install OO Studio 9.0 (for installation instructions, see the platform's installation manual).

7 Import **VM RAS operations—IActions**.

a From **Start** > **Programs/Control Panel** > **Administrative Tools** > **Services**, select **RSJRAS** and click the **Stop** button.

b From the **CCRM with OO** folder you downloaded on desktop in step 2, select **VM IActiona Jar Files** and copy it to the OO server.

c In the OO server file system, copy the **vmware-cmd-1.0.jar** file to **C:\Program Files\Hewlett-Packard\Operation Orchestration\RAS\Java\Default\repository** and copy the **vmware-cmd-1.0.jar** directory to **C:\Program Files\Hewlett-Packard\Operation Orchestration\RAS\Java\Default\repository\lib**.

d Click the **Start** button to start RSJRAS service on the OO server.

e Log in to OO Studio client.

f Navigate to **Library** > **My Ops Flows** and create a new folder called **IActions**.

g In the **IActions** folder, click **File** > **Create Operations from RAS**.

h Select which RAS to import the new operations from, then click **OK**.

i Select the RAS **vmware-cmd-01.jar** operation to import, and click **OK**. Wait for the process to finish.

Note: Your new operations are now located in the chosen directory. You can use the new operations in your flows like you would normally use other OOB operations.

---

8 Import the OO integration flows.

a From the **CCRM with OO** folder you downloaded on desktop in step 2, select the **CCRM OO Flows** file and extract it to your desktop.

b Log in to OO Studio client.

c In the **Public Repository tree**, navigate to **Library** > **My Ops Flows**.

d On the **Repository** menu, click **Import Repository**.

e Browse to the extracted **CCRM OO Flows** folder and click **Open**.

f In the import tool window, in the **Action** column, click the **Modify in Repository** button for both Library and Configuration trees, and then click the **Apply** button.

The **My Ops Flows** folder now contains all needed CCRM flows and operations.

Integration Configuration

Note: All configurations in SM will be done via its user interface (UI) Web tier.)

---

1 Log in to SM as a system administrator.

2 Create a new operator. The same user should be opened in OO as an external user.

a Navigate to **System Administration** > **Ongoing Maintenance** > **User Quick Add Utility**.

b Fill out the **Create User Wizard** form, and click **Next**. The Create User Wizard window is displayed.

c In the **Select User to Clone** drop-down box, select **falcon** and click **Finish**.

d Select the **Operator:Admin** tab and the Operator Record window is displayed.

e Select the **Security** tab and replace the password with your own. Click **Save** and **OK**.

3 Navigate to **Tailoring** > **Integration Manager**.

4 Click the **Add** button.

5 Select the **Wizard Integration Template Select** tab.

6 In the **Integration Template** drop-down box, select **SMOO** and **Next**.

7 In the Integration Instance Information window, fill in the required fields as follows, and click **Next**.

Name	Recommended Value	Description
Interval time	**<user defined>**	The time interval in seconds between when the adapter runs.
SM server	**<user defined>**	FQDN.
Log level	**<user defined>**	The default log level.
Log file directory	**<user defined>**	The log file directory on the Service Manager file system.
Max Retry Times	**<user defined>**	How many times to retry upon failure.
Endpoint server	**<user defined>**	FQDN.
Run on Startup	**<user defined>**	Selection check box if you want the adapter to run on system startup.

8 In the Integration Instance Parameters window, select the **General Parameters** tab and complete the following required fields:

Name	Recommended Value	Description
oo.server.url:	**https://oohostname:8443**	The location of the OO server.
oo.user.name	**<user defined>**	The OO user account created for the integration (admin).
Basepath	**<user defined>**	The OO library path.

9 Select the **Secure Parameters** tab and fill out the required fields.

10 Click **Next** > **oo.password** > **OO account password** > **Next** > **Finish**.

To enable the integration:

1 Press the **Ctrl** key and select the integration line.

2 Click the **Enable** button.

3 Click **Yes** to approve.

Note: The integration instance runs at predefined intervals and does not always run. It sleeps between the predefined intervals.

Service Manager – Operations Orchestration Security Configuration

➤ "Operations Orchestration SSL Configuration" on page 70

➤ "Service Manager SSL Configuration" on page 74

Operations Orchestration SSL Configuration

There are three modules to configure SSL.

➤ "Configure SSL on OO Central" on page 70

➤ "Configure SSL in OO RAS" on page 73

➤ "Configure SSL in OO Scheduler" on page 73

Configure SSL on OO Central

1 Stop the **RSCentral** service.

2 Install **OpenSSL Light 1.0** on the OO Central server.

3 Append the **OpenSSL** bin folder to the Path variable in the system environment.

4 Search for the **openssl.cnf** file location under the **OpenSSL** installation directory and create a new system environment variable named **OPENSSL_CONF**. Its value should be the full path to the file (the file name must be included).

5 Search for the **keytool.exe** file and append its location to the Path variable in the system environment.

6 Backup OO Central's **rc_keystore** file, located under **%OO_Home%\Central\Conf**.

7 Generate a private / public key pair for Root Certificate Authority as follows:

a Open a CMD window and change the directory to **%OO_Home%\Central\Conf**.

b Run the command: **openssl genrsa -des3 -out cakey.pem 2048**.

Note: Give any string for "passphrase". Remember the string for later commands.

---

c Run the command: **openssl req -new -key cakey.pem -x509 -days 1095 -out mycacert.pem**.

Note: The Common Name field in the above command must be filled with the OO server FQDN name (for instance, ooserver.devlab.ad).

Examples of data to enter during the command execution follows:

Country Name (two-letter code) [AU]	IL
State or Province Name (full name) [State name]	Israel

Locality Name (for instance, City) []	Yehud
Organization Name (for instance, Company) [Internet Widgits Pty Ltd]	HP Software
Organizational Unit Name (for instance, section) []	SSG
Common Name (for instance, your name) []	vmamqa162.devlab.ad
Email Address []	name@devlab.ad

8 Use a Java keytool to generate a request as follows:

a Run the command (use values from the previous step to populate corresponding fields): **keytool -genkey -alias sm -keyalg RSA -keystore rc_keystore -storepass bran507025 -keypass bran507025 -dname "CN=vmamqa162.devlab.ad, OU=SSG, O='HP Software', L=Yehud, ST=Israel, C=IL"**.

Note: The default value for both <store password for rc_keystore> and <key password for rc_keystore> is **bran507025**.

---

b Run the command: **keytool -certreq -keystore rc_keystore -alias sm -storepass bran507025 -file req.crs**.

c Run the command: **openssl x509 -req -days 1095 -in req.crs -CA mycacert.pem -CAkey cakey.pem -CAcreateserial -out smcert.pem**.

9 Import the root CA and self-signed certificate to rc_keystore as follows:

a Run the command: **keytool -import -v -alias rootca -keystore rc_keystore -storepass bran507025 -file mycacert.pem**.

b The command window prompts the certificate information. When asked to **Trust this certificate?[no]: y**, answer yes.

The following confirmation message is displayed:

Certificate was added to keystore.

[Storing rc_keystore]

c Run the command: **keytool -import -v -alias sm -keystore rc_keystore -storepass bran507025 -file smcert.pem**.

The following confirmation message is displayed:

Certificate reply was installed in keystore.

[Storing rc_keystore]

10 Start RSCentral service.

Configure SSL in OO RAS

1 Stop the RSJRAS service.

2 Copy the generated mycacert.pem and smcert.pem from **%OO_Home%\Central\Conf** to **%OO_HOME%\RAS\Java\Default\webapp\conf**.

3 Open a CMD window and change the directory to **%OO_HOME%\RAS\Java\Default\webapp\conf**.

4 Run the command: **keytool -import -v -alias rootca -keystore ras_keystore.jks -storepass bran507025 -file mycacert.pem**.

5 Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** is displayed.

6 Run the command: **keytool -import -v -alias sm -keystore keystore.jks -storepass bran507025 -file smcert.pem**.

7 Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** is displayed.

8 Start RSJRAS service.

Configure SSL in OO Scheduler

1 Stop the RSScheduler service.

2 Copy the generated mycacert.pem and smcert.pem from **%OO_Home%\Central\Conf** to **%OO_HOME%\ Scheduler\conf**.

3 Open a CMD window and change the directory from **%OO_Home%\Central\Conf** to **%OO_HOME%\Scheduler\conf**.

4 Run the command: **keytool -import -v -alias rootca -keystore rc_keystore -storepass bran507025 -file mycacert.pem**.

5 Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** is displayed.

6 Run the command: **keytool -import -v -alias sm -keystore rc_keystore -storepass bran507025 -file smcert.pem**.

7 Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** is displayed.

8 Start RSScheduler service.

Note: Use the same procedure to configure SSL on OO Studio.

Service Manager SSL Configuration

1 Stop the SM service.

2 Install **OpenSSL Light 1.0** on the SM server.

3 Append the **OpenSS**L bin folder to the Path variable in the system environment.

4 Search for the **openssl.cnf** file location under the **OpenSSL** installation directory and create a new system environment variable called **OPENSSL_CONF**. Its value should be the full path to the file (the file name must be included).

5 Search for the **keytool.exe** file and append its location to the Path variable in the system environment.

6 Create a trust store for SM as follows:

   a Copy the generated mycacert.pem and smcert.pem from **%OO_Home%\Central\Conf** to **%SM_home%\Server\RUN**.

   b Open a CMD window and change the directory to **%SM_home%\Server\RUN.**

c Run the command: **keytool -import -v -alias rootca -keystore rc_keystore -storepass bran507025 -file mycacert.pem**.

d Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** is displayed.

e Run the command: **keytool -import -v -alias sm -keystore rc_keystore -storepass bran507025 -file smcert.pem**.

f Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** is displayed.

g Verify smtrust was created under %SM_home%\Server\RUN.

h Append the following lines to the **sm.ini** file under the above location:

```
#
# Certificates
#
truststoreFile:<keystore_file>
truststorePass:<password>
```

If you have used this document's defaults, the sm.ini file looks as follows:

```
#
# Certificates
#
truststoreFile:smtrust
truststorePass:bran507025
```

7 Start the SM service.

Configure LWSSO

➤ "Configure LWSSO in Operations Orchestration" on page 76

➤ "Configure LWSSO in Service Manager" on page 78

Configure LWSSO in Operations Orchestration

If Lightweight Single Sign-On (LWSSO) is enabled in both Service Manager and Operations Orchestration (OO), users who have logged on to Service Manager are allowed to sign on to Operations Orchestration through the Web tier without providing a user name and password.

Note: In the following procedure, %OO_HOME% represents the Operations Orchestration home directory.

To configure LWSSO in Operations Orchestration:

1. In %OO_HOME%\Central\WEB-INF\applicationContext.xml, enable the import between **LWSSO_SECTION_BEGIN** and **LWSSO_SECTION_END**.
2. In %OO_HOME%\Central\WEB-INF\web.xml, enable all the filters and mappings between **LWSSO_SECTION_BEGIN** and **LWSSO_SECTION_END**. You should find two instances. Enable both of them.
3. In %OO_HOME%\Central\conf\lwssofmconf.xml, edit the following two parameters:
   a. **domain**: Domain name of the Service Manager Web tier server
   b. **initString**: Must match the initString value in the Service Manager LWSSO configuration

   ---

   Note: The init string parameter should match the init string defined earlier.

For example:

```
<webui>
        <validation>
            <in-ui-lwsso>
                <lwssoValidation  id="ID000001">
                    <domain>asia.hpqc.net</domain>
                    <crypto cipherType="symmetricBlockCipher"
                        engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                        initString=" SMOOIntegration "></crypto>
                </lwssoValidation>
            </in-ui-lwsso>
        </validation>
        <creation>
            <lwssoCreationRef id="ID000002">
                <lwssoValidationRef refid="ID000001"/>
                <expirationPeriod>600000</expirationPeriod>

                </lwssoCreationRef>
        </creation>
</webui>
```

4 In lwssofmconf.xml, add protected domains data immediately following / creation element:

```
</creation>
<protectedDomains>
            <url>devlab.ad</url>
            <url>emea.hpqcorp.net</url>
</protectedDomains>
</webui>
```

5 Restart Operations Orchestration Central for the configuration to take effect.

Configure LWSSO in Service Manager

Note: The LWSSO configuration must be done once for all integrations.

If Lightweight Single Sign-On (LWSSO) is enabled in both Service Manager and another HP Product (for example, HP Operations Orchestration), users who have logged on to Service Manager are allowed to sign on to the other HP product through the Web tier without providing a user name and password.

Note: The following procedure is provided as an example, assuming the Service Manager Web tier is deployed on Tomcat.

To configure LWSSO in Service Manager:

1. Deploy the Service Manager Web tier on a Web application server (for example, Tomcat), and modify the Service Manager server name and port in web.xml if necessary.
2. Modify the **<tomcat_root>\conf\server.xml** by adding **tomcatAuthentication="false"** to the following node:

```
<Connector port="8009"
        enableLookups="false" tomcatAuthentication="false" redirectPort="8443"
debug="0"
        protocol="AJP/1.3" />
```

3. Modify **<Service Manager Web tier>\WEB-INF\web.xml**.
   a. Change the value of the context parameter **isCustomAuthenticationUsed** to **false**.
   b. Search for the **<filter-name>LWSSO</filter-name>** string, and remove the comment tags (<!-- and -->) enclosing the filter element to enable LWSSO authentication.

Note: This occurs twice—once with class name and once with filter mapping.

---

c Search for the <**param-name**>**querySecurity**</**param-name**> element, and change its value to **false**.

d If you have not already done so, modify the parameter serverHost to the SM server FQDN name.

4 In the <**Service Manager Web tier**>**WEB-INF****classes****lwssofmconf.xml**, modify the following parameters in the **webui** node.

- <**domain**>: Domain name of the server where you deploy your Service Manager Web tier.
- **initString**: Password used to connect HP products. Make sure this is the same value as that used to connect to the other HP products (such as Operations Orchestration) that you want to connect via LWSSO.
- <**protectedDomain**>:
  - Replace the domain value with the domain name portion of your Service Manager Web tier server.

    For example, if your Web tier's fully qualified domain name is **mywebtier.domain.hp.com**, then the domain portion is **domain.hp.com**. The new value should appear as in the following example:

```
<protectedDomains>
  <url>domain.hp.com</url>
</protectedDomains>
```

  - <**lwsso startLWSSO**>: Replace the value with **enabled**.
  - Add any additional domain URLs as needed for your network. You must add a separate <**url**> element for each domain you want to support with LWSSO.

Note: The init string parameter should match the init string defined earlier.

For example:

```
<webui enabled="true">
......
<web-lwsso>
<lwsso startLWSSO="enabled">
<domain>domain.hp.com</domain>
<crypto cipherType="symmetricBlockCipher"
engineName="AES" paddingModeName="CBC" keySize="256"
encodingMode="Base64Url" initString="SMOOIntegration "></crypto>
<expirationPeriod>50</expirationPeriod>
</lwsso>
......
<protectedDomains>
<url>domain1.hp.com</url>
 <url>domain2.hp.com</url>
</protectedDomains>
......
</webui>
```

5 Modify <**Service Manager Web tier**>**WEB-INF****classes****application-context.xml**.

➤ Add **lwSsoFilter** to **filterChainProxy**:

```
/**=httpSessionContextIntegrationFilter,lwSsoFilter,anonymousProcessingFilter
```

➤ Uncomment **bean lwSsoFilter** for HP Lightweight Single Sign-on:

```
<bean id="lwSsoFilter"
class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
```

➤ Add the following:

```
<bean id="lwSsoIntegrationBean"
class="com.hp.ov.sm.client.webtier.lwsso.LwSsoIntegration"/>
</beans>
```

6 Restart Tomcat for the configuration to take effect.

8

Solution Verification for HP Service Manager and HP Operations Orchestration

This chapter includes:

Concepts

Tasks

Concepts

Introduction

The Service Manager server uses a proprietary SSO protocol that is based on a mutually authenticated Secure Sockets Layer.

Tasks

Verify Service Manager – Operations Orchestration Integration with Security Enabled

1. In SM, create a new Request for Change (RFC).
2. Fill out the mandatory fields and click **Save**.
3. In the new ticket, scroll down to the OO flows links section.
4. Select the OO flow you want to run and click **Add link**.
5. In OO flow link Details window, fill out all mandatory fields and the flow's input parameters, then click **Add**.
6. Return to the ticket's OO flow links section and choose the automation type as follows:
   a. **When approved:** Change the ticket's phase to **Change Implementation**. View the ticket's log to confirm that the OO flow was executed.
   b. **By fixed date:** Select the date and time combination. View the ticket's log to verify the OO flow was triggered properly.

Index

O

P

Q

R

S

T

U

V