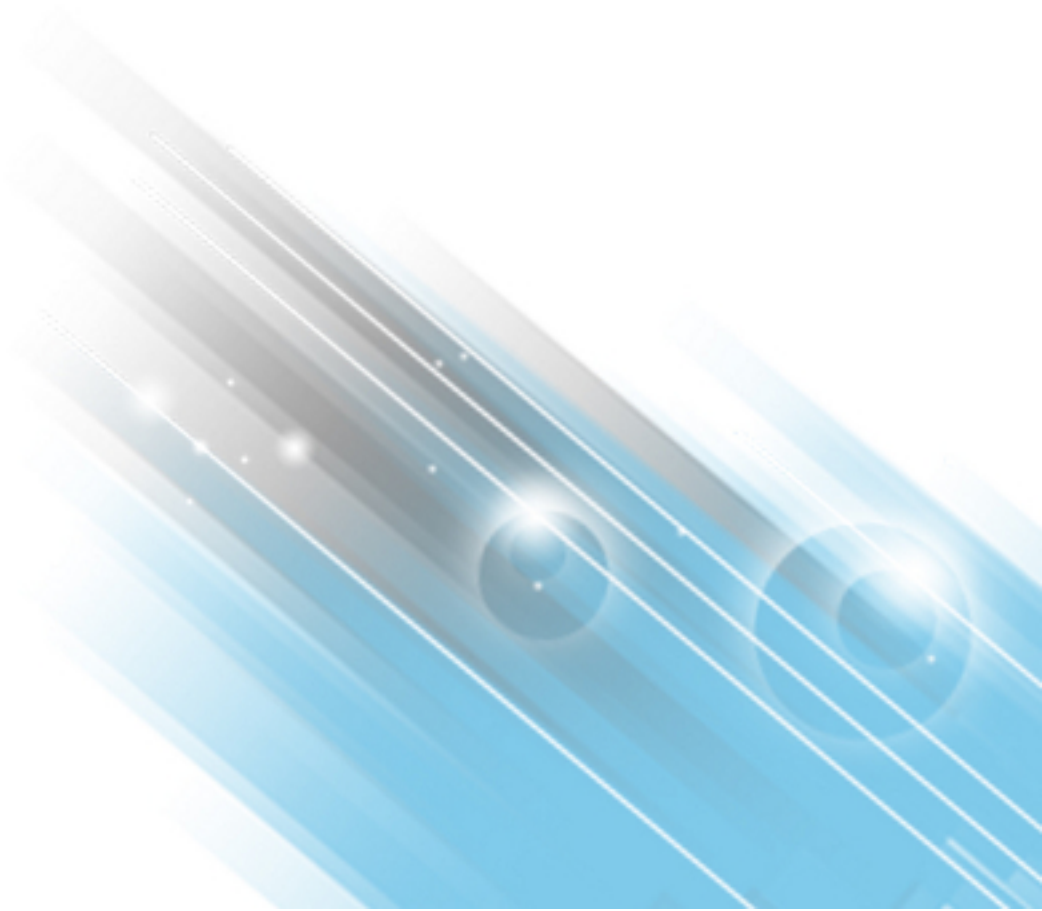
HP Value Stream

Software Version: 1.1

Request to Fulfill Concept and Configuration Guide



Document Release Date: April 2015

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 Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

SAP® is a registered trademark of SAP AG in Germany and in several other countries.

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 Online 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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Part I: Request to Fulfill Concept Guide

Chapter 1: Request to FulFill Value Stream Concepts

This chapter includes:

Overview

The Request to Fulfill (R2F) Value Stream is a framework connecting the various consumers (business users, IT practitioners, or end customers) with goods and services that they need to drive productivity and innovation. Many IT organizations have multiple request catalogs addressing the needs of business users, IT practitioners, or end customers. The Request to Fulfill Value Stream brings these different request catalogs and consumer personas under a single consumption experience using the Offer Catalog. The value stream goal is to provide a blueprint for a unified experience that consistently engages consumers.

The Request to Fulfill Value Stream represents the consumption engagement model and goes beyond the traditional IT request management for goods and services. It fosters service consumption/fulfillment, knowledge sharing, and collaboration between communities of interest to improve service experience and enable self-service support. The life cycle begins with the consumption experience itself, based on an engagement portal which exposes a variety of opportunities to acquire services, goods, knowledge and/or support. Requests are captured using an Offer Catalog and fulfilled based on the content from one or more Composition Catalogs made available from internal or external providers.

The Offer Catalog makes it easy for a consumer to engage with and consume services from IT. In order to do so, it is imperative that catalog entries are created from the consumer point of view with provider technology choices and fulfillment complexity abstracted away. The catalog entries available for consumption can be tailored to different personas, roles, or functions using profiling. Catalog items within the Offer Catalog are associated with subscriptions. A subscription is a contract specifying a specific right to use a service or consume goods. Individual subscriptions are governed by overall service contracts and ensure that the service will be charged as agreed.

The Composition Catalog and individual service providers' capabilities are used to fulfill subscription requests captured by the Offer Catalog. The Composition catalog maintains the link between service components to underlying resources.

The Offer Catalog manages the composition of services from various Composition Catalogs.

Large enterprises often require multiple Composition Catalogs as fulfillments are provided by many providers—some may be internal while others are external.

Some IT organizations have multiple request catalogs to address different consumers and organize goods and services that can be ordered. The capabilities of each catalog can vary and lines between Offer and Composition Catalogs often blur, resulting in less than optimal conditions for the service request and fulfillment experience. The common limitations for enterprises managing a request to fulfillment value stream include:

- A service consumption experience that provides technology/IT capabilities rather than valued services
- Multiple catalogs required for consumers to view and subscribe to available services
- Too many customer service requests requiring creation of fulfillment incidents or projects
- Lack of service subscription, usage, and chargeback traceability

Who Should Read This Guide

This guide explains the motivation to install and use the Request to Fulfill Value Stream. It describes what the value stream implementation will achieve, which ITIL processes it will answer, and describes the workflow between the products comprising the value stream.

This guide is intended for:

- Deployment technicians
- Quality automation engineers
- IT personnel
- Network managers
- Presales and sales personnel
- PSO
- Anyone who wants to learn about the end-to end service monitoring and event management best practices as well as incident management and change management

The information in this guide may duplicate information available in other Value Stream 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.

Request to Fulfill Value Stream Objectives

The Request to Fulfill Value Stream places emphasis on time-to-value, repeatability, and consistency for consumers looking to request and obtain services from IT. Optimize both service consumption and fulfillment experiences by delineating functions for an Offer Catalog and Composition Catalogs.

Today IT organizations struggle to increase the ratio of self-sourced fulfillments over workflows requiring direct human support. Many fulfillments today too much intervention that consumes valuable IT resources. By increasing self-sourced fulfillments, companies will see improved business velocity reduction in friction. They will also be able to reduce “shadow sourcing” within the business because of more responsive consumption experiences. Today’s IT is focused on delivery of technical capabilities —tomorrow’s IT must be positioned to focus on self-service consumption of multi-sourced services.

The value stream underlines the importance of deploying standard changes (a form of request management) rather than normal changes for internal fulfillments. Normal, risk-assessed and individually approved changes are one of the most time consuming and resource intensive activities in an IT organization. Service fulfillments should be based on predefined models where request criteria and approvals are collected at the start and fully automated fulfillment processes orchestrate all necessary provisioning and standard changes.(Note that Change Management per se is part of the Require to Deploy value stream.)

The Request to Fulfill Value Stream plays an important role in helping IT organizations transition to a service broker model. Enterprise customers have been using external suppliers for goods and services for many years. The IT multi-sourcing environment will accelerate as companies adopt cloud computing offerings like Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The Request to Fulfill Value Stream aggregates service catalog items from multiple supplier Composition Catalogs, along with internal fulfillments, as a single consumption experience through the Offer Catalog. IT provides a single consumption experience to consumers for seamless subscription to both internal and external services, as well as managing subscriptions and routing fulfillments to different service providers using the Request to Fulfill Value Stream framework.

The Request to Fulfill Value Stream also describes the life cycle of a service delivered to consumer. The delivery of a service request through fulfillment is not the end of the life cycle. A service request may result in a subscription to a service for a period of time. A consumer loses their right to use the service after reaching the end date of the subscription. The life cycle requires a service requesting capability, a service usage metering capability, a charging, showback or cost allocation capability.

The key value propositions for adopting the R2F Value Stream are:

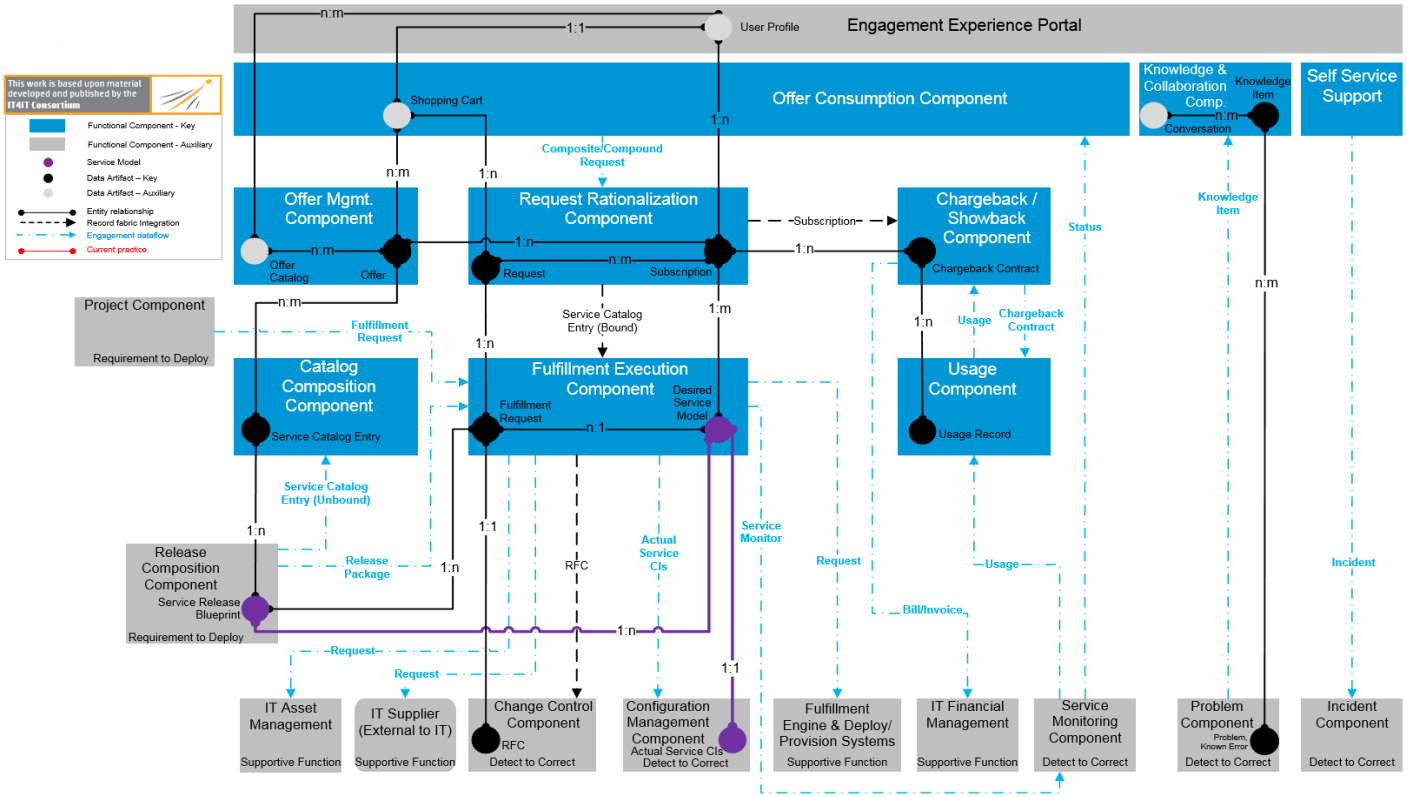
- Provide a portal and catalog blueprint for facilitating a service consumption experience that allows consumers to easily find and subscribe to services through self-service, regardless of sourcing approach
- Provide a functional framework between a single Offer Catalog and multiple Composition Catalogs
- Establish the model for moving from traditional IT request management to service brokerage
- Increase fulfillment efficiency through standard change deployment and automation

- Leverage the common service model to reduce custom service request fulfillment and design automated fulfillment
- Facilitate a holistic view and traceability across service subscription, usage, and charge-back
- Optimize costs by canceling expired subscriptions and reclaiming subscriptions and licenses that are unused

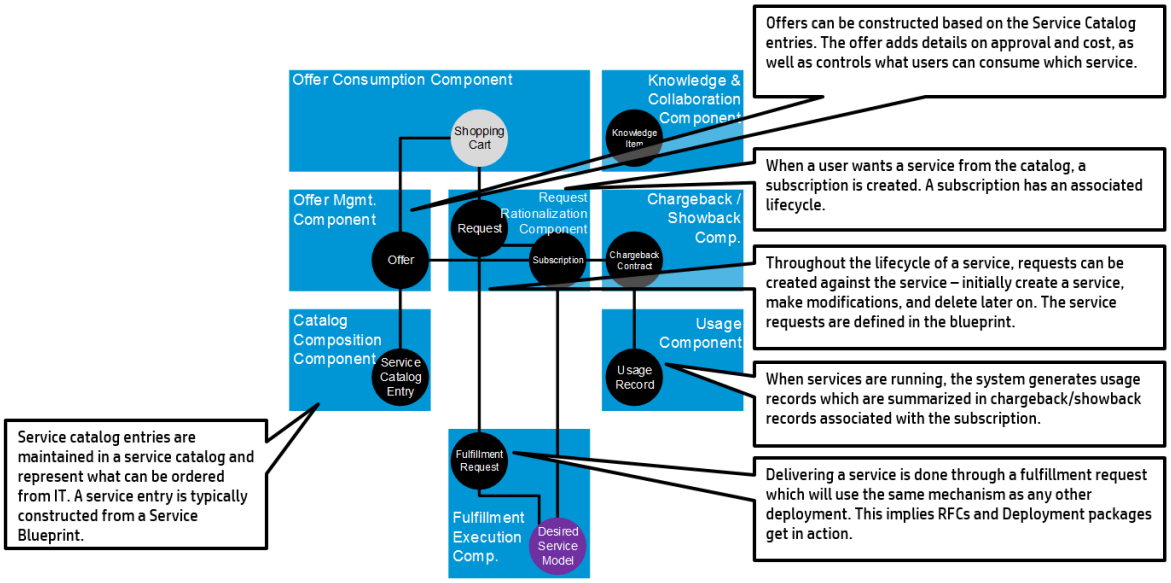
Note: For deployment and configuration instructions, see Part III: "Request to Fulfill Configuration Guide" on page 40.

Request to Fulfill Value Stream Diagram

The following diagram illustrates the Functional Components and Artifacts that comprise the Request to Fulfill Value Stream as described in version 1.3 of Reference Architecture.



Request to Fulfill Functional Components



The key functional components for this value stream are:

- **Self-Service Support.** Provide IT service consumers with a way to address more of their IT-related issues, as well as receive information regarding their existing records without necessarily engaging IT providers directly.
- **Knowledge & Collaboration.** Provide knowledge in the form of content and conversations that help to address the needs of IT Service consumers. Knowledge includes structured IT/supplier produced articles, or unstructured conversations from business/IT users, webinars, videos, training materials, and so on.
- **Offer Consumption.** Make services consumable to various classes of economic buyers and facilitate ordering IT services, supports saving partial activities, as well as supporting service bundles.
- **Offer Management.** Mash all composition catalog items and external supplier catalogs (by aggregating them) into consumable catalog items that users can order through Offer Consumption.
- **Request Rationalization.** Rationalize and break down Composite/Compound Requests into individual bound service catalog entries that can then be routed to fulfillment. In addition, this functional component also manages the life cycle of all subscriptions related to the requests
- **Chargeback/Showback.** Associates the price of Services ordered to the relevant organization. The association enables the implementation of the charging policy, be it notional, or actual chargebacks. The calculation of price may take into consideration subscription and usage information.
- **Catalog Composition.** Create and manage the service catalog entries in the underlying

Composition Catalogs that are aggregated and made available by Offer Management.

- **Fulfillment Execution.** Generates and manages the execution of all Fulfillment Requests necessary in order to provide the Services ordered. Engages the underlying Fulfillment Engines and returns the status of their actions back to Request Rationalization.
- **Usage Management.** Track actual usage of subscribed services by gathering service usage metrics, activity, and history for all services.
- **Engagement Experience Portal (Auxiliary Functional Component).** Create a unified experience for the consumption of all services and engagement of IT. This experience remains consistent regardless of the underlying systems, providers fulfilling the requests.

Request to Fulfill Artifacts

The Request to Fulfill (R2F) Value Stream contains both key and auxiliary artifacts that interact with the configuration items that comprise the service model.

The artifacts for this value stream are:

- **Chargeback Contract.** An artifact within the R2F Value Stream managed by the Billing/Chargeback/Showback Functional Component. It is the required payment for IT services used.
- **Conversation.** Represents the interactions between users related to IT topics. These conversations may be used to create new knowledge, or to recognize subject matter experts in different domains within IT.
- **Desired Service (CI).** Desired Service is a service model that describes how the service should look after it has been instantiated. The Desired Service state describes the desired state of the service. This state reflects the instantiation of the service that realizes a specific request for the service.
- **Fulfillment Request.** Managed by the Request & Routing Management Functional Component. Represents the breakdown of requests needed in order to fulfill a subscription.
- **Knowledge.** Structured and unstructured knowledge from Knowledge Management.
- **Offer.** Defines how a service catalog entry will be instantiated and under what terms and conditions—price, deployment, approval, workflow, Service Level Agreements (SLA), and so on.
- **Offer Catalog.** A set or collection of offers that are grouped together as something that can be consumed by certain consumers or consumer groups.
- **Request.** An artifact representing the need to invoke fulfillment from suppliers, or an internal fulfillment such as an asset being provided by Asset Management.
- **Request for Change (RFC).** A shared artifact that was previously defined in the Requirement to

Deploy (R2D) Value Stream. In this context, it is used to capture any changes needed as a result of run book execution or operational modifications needed to restore the service to a usable state.

- **Service Catalog Entry.** A logical service model within the R2F Value Stream managed by a Catalog Management Functional Component. It is an authoritative source for the consolidated set of services that can be consumed. An unbound part of the superset of service definitions is available for promotion to the status of Offer. A catalog entry would need to be bound to aspects relating to the delivery of the service such as price, deployment, approval, workflow, and SLA in order to be promoted to Offer.
- **Service Catalog Entry (bound).** This is an instantiation of the unbound service catalog entry, which is the binding of the relevant parameters that determine how a service will be deployed. This results in a single realized deployment for the service. The parameters are set by the user's selections made in the Shop/Buy/Pay/Manage Functional Component, as well as the determinations made in the design of the service which are interpreted by the Request & Routing Management Functional Component.
- **Service Release Blueprint.** Service Release Blueprint is a part of the realized service model that contains description and procedures necessary to activate, deploy, and operate a service or application. The Service Release Blueprint is a part of the release package and describes the elements contained in the release package.
- **Shopping Cart.** Enables ordering IT services in a manner that is consistent with other online shopping experiences.
- **Subscription.** Managed by the Subscription Management Functional Component. This artifact represents a service that has been provided to a consumer.
- **Usage Record.** An artifact within the R2F Value Stream managed by the Usage Management Functional Component. It is the actual (measured) use of a particular service or service component based on subscription. An example usage can be composed of (internal) hours, system usage (capacity, CPUs, and so on), or external supplier usage or costs.
- **User Profile.** Personal data associated with a specific user and the explicit digital representation of a person's identity. A user profile consists of different attributes managed by a user or consumed by other authoritative sources. User profile attributes must be secure, protected, and access restricted based on roles (for example, HR Manager) or system.

Part II: Request to Fulfill Use Cases

Chapter 2: Request to Fulfill Use Cases

This chapter includes:

Overview

The use cases in this document describe instances of using the Request to Fulfill Value Stream, which covers running the business of IT using an IT value chain-based IT operating model. Each request is fulfilled by streamlining the process to fulfill it.

Use Case 1: Request and Fulfill SaaS Online Business Service

To order (request) and consume (fulfill) a SaaS online business service is a real-life example of the generic use case. It describes the Request-to-Fulfill IT Value Stream's full service life cycle from the early order (request) phase until the fulfillment and consumption phase.

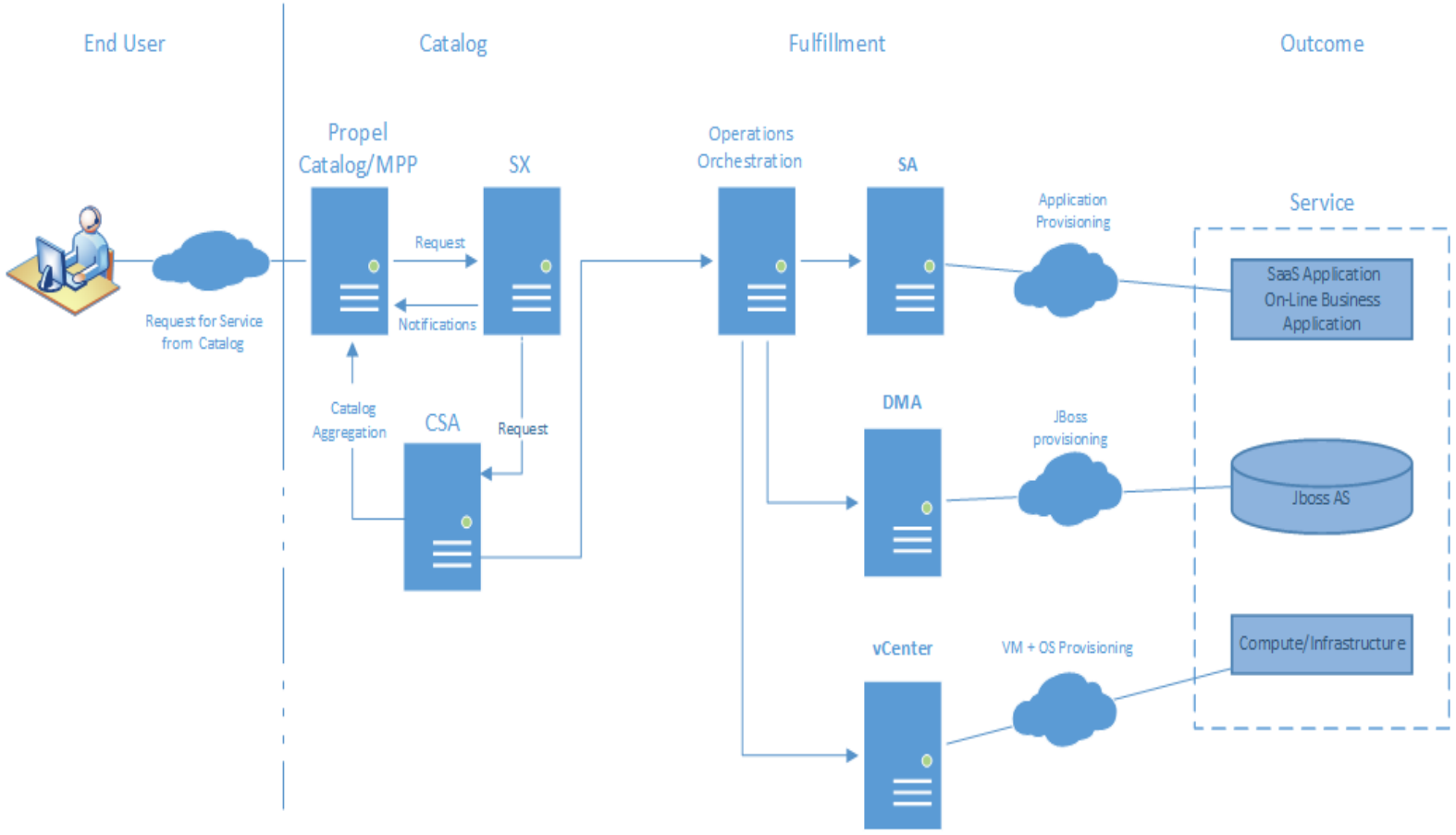
This section contains the following topics:

Overview

This use case describes a business request to implement a new SaaS-based financial application that provides new features and a better user interface when compared to the current existing financial application. The business request is prioritized and an IT project is executed to start delivering this new SaaS-based financial application service. Once the IT project has delivered the SaaS-based financial application services in the service catalog, finance employees can order the item. This use case begins once the IT project, based on proper approvals, delivers the SaaS-based financial application service into the service catalog.

Request and Fulfill SaaS Online Business Service Use Case Diagram

The following diagram illustrates the use case to request and fulfill a SaaS online business service:



Request and Fulfill SaaS Online Business Service

The service that is requested is a new financial business service for Finance employees—accessible from the financial employees' desktops. It is an IT service composed of three levels of deployment:

1. **Infrastructure.** Use compute services to provision a physical or virtual machine that will host the service platform and application
2. **Middleware / Platform.** Provision and configure an application server / database—for example, JBoss AS / MySQL—that will serve as the service platform
3. **Application.** Provision and configure the finance application

The service will be able to handle bookkeeping, accounting, and monitoring of cash transactions.

This section contains the following steps:

Step 1: Plan and Create the Service Design (Modeling)

The selected financial business service (known as Cyclos) is based on the deployment of three levels. The first level is the infrastructure, which provides compute services for the operating system (MS-Windows 2008 R2 Server). Middleware is the second level and includes the application server (Red-Hat Jboss 5.1.1) serving as the application infrastructure. Finally there is the application level. This level includes the Cyclos finance application that completes the business service topology.

HP Cloud Service Automation (HP CSA) Service Design enables you to build and develop the actual topology. This topology is based on two to three resource offerings that consist of one or more HP Operations Orchestration (HP OO) flows designed to execute at the specified life cycle state using an associated resource provider.

The following provisioning layers are needed to complete the service design:

1. **Infrastructure.** Provides compute services. VMWare Virtual Center is used for the virtual machine (and operating system) provisioning and HP Server Automation (SA) is used for the physical machine. For more information about SA, see the "HP Server Automation – Overview" on page 49.
2. **Middleware / Platform.** HP Database and Middleware Automation (DMA) is used for application server / database provisioning and configuration. For more information about DMA, see the "HP Database and Middleware Automation – Overview (Optional)" on page 49.

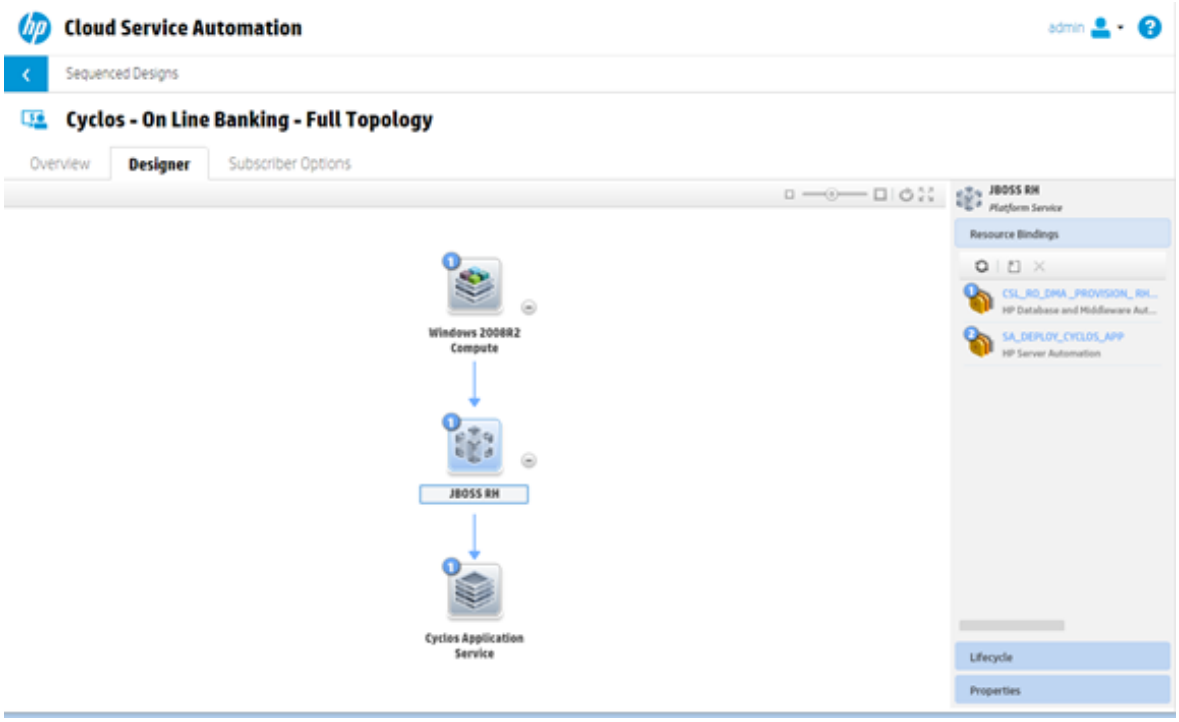
3. **Application.** HP Server Automation is used for application provisioning. For more information about SA, see the "HP Server Automation – Overview" on page 49.

Behind the scenes, HP OO serves as the Service Design **Orchestrator** that triggers each of the resource providers to run and complete its task.

Note: In the R2F environment, there are two different OO machines which act as follows:

- HP OO assists HP CSA in invoking all of the various fulfillment engines necessary throughout the fullfillment process.
- HP OO is an internal part of HP Propel's Service Exchange (SX) orchestrating the high level business flows.

The following figure shows how this example service design may look. The **Designer** tab (left pane) presents the service topology, while the right pane shows Resource Offerings that are in use.

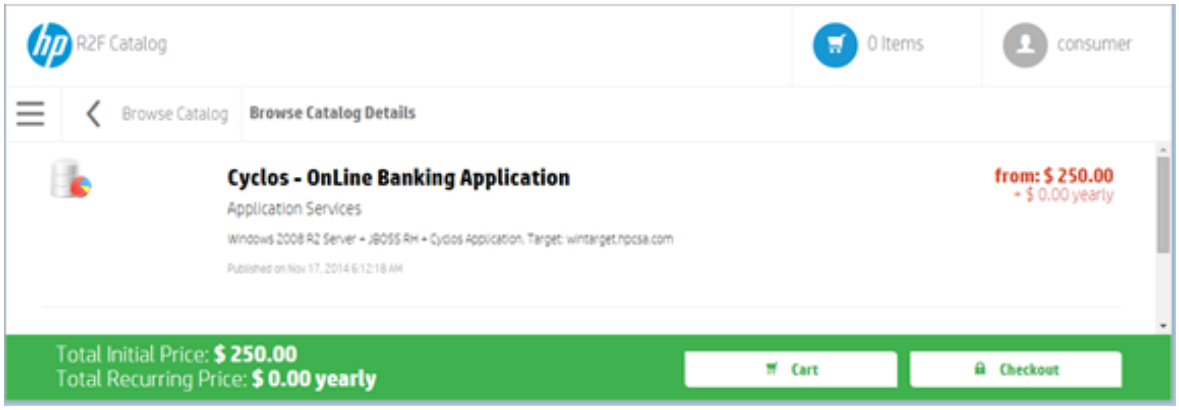


Once the service design is complete, the service can be published to the relevant CSA catalog (in the form of an Offering).

Before requesting the service from the HP Propel marketplace portal (MPP), first you must aggregate the HP CSA catalog into the HP Propel catalog. HP Propel SX provides adapters that communicate directly with HP CSA and HP Service Manager (SM) so that you can aggregate their product and service offerings into catalogs, which are then available in MPP. For details, refer to Appendix A, "Catalog Aggregation" on page 142 to learn how to aggregate the catalogs.

Step 2: Request the Service via HP Propel's Aggregating Portal

Once the HP CSA catalog has been aggregated to the HP Propel catalog and published in the marketplace portal, you may start requesting this service offering item. The following figure shows how the new service offering might look in the HP Propel catalog:



By clicking **Checkout** (and later clicking **Submit Request**), depending on the approval policy (if any), your service request is submitted.

Once the service request is approved, two entries appear in HP Propel's Service Exchange (SX):

1. An entry in the **Requests** table with the **Name** field containing your subscription name and with the **Status** showing as **Complete**.
2. An entry in the **Subscriptions** table with **Name** being your subscription name.

At this stage, the actual fulfillment process begins.

Step 3: Service Fulfillment Process

At this stage, SX communicates with HP CSA in order to run the business service provisioning process based on the service design created in Step 1.

The following are the expected tasks in order to complete the business service fulfillment:

1. **Infrastructure.** CSA instructs its associated HP OO to trigger the VMWare vCenter. Using an HP OO flow as an orchestrator, the vCenter provisions a virtual machine that includes MS-Windows 2008 R2 Server. The VM provisioning is based on a template with a sanitized SA agent.

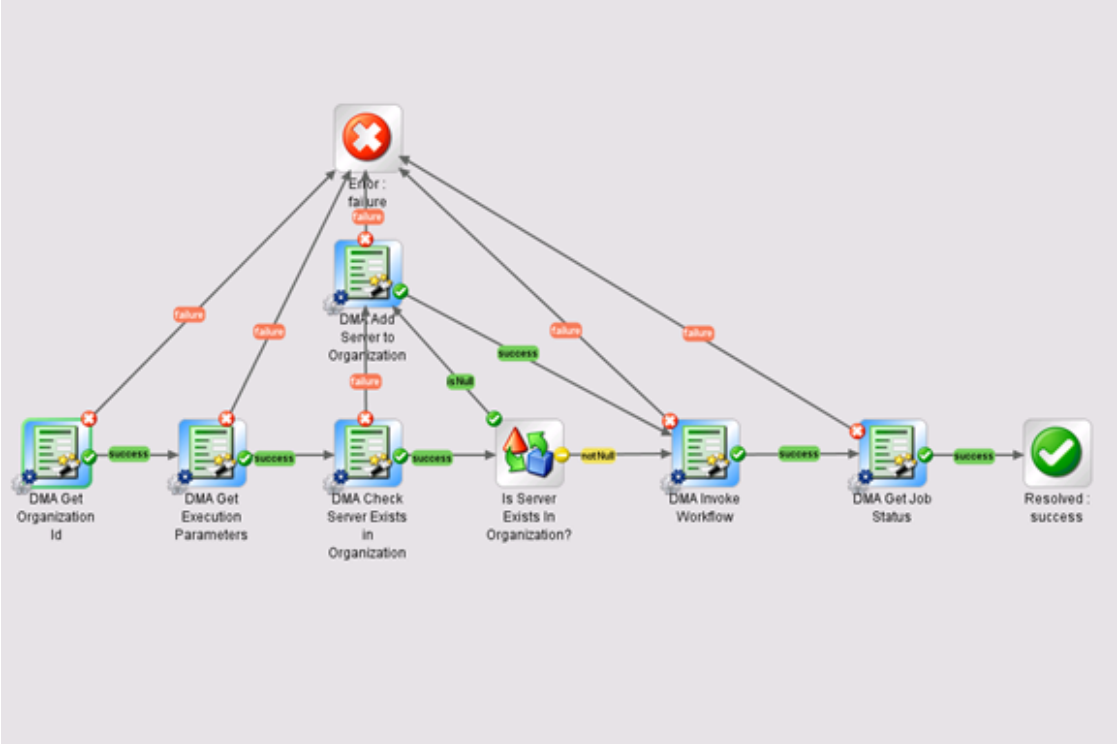
   Note: A VM template with a sanitized SA agent is mandatory for this task. For details, refer to Chapter 17, ""Sanitize" Server Automation Agent (Virtual Machine Template)" on page 117 to understand how to create the virtual machine template.

Expected result. The virtual machine, including MS-Windows 2008 R2 Server, with a sanitized SA agent, is up and running. The SA agent is needed for a few tasks—such as to enable the machine to be managed by SA and communicate with DMA. For more information, see Chapter 17, "“Sanitize” Server Automation Agent (Virtual Machine Template)" on page 117.

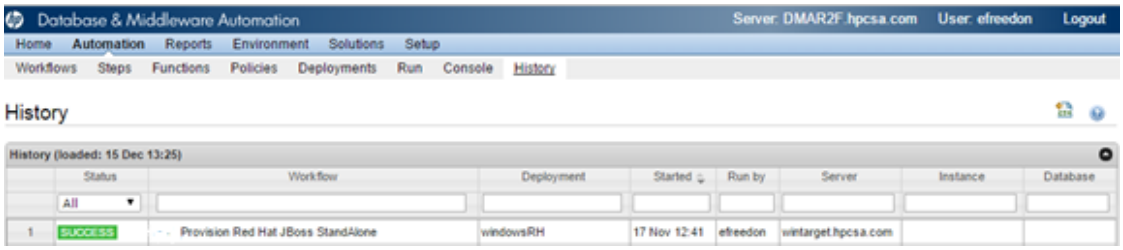
Once the compute task is fulfilled, the infrastructure provisioning task begins.

2. **Middleware.** CSA instructs its associated HP OO to trigger the DMA service provider. Using an HP OO flow as an orchestrator, the DMA’s Red-Hat JBoss Workflow is invoked and the provisioning job begins. Once completed, the Red-Hat Jboss 5.1.1 application server is up, configured, and ready to use.

   The following figure shows an example of the HP OO flow that triggers the DMA service provider (DMA application deployment).



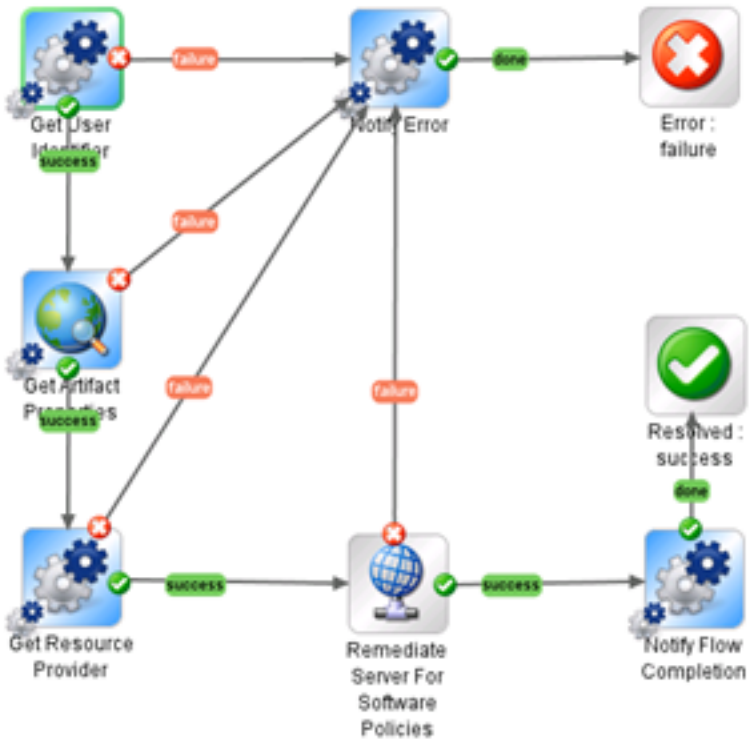
Expected result. Red-Hat Jboss 5.1.1 application server is successfully installed and configured above the already provisioned Windows 2008 R2 server VM.



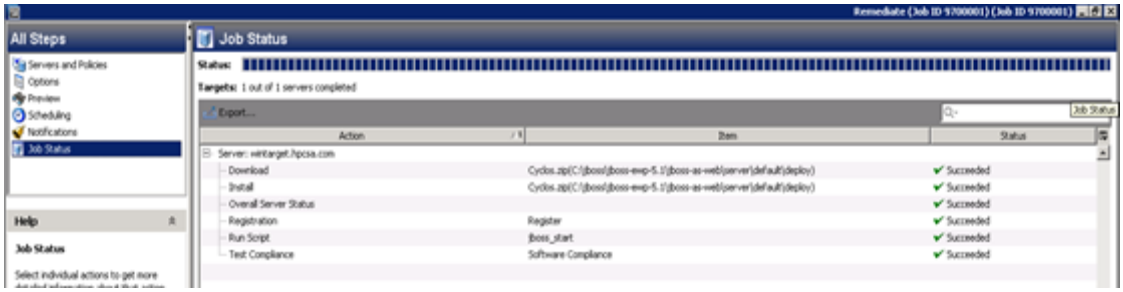
Once the infrastructure task is fulfilled, the application provisioning task begins.

3. **Application.** CSA instructs its associated HP OO to trigger the SA service provider. Using an HP OO flow as an orchestrator, the SA remediation server (or application deployment) job is invoked and the application deployment process begins.

   The following figure shows an example of the HP OO (associated with CSA) flow that triggers the SA service provider (remediate servers) to run a predefined software policy job called **Cyclos Software Policy**, which downloads the application to the VM, deploys the application, and starts the JBoss.



The following figure shows SA running the **Cyclos Software Policy** job and provisioning the application:

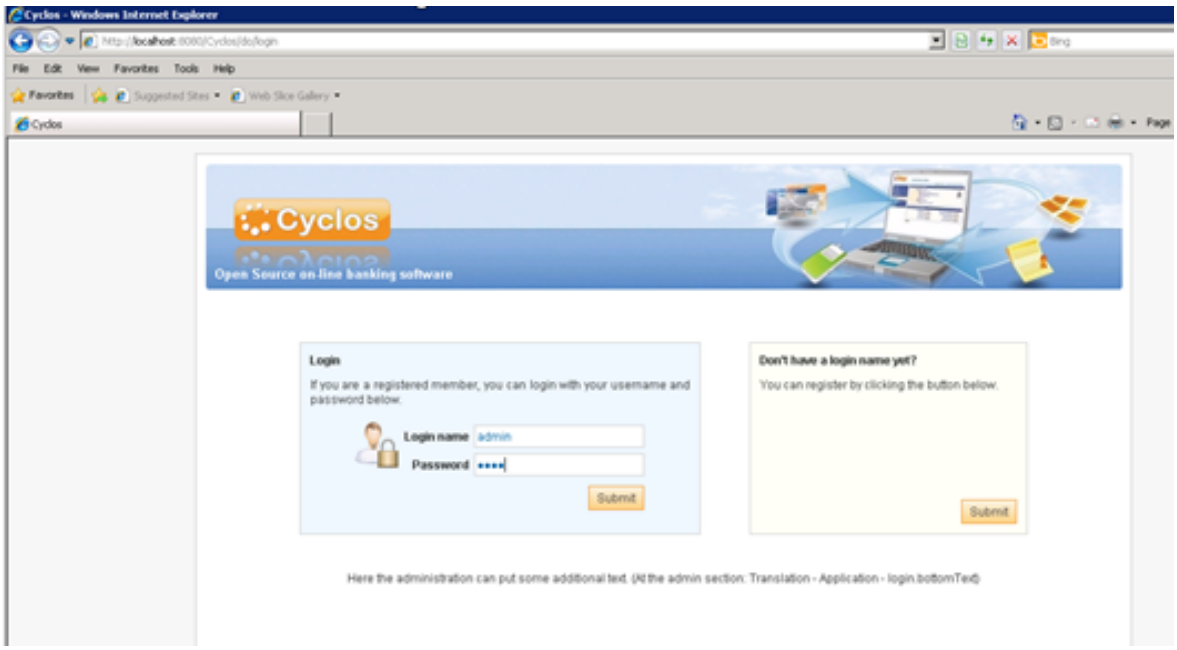


Expected result. The business service application is successfully installed and is up and running.

When you examine SX during this three-level process, you will see a few entries. The last entry will contain **Send completed notification (email)**. You will receive an email announcing that your subscription is complete.

Step 4: Consume the Service

At this stage, your business service is ready for you to log on and use.



You may check your subscription in the HP Propel portal and the HP CSA portal. You should be able to find your subscription (by subscription name) and its status should appear as **Active**.

You may check also that your associated request status is **Approved-Success**.

Use Case 2: Order New Employee Laptop

To order (request) and receive (fulfill) a new employee laptop is a real life example of the generic use case. It describes the full service Request-to-Fulfill life cycle from the early order (request) phase until the fulfillment and consumption phase.

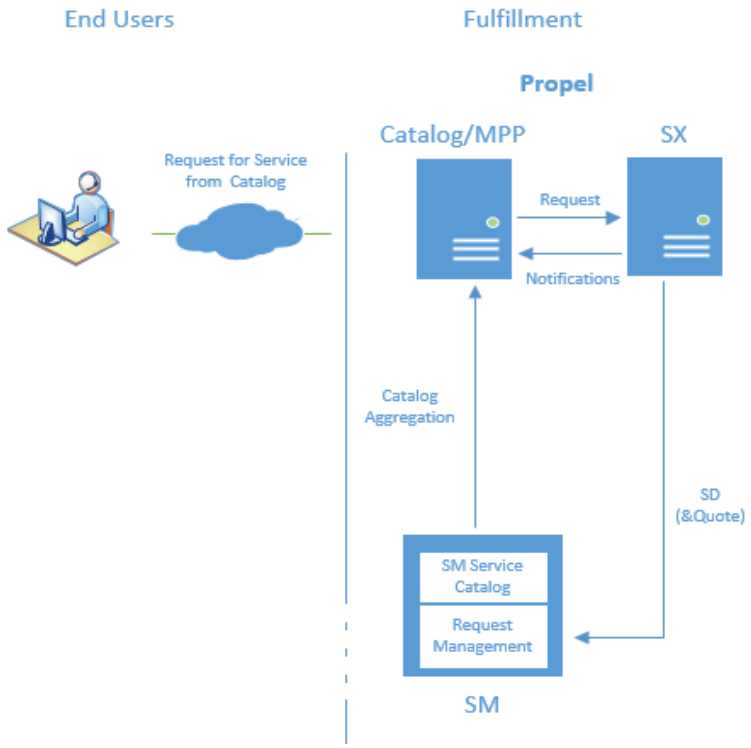
This section contains the following topics:

Overview

A new employee is about to join the organization. Based on the employee's job definitions, a new laptop needs to be ordered. Based on the laptop's predefined menu that appears in the HP Propel catalog (created by an aggregation of both the Service Manager catalog and HP Cloud Service Automation catalog), the new employee's manager/IT may order (and receive) the laptop on his behalf.

Request and Fulfill a New Employee Laptop Use Case Diagram

The following diagram illustrates the use case to request and fulfill a new employee laptop:



Request and Fulfill a New Employee Laptop Flow

This flow's goal is to order and receive a new laptop for a new employee. This request can be placed by the new employee's manager or an IT person.

This section contains the following steps:

Note: Request and Fulfill a New Employee Laptop Flow is based on SM Quotes. Therefore, the item which is going to be requested (that is, the **Basic PC Package**) should be configured to use the **Open New Request** connector and not use SM Subscriptions.

Step 1: Request the Service via HP Propel's Aggregated Portal

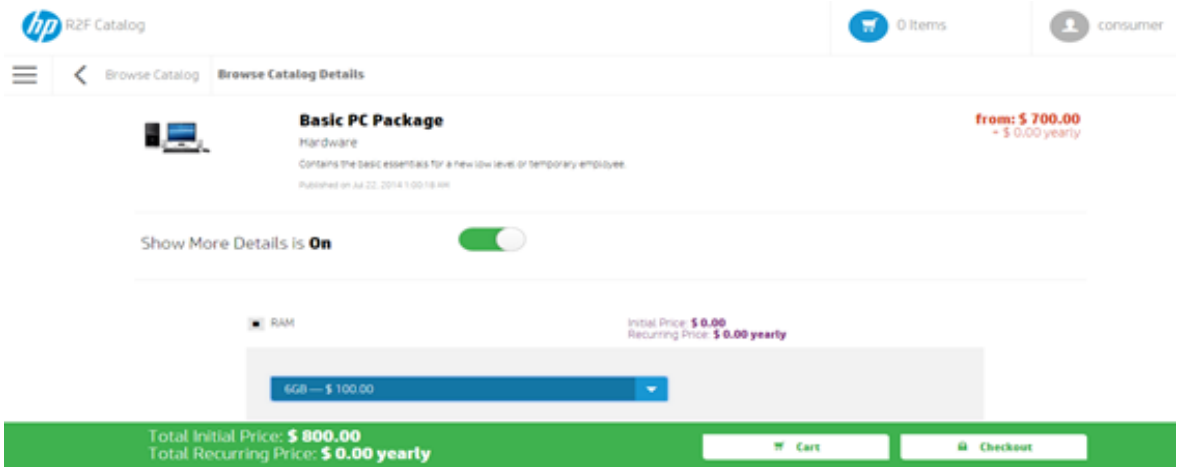
As mentioned in "Use Case 1: Request and Fulfill SaaS Online Business Service" on page 21, HP Propel provides adapters that communicate directly with HP CSA and SM so that you can aggregate their offerings of products and services into catalogs that are then available in HP Propel.

Before requesting the service from HP Propel's catalog, you need to first aggregate the SM catalog into the HP Propel catalog. For details, refer to Appendix A, "Catalog Aggregation" on page 142 to learn how to aggregate the catalogs.

Once the SM catalog has been aggregated to the HP Propel catalog, you may start requesting this service offering item.

Note: In order to request on behalf of someone else, first you need to use the corresponding widget. Then choose the relevant user the request is aimed for.

The following is an example of how the new service offering might look in the Propel catalog:

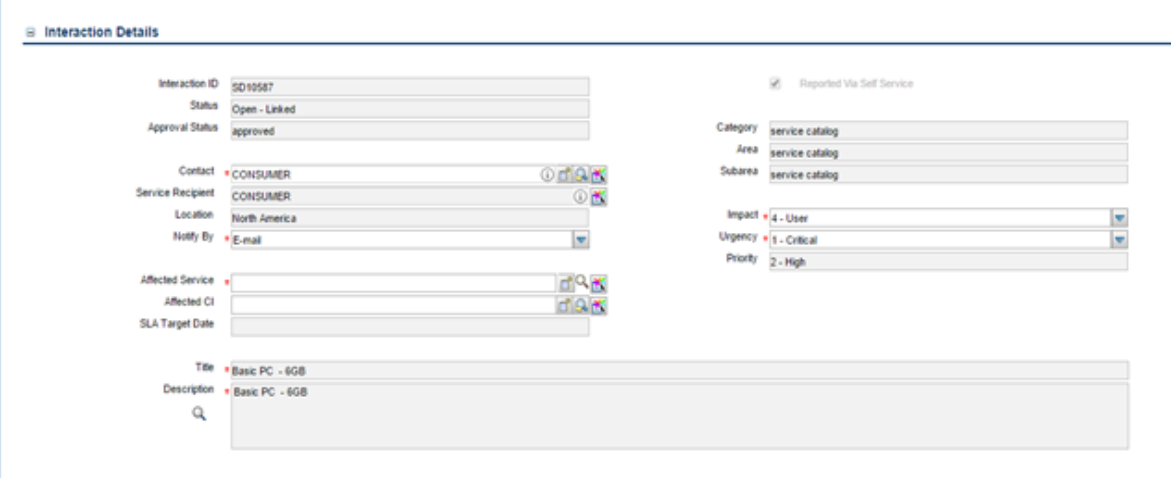


By clicking **Checkout** (and later clicking **Submit Request**), depending on the approval policy (if any), your service request is submitted.

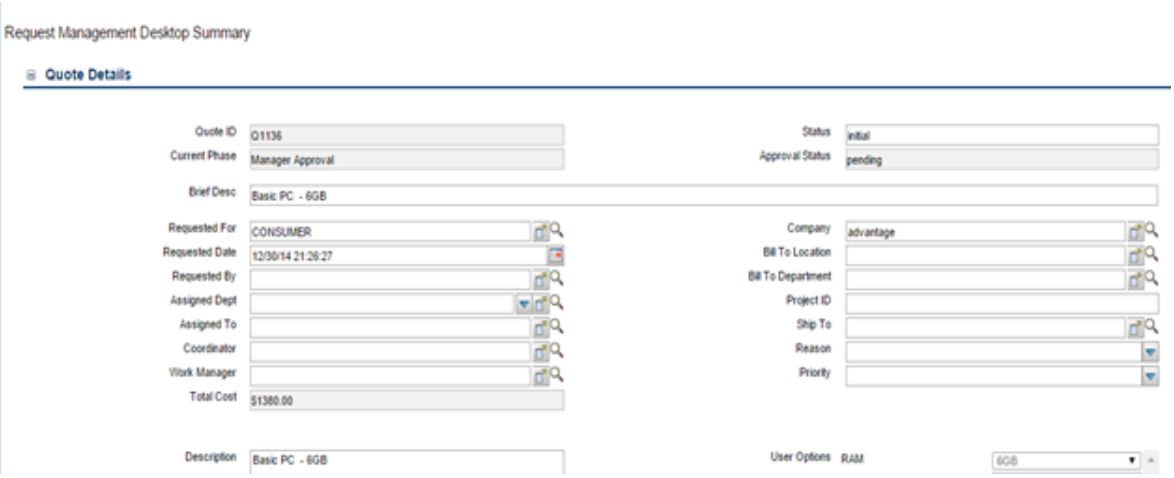
Once the service request is approved, your service request is submitted to SM via SX.

At this stage in SX, you will find an entry in the **Requests** table, with the **Name** field containing your subscription name and with the **Status** showing as **pending_approval**. On the SM side, an **SM interaction (SD)** and a related **SM Quote** are created as follows:

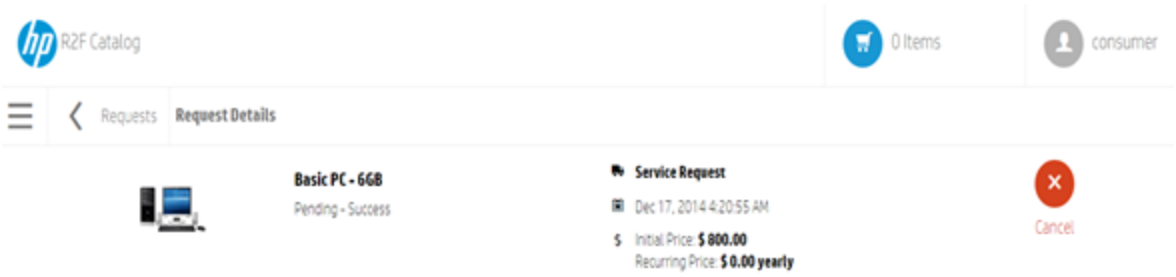
SM interaction (SD)



Related SM Quote



Then, in the HP Propel catalog, you may find your request with the status pending as follows:

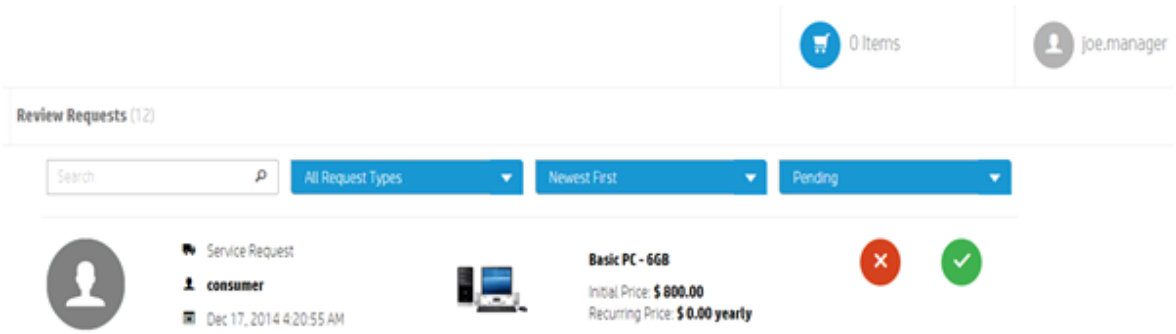


At this stage, the actual fulfillment process begins.

Step 2: Fulfillment Process

Once the request is placed, it should be reviewed and Approved/Denied.

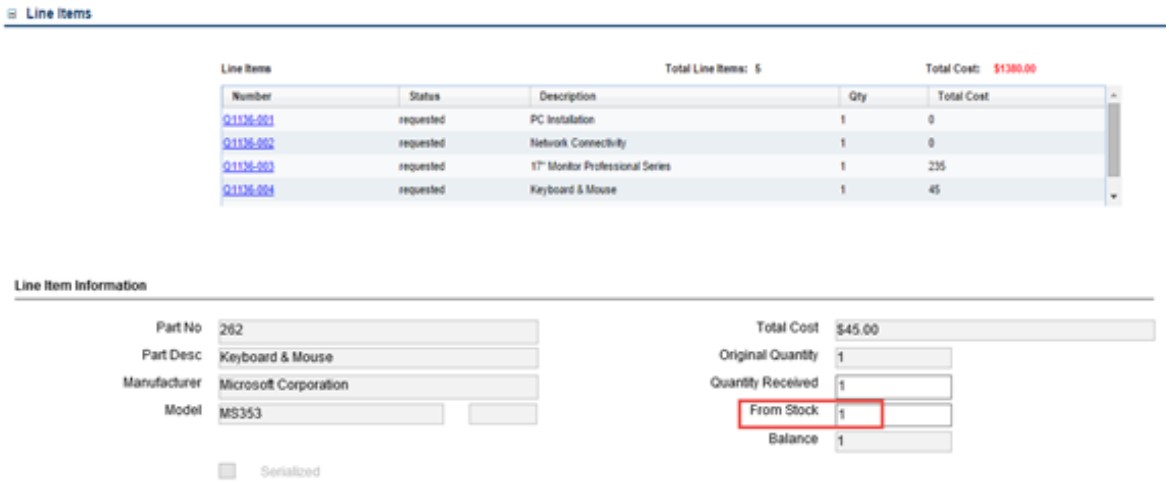
In order to do so, the request reviewer/approver (that is, joe.manager) logs into HP Propel's catalog using his credentials. He reviews and examines the pending request and decides whether to approve or deny it—for example:



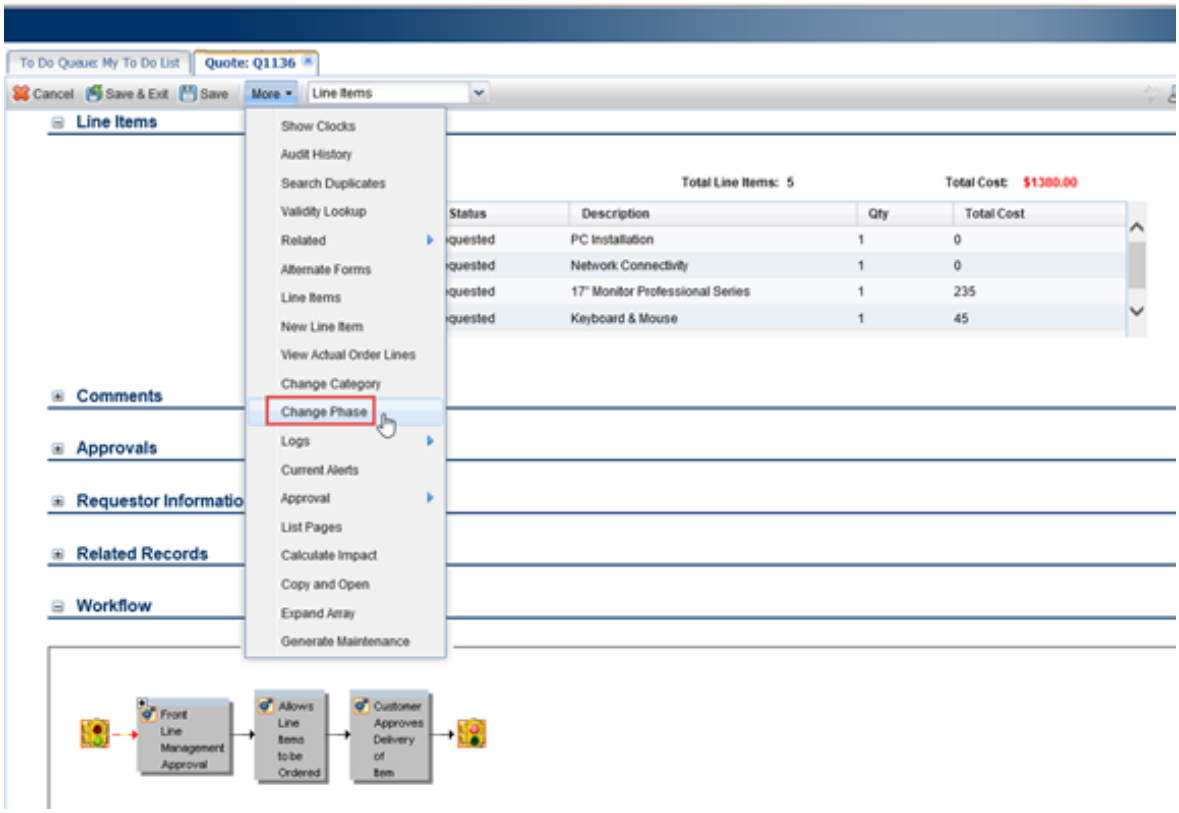
Once approved, you may find the following:

- **Service Exchange (SX).** An entry in the **Requests** table with the name **quotes.approve request SD10587** (corresponding to the SD ID example). Also, the request status is approved.
- **Service Manager (SM).** Check the quote. The **Current Phase** should be equal to **Ordering**. Approval Status should be equal to **Approved**.
- **Propel's Catalog (as the requester).**
  - Subscription status is **Pending**.
  - Associated request status is **Approved-Success**.

At this stage, if there are any Line Items in the quote (such as PC accessories), the Line Items should be handled and complete—for example:

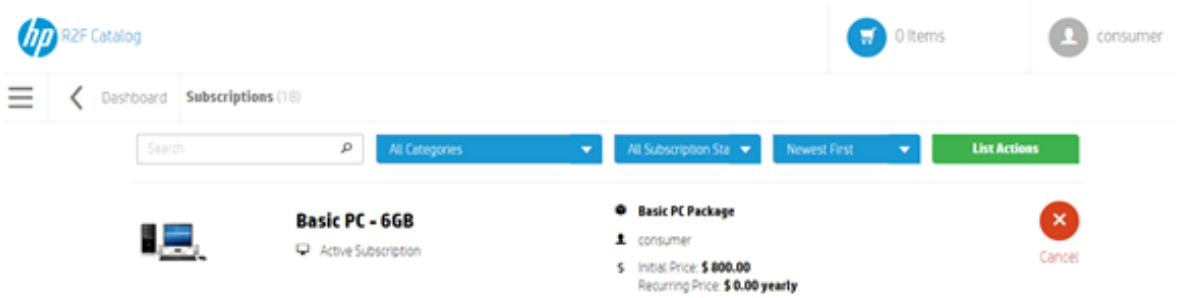


Once the Line Items are resolved, the quote phase is moved to **Customer follow-up** where the Customer (Requester) should approve the Laptop delivery.



Next SX updates the **Requests** table with a corresponding entry containing the status **in_progress** and sends a confirmation email to the requester.

Once the requester confirms the delivery by the corresponding link, both the SM quote and its related SM interaction (SD) are closed. Then the subscription is **Active**.



Use Case 3: Employee Onboarding Bundle

HP Propel catalog also offers the option to bundle services residing in the aggregated catalog into one service offering. In this section, an employee onboarding bundle is presented.

This section contains the following topics:

Overview

The use cases described in "Use Case 1: Request and Fulfill SaaS Online Business Service" on page 21 and "Use Case 2: Order New Employee Laptop" on page 29 present the Request-to-Fulfill flow based on a service offering that contains one service.

In some cases, you might like to have an offering that contains more than one service. A good example might be employee onboarding. A common employee onboarding needs, of course, many items—such as a desktop PC/laptop, cell phone, software licenses, ID badges, and so on.

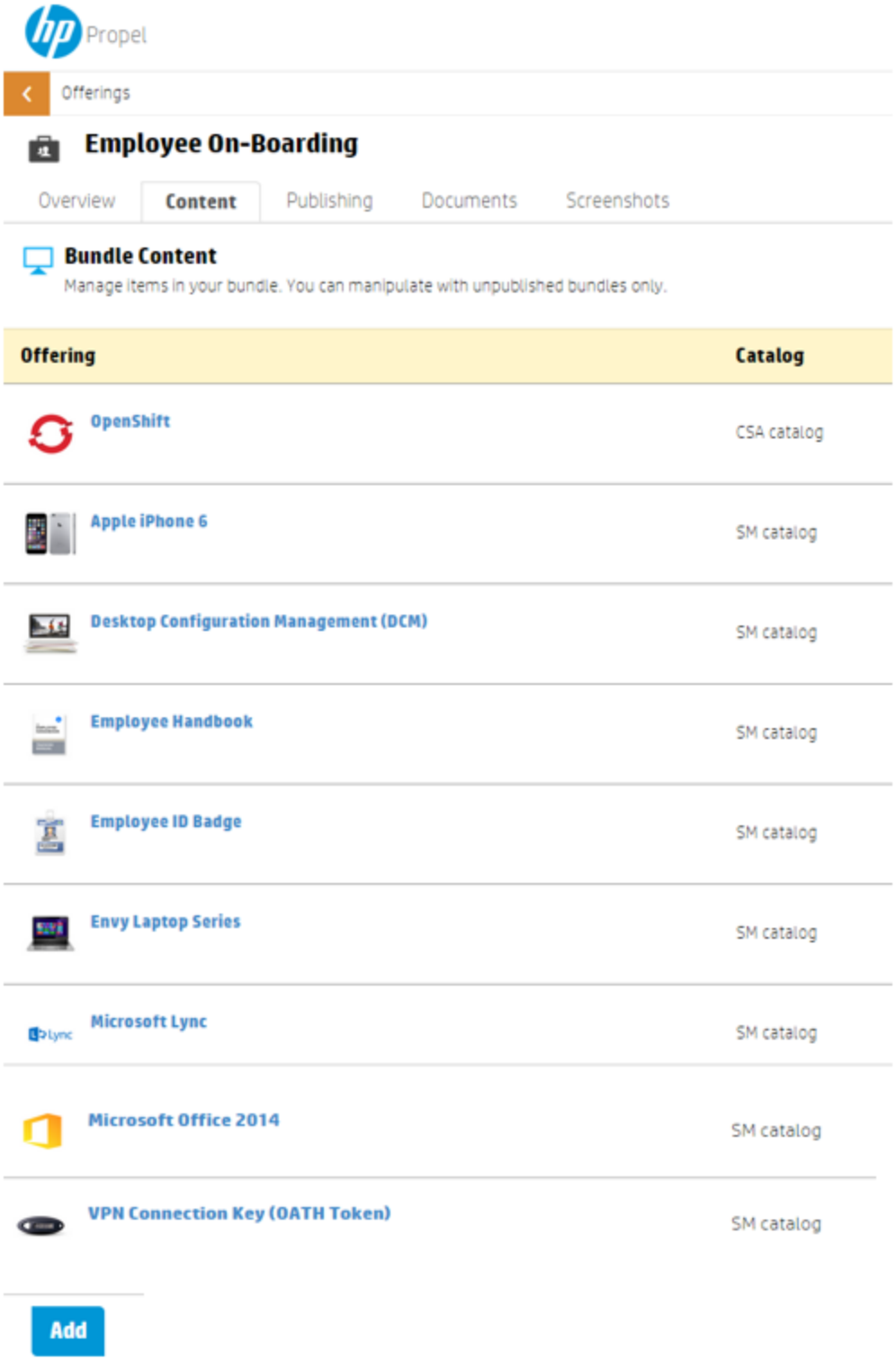
In order to avoid ordering each item/service separately, a predefined employee onboarding bundle offering saves time and is easy to follow and manage.

Create an Employee Onboarding Bundle Offering

Before you create any bundled offering in HP Propel's catalog, you first need to aggregate the SM/CSA/both catalogs into HP Propel's catalog. Creating a bundled offering can only be based on offerings that already exist in HP Propel's aggregated catalog. For details, refer to Appendix A, "Catalog Aggregation" on page 142 to learn how to aggregate the catalogs.

Creating a bundled service offering in the HP Propel catalog is similar to the way a single service offering is created in HP CSA. The main difference is adding more than one offering to its content.

The following figure shows the offering loaded with a few services that a common employee onboarding bundle might contain.



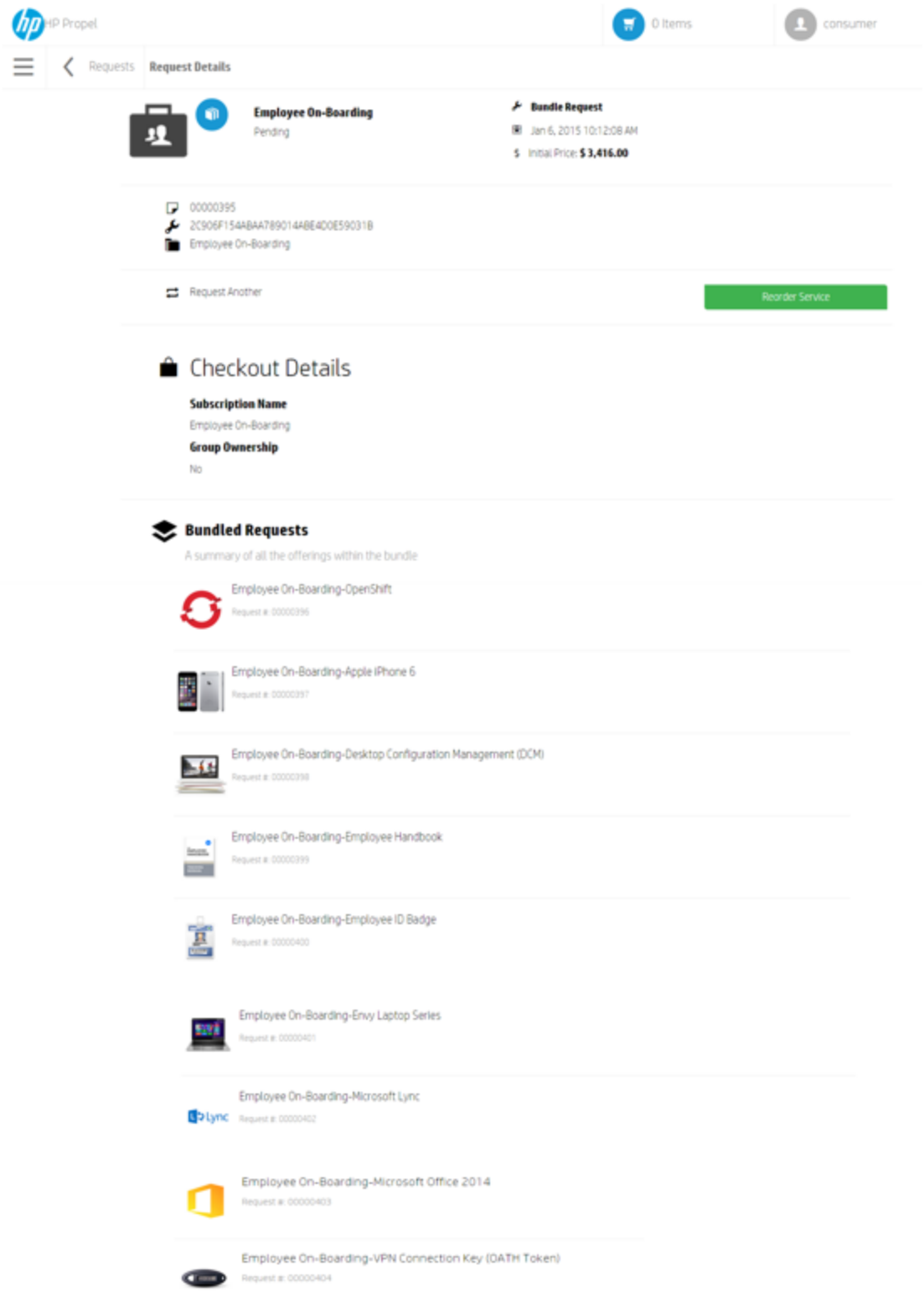
Once completed, the bundled offering is published to the catalog and is ready to be consumed.

Request and Fulfill the Onboarding Service Bundles

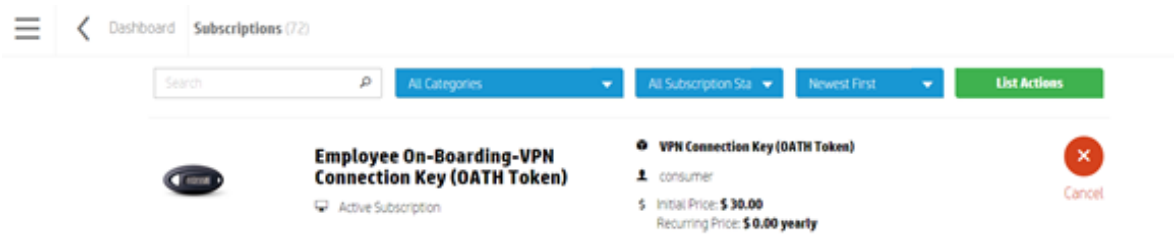
Requesting a bundled offering is done in a similar way to an offering that contains a single service. Once the user logs on to the portal, he also finds (in addition to the other published offerings) the recently published employee onboarding bundled offering.

By clicking **Checkout** (and later clicking **Submit Request**), depending on the approval policy, if any, the service request is submitted. As a result, a bundle of corresponding requests are issued.

As shown in the following figure, the main request ID appears in the request header pane and the list of bundled requests appears in the Bundled Requests pane.



Once the requests are submitted, the fulfillment of each embedded offering is executed in the same way as described in Use Cases 1, 2, or both—depending on the use case flow. At the end of the process, a related subscription appears for each embedded offering, wrapped with a prefix as the request name—for example:



Part III: Request to Fulfill Configuration Guide

Chapter 3: Request to Fulfill Value Stream Configurations

This chapter includes:

Overview

The balance of this guide provides the information necessary to implement the integrations needed to achieve the preferred IT management ecosystem. The user decides how many configurations to implement in order to achieve the management level required.

Feel free to use the entire solution, a mix of the various products, or just use a single product to address your monitoring needs.

Note: Throughout this document, italicized text enclosed in angle brackets (for example, "<your_server_name>") indicates replaceable text.

Prerequisites

This guide expects that the following products are installed and fully functional.

- **HP Propel.** Both Service Exchange and Catalog are installed, configured, and up and running.
- **HP Universal CMDB.** Server is installed. Data flow probe is connected and running (different server than BSM server).
- **HP Asset Manager.** Server, Client, and Web client are installed.
- **HP Connect-It.** Installed.
- **HP Cloud Service Automation.** Server is installed.
- **HP Service Manager.** Server, Client, Help Server, Web Tier, and Knowledge Management are installed and running.
- **HP Operations Orchestration.** Central and Studio are installed, including CSA Content Packs.
- **HP Server Automation.** Server and Client are installed, configured, and up and running.
- **HP Database and Middleware Automation (Optional).** Installed, Configured, and up and running.

Hardware and Software Requirements

This section contains the following topics:

Supported Versions

Note: For the hardware and software requirements, see the product documentation.

Product	Version	Instructions
HP Propel	• 1.10 or later	For installation instructions, see the *HP Propel version 1.10 Installation and Configuration Guide*.
Cloud Service Automation	• 4.10 or later	For installation instructions, see the *HP Cloud Service Automation version 4.10 Installation Guide*.
Service Manager	• 9.32 or later	For installation instructions, see the *HP Service Manager version 9.30 Interactive Installation Guide* and then select *Release Notes version 9.32*.
Universal CMDB	• 10.01 or later	For installation instructions, see the *HP Universal CMDB version 10.01 Interactive Deployment Guide*.
Operations Orchestration	• 10.10 or later	For installation instructions, see the *HP Operations Orchestration version 10.10 Installation Guide*.
Asset Manager	• 9.32 or later	For installation instructions, see the *HP Asset Manager version 9.32 Release Notes*.
Connect-It	• 9.50 or later	For installation instructions, see the *HP Connect-It version 9.50 User Guide*.
Server Automation	• 10.01 or later	For installation instructions, see the *HP Server Automation version 10.0x All Manuals Download*.
Database and Middleware Automation (optional)	• 10.21 or later	For installation instructions, see the *HP Database and Middleware Automation version 10.21 Installation Guide*.

Note: Make sure that each application you install is up and running before you perform any configuration steps.

Enterprise Hardware and Software Requirements

Note: The following tables detail the deployment environments that have been rigorously tested by HP quality assurance personnel.

For the complete listing of hardware and software requirements, see the relevant Support Matrix for each product.

- **HP Propel.** For more information, see the *HP Propel version 1.10 System and Software Support Matrix*.

  HP Cloud Service Automation. For more information, see the *HP Cloud Service Automation version 4.10 Support Matrix*.
- **HP Service Manager.** For more information, see the *HP Service Manager version 9.32 Compatibility Matrix*.
- **HP Universal CMDB.** For more information, see the *HP Universal CMDB version 10.01 Support Matrix*.
- **HP Operations Orchestration.** For more information, see the *HP Operations Orchestration version 10.x Compatibility Matrix*.
- **HP Asset Manager.** For more information, see the *HP Asset Manager version 9.32 Compatibility Matrix*.
- **HP Connect-IT.** For more information, see the *HP Connect-IT version 9.50 Compatibility Matrix*.
- **HP Server Automation.** For more information, see the *HP Server Automation version 10.0x Compatibility Matrix*.
- **HP Database and Middleware Automation (optional).** For more information, see the *HP Database and Middleware Automation version 10.21 Support Matrix*.

HP Propel – Overview

HP Propel allows IT departments to offer their services in an online shopping experience, similar to what users experience today at popular online retailers. Users may select from a variety of service providers, giving back to IT a level of control over the computing environment, while allowing their consumers to choose from a wide variety of sources.

Organizations that currently use HP Cloud Service Automation (HP CSA) and HP Service Manager (SM) will find HP Propel to be a useful extension of their current environment. HP Propel directly accesses the cataloging functions currently available in HP CSA and SM.

HP Propel provides adapters that communicate directly with HP CSA and SM so that you can aggregate their offerings of products and services into catalogs, which are then available in HP Propel.

HP Cloud Service Automation – Overview

HP Cloud Service Automation (HP CSA) is a unique platform that orchestrates the deployment of compute and infrastructure resources and of complex multi-tier application architectures. HP CSA integrates and leverages the strengths of several HP data center management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

HP Service Manager – Overview

HP Service Manager (SM) stores the managed or expected state of configuration items (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 SM CI record. You can add, remove, or update the managed fields that are part of the integration by tailoring the SM Web services that manage the integration.

SM 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 SM 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 Universal CMDB – Overview

HP Universal CMDB (UCMDB) consists of a rich business-service-oriented data model with built-in discovery of configuration items and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

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)). For example, the IT infrastructure of a large business represents a managed world, where the topology comprises multiple layers such as networks, protocols, databases, operating systems, and so on. You manage views to view the information in exactly the format you require.

Additionally, the information contained in the results of each TQL is updated automatically with the latest data entering the configuration management database (CMDB). As a result, once a TQL and View have been defined, they continue to provide up-to-date information about the current state of your managed world. Views appear in multi-level maps that enable you to identify key CIs, as required. You can also create reports (in HTML, Excel, or table format) about information collected by the system.

HP Operations Orchestration – Overview

HP Operations Orchestration (HP OO) is a system for creating and using actions in structured sequences (called Ops flows, or flows) which maintain, troubleshoot, repair, and provision your IT resources by:

- Checking the health of, diagnosing and repairing, networks, servers, services, software applications and individual workstations
- Checking client, server, and virtual machines for needed software and updates, and, if needed, performing the necessary installations, updates, and distributions
- Performing repetitive tasks, such as checking status on internal or external Web site pages

The two main components of HP OO are Central and Studio.

HP OO Central

This is a Web-based interface in which you can:

- Run flows
- Administer the system
- Extract and analyze data resulting from the flow runs

HP OO Studio

This is a standalone authoring program in which you can:

- Create, modify, and test flows, including flows that run automatically, as scheduled
- Create new operations

  You can create operations within Studio and run them in Central. You can also create operations that execute outside of Central in a remote action service (RAS). You do so in a development environment that is appropriate to the task, then associate the code you have created with an operation that you create in Studio.
- Specify which levels of users are allowed to run various parts of flows

HP Asset Manager – Overview

HP Asset Manager (AM) helps IT organizations minimize their compliance risk, effectively manage their IT services, and maximize the utilization of IT.

AM supports the life cycle management of physical and logical assets. AM's modules—Asset Tracking, IT Procurement, Contract Management, Software Asset Management and Financial Management—will ensure that IT organizations get full visibility on their portfolio and can smoothly run operations and optimize their use of IT.

AM's main benefits are described as follows:

- **Asset Tracking**
  - Track and manage fiscally relevant physical and virtual assets throughout their life cycle
  - Optimize IT spending
  - Reduce the number of lost and unused assets
  - Improve IT governance
- **IT Procurement**
  - Streamline IT procurement life cycle process
  - Optimize purchase costs by tracking vendor prices
  - Manage approvals and fulfillment of requests
  - Measure contract objectives against vendor delivery metrics

- **Contract Management**
  - Automatically manage the operational state of contracts in use
  - Track compliance with vendor terms and conditions
  - Link assets to contracts (purchase, leasing, maintenance, support contracts)
  - Monitor and re-evaluate contracts and suppliers
  - Optimize cost of IT contracts
- **Software Asset Management (SAM)**
  - Ensure vendor software license compliance using out-of-the-box SAM best practices
  - Allow organizations to optimize what is already owned
  - Enable active management for the authoritative state of software CIs
- **IT Financial Management**
  - Track cost of assets and business services
  - Define Service Offerings, manage user subscriptions
  - Support showback/chargeback for use of business services
  - Execute Budget Management Best Practices

HP Connect-It – Overview

HP Connect-It (CIT) is an Enterprise Application Integration (EAI) type integration platform. An EAI solution enables a company to integrate the different applications from which it can obtain or to which it can provide internal data (Internal support, equipment management software, and so on) or external data (ERP, B2B, B2C). Connect-It integrates not only data, but also a company's application processes.

You can use Connect-It to:

- Transfer information from one database to another
- Duplicate the information from one database to another in real-time
- Import information from e-mails, delimited text files, XML files or other formats into a database
- Export information from a database to e-mails, delimited text files, XML files or other formats
- Import NT Security-based information into a database

HP Server Automation – Overview

HP Server Automation (SA) is data center automation software that centralizes and streamlines many data center functions and automates critical areas of the data center's server management, including:

- Server Discovery
- Operating System Provisioning
- Operating System Patching
- Software Provisioning
- Audit and Compliance
- Application Configuration
- Application Deployment
- Software Compliance
- Reporting

SA allows changes to be made safely and more consistently, because you can model and validate changes before you actually commit the changes to a managed server. SA also provides methods to ensure that modifications you plan for your managed servers work the first time, because they have been tested before being applied, thereby reducing downtime.

HP Database and Middleware Automation – Overview (Optional)

HP Database and Middleware Automation (DMA) software automates administrative tasks like provisioning and configuration, compliance, patching, and release management for databases and application servers. When performed manually, these day-to-day operations are error prone, time consuming, and difficult to scale. Automating these tasks enables greater efficiency and faster change delivery with higher quality and better predictability. DMA provides role-based access to automation content. This enables better utilization of resources at every level:

- End-users can deliver routine, yet complex, database administrator (DBA) and middleware tasks.
- Operators can execute expert level tasks across multiple servers including provisioning, patching, configuration, and compliance checking.
- Subject matter experts can define, enforce, and audit full stack automation across network, storage, server, database, and middleware.

Chapter 4: UCMDB – SM Integration Configuration

This chapter includes:

Overview

This chapter describes the necessary steps to configure and verify the integration between HP Universal CMDB (UCMDB) and HP Service Manager (SM).

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

Set Up UCMDB for Integration with SM Using ServiceManagerAdapter9-x

This task lists the steps necessary to configure UCMDB in order to perform the integration with SM using ServiceManagerAdapter9-x.

This task includes the following steps:

Prerequisites

- Log on to the UCMDB system as an administrator.
- Verify that all UCMDB services are running (**http://<UCMDB FQDN>:8080/status/**).

Configure SM Adapter in UCMDB

To configure an SM adapter in UCMDB:

1. Browse to your UCMDB user interface.
2. Select the **Data Flow Management** tab.
3. Select **Adapter Management**.
4. From the resources window, select **ServiceManagerAdapter9-x** and expand it.
5. Expand the **configuration files** item.
6. Select **ServiceManagerAdapter9-x/sm.properties** from the list of items.
7. In the pane on the right side of the window, modify the **use.global.id** parameter, set it to **false**, and click **OK**.

Create a New Integration Point

To create a new integration point:

1. Navigate to **Data Flow Management > Integration Studio**.
2. In the Integration Point pane, click the **Create New Integration Point**  button. The Create New Integration Point dialog box opens.

   Enter the following information:

Name	Recommended Value	Description
Integration Name	SM Integration	The name you give to the integration point.

Name	Recommended Value	Description
Adapter	<user defined>	Select the appropriate adapter for the version of SM that you are using.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the SM server.
Port	<user defined>	The port through which you access SM.
Credentials	<user defined>	If SM credentials appear in the Credentials column, select them. If no SM 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 SM user name. The default value is **falcon**. **User Password.** Enter and confirm a password.
Probe Name	<user defined>	The probe is selected from a drop-down list.

Note: It is recommended to click the **Test Connection** button to verify that the details entered are working before continuing.

3. Click **OK**.
4. On the **Federation** tab, verify the **Incident**, **Problem**, and **RequestForChange** CI types are checked and click the **Save Integration** button.

Set Up the Data Push Job

To push CIs and Relations from UCMDB to SM:

1. Edit the **SM Push** job.
2. Select **Scheduler Definition**.

3. For the **Repeat** field, select **Changes Sync/All Data Sync**.
4. Set the **Repeat Every** field to **1 Day**.
5. Click **OK**.

Run the Data Push Jobs

To run the Data Push jobs:

1. In the Integration Point pane, select the correct integration.
2. Select the **Data Push** tab. The Job Definition pane appears.

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

3. Select your job and click **Full Synchronization**  .
4. When the Confirm synchronizing window appears, click **Yes**.
5. Click the **Statistics** tab to view the progress of the synchronization.
6. Click **Refresh** to view the updated synchronization status.

Run the Population Jobs

Note: To verify that population is working, create a new CI in SM.

To run the Population jobs:

1. Log on to UCMDB.
2. From the left-hand navigation pane, select **Data Flow Management > Integration Studio**.
3. In the Integration Point pane, click the correct integration.
4. Click the **Population** tab.
5. Select the **SM Configuration Items Population** job and click the **Full Synchronization**  button to run the population job.
6. When the Confirm synchronizing window is displayed, click **Yes**.

7. Click the **Refresh**  button and wait until the **Succeeded** message appears in the **Status** tab. The updated synchronization status appears.
8. Take the same action with the **SM Relations Population** job.
9. Log on to UCMDB and validate that the CI that was created in SM is validated in UCMDB.

Set Up SM for Integration with UCMDB

This task lists the steps necessary to configure SM, in order to perform the integration with UCMDB.

This task includes the following steps:

Prerequisites

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

Add the UCMDB Connection Information to the System Information Record

To add the UCMDB Connection Information to the System Information Record:

1. Log on to your SM 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 UCMDB 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 – SM Integration

To verify the UCMDB – SM Integration:

1. Browse to your UCMDB server.
2. Navigate to **Managers > Modeling > CI Type Manager**.
3. Under **Managed Object > ConfigurationItem > InfrastructureElement**, click **Node**.
4. Right-click a Node object and select **Show CIT Instances**. The CIT Instances window for the selected Node object appears.
5. From the list of CIT instances, select one CI and right-click **Properties**. The Configuration Item Properties window appears showing the UCMDB ID at the top of the window.
6. Click **OK**. The Configuration Item Properties window closes.
7. Click **OK**. The Show IT Instances window closes.
8. Browse to your SM server.
9. Navigate to **Configuration Management > Resources > Search CIs**.
10. Click the **Search**  button.
11. Click **More** on selected CI.
12. Select **Modify Columns**.
13. Click the down arrow and select your UCMDB ID, then click **Proceed**.
14. Verify that all the CIs from UCMDB are listed in SM and select the **Actual State** tab to view the CI properties in UCMDB.

Chapter 5: Populating UCMDB from AM

This chapter includes:

Overview

This section describes the necessary steps to configure and verify the integration between HP Universal CMDB (UCMDB) and HP Asset Manager (AM) as it comes out of the box, without customizing it to specific customer requirements. In this integration, IT management-related assets are copied from AM to UCMDB. Depending on the asset type, a CI is created and assigned a unique Global ID.

Configure Connection from UCMDB to AM

This section contains the following steps:

Step 1: Get the Adapter Content Package

1. Log on to **UCMDB**.
2. Browse to **Data Flow Management > Adapter Management**.
3. Expand **AMAdapter** from the resources list.
4. Expand **External resources** and select **AMadapter/Content.zip**.
5. Export to the local server and extract all files from **Content.zip**. The AMdatakit and AMDBUpdate folders are displayed. AMdatakit is used to sync dtLastModif among amAsset, amPortfolio, and amComputer tables.

Step 2: Import the Workflow into AM

1. Log on to **Asset Manager Client**.
2. Select **File > Import**.
3. Click **Execute a script**.
4. Browse the Content directory described in "Step 1: Get the Adapter Content Package" on the previous page.
5. Select **WF_SACM.scr**.
6. Enter the password and click **Import**.
7. Confirm the imported workflow by clicking **tools > workflow > workflow schemes** and find **Update dtRecCreation**.

Step 3: Create SQL Views in the AM Database

Caution: This batch file can only be used on Windows computers, not UNIX computers.

The batch file should be run from a computer where the client layers of the DBMS (for example, Oracle Database 10g Client R2) used for the AM database are installed.

Running this batch file alters the AM database structure.

Administrative privileges are required at the DBMS level to create the SQL views.

1. Set the ORACLE_HOME environment variable.
2. Run the create view script.
   a. Click **start > Run**.
   b. Enter **cmd**.
   c. Enter **sqlplus <schema name>/<schema password>@<SID_Hostname of oracle server>**.
   d. Enter **GRANT create ANY VIEW to <Username>**.
   e. Enter **GRANT SELECT ANY TABLE to <Username>**.
   f. Enter **GRANT create MATERIALIZED VIEW to <Username>**.
   g. Enter **Exit** to exit Oracle.

3. Browse to the AMDBupdate folder.
4. If using an Oracle server, run the command **CreateViews.bat Oracle <Oracle SID> <Username> <Password>**—for example, **CreateViews.bat Oracle SSG_labm3amdb35 SACM4 topaz**.

   If using an SQL server, run the command **CreateViews.bat [MSSQL2005|MSSQL2008] <Server> <Database> <Username> <Password>**.
5. Confirm all views created in the AM database.

Step 4: Create an Integration Point

1. Log on to **UCMDB**.
2. Browse to **Data Flow Management > Integration Studio**.
3. Click the **New Integration Point**  button.
4. In the New Integration Point dialog box, fill in the following **Integration Properties**.

Name	Recommended Value	Description
Adapter	AM Population and Federation Adapter 9.30 or later	Adapter to be used for the integration point.
Integration Name	AM Population and Federation Adapter 9.30 or later	Name given to the integration point.
Is Integration Activated	Selected	Select check box to create an active integration point.

5. In the Adapter Properties, fill in the relevant details as follows:

Name	Recommended Value	Description
Hostname/IP	<user defined>	Enter the hostname of the database server.
Database Type	<user defined>	Select the database type—Oracle or SQL.
DB port	<user defined>	Enter the database default port for Oracle 1521 and SQL 1433.
DB Name/SID	<user defined>	Enter the database name (MSSQL) or SID (Oracle) of the database.
Credentials ID	<user defined>	Click the **Add new connection details for selected protocol type** button. Enter the following information: ■ For the AM User Name, enter **Admin**. ■ For the AM password, enter the password of the AM log on. ■ For the database user name, enter the name of the schema. ■ For the database password, enter the password of the schema.
Data Flow Probe	<user defined>	Select the correct Probe from the drop-down list.
Push Back IDs	Enabled	Identify a unique CI if the feature is disabled and the reconciliation of CIs will not work.
Version	<user defined>	Select AM version.

6. Click **Test connection** and **OK**.

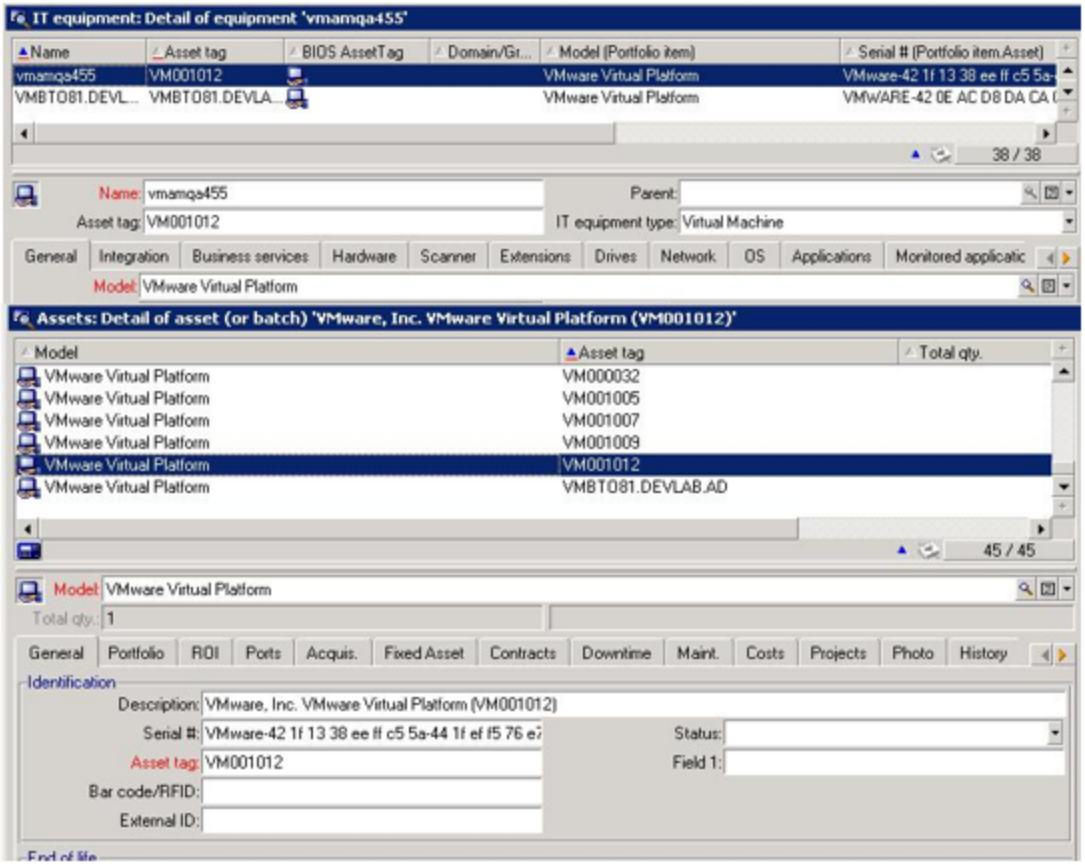
Verify UCMDB to AM Configuration

Note: On first use, run the full population job. After any changes are made, only run the **Delta Synchronization** population job.

In order to verify Asset Manager to UCMDB Population flow, create an Asset in Asset Manager, and verify it is synchronized as a configuration item in UCMDB.

To verify the UCMDB to AM configuration:

1. Log on to Asset Manager.
2. Create a new virtual machine in the IT equipment module, specifying its name and IT equipment type (in this case, **Virtual Machine**).



3. In the **Assets** view, add the serial number view, add the serial number.
4. Log on to **UCMDB**.

5. Browse to **Data Flow Management > Integration Studio**.
6. Select the **AM Population** integration point.
7. In the Integration Jobs pane, select the **Population** tab and click the **AM Population and Federation Adapter 9.30** job.
8. Click the **Full Synchronization**  button.
9. When the Confirm synchronizing window appears, click **Yes**.
10. Click the **Refresh**  button and wait until the **Succeeded** message appears in the **Status** tab. The updated synchronization status appears.
11. Browse to **Modeling > IT Universe Manager**.
12. Select the **Search CIs** tab and search for the name of the virtual machine specified in step 2.
13. Confirm that a corresponding CI exists in UCMDB.

Note: Note its name as it will be used in the next section.

Chapter 6: Data Push from UCMDB to AM

This chapter includes:

Overview

This section describes the necessary steps to configure and verify the integration between HP Universal CMDB (UCMDB) and HP Asset Manager (AM) as it comes out of the box, without customizing it to specific customer requirements. This involves taking configuration items (CIs) from UCMDB and pushing them into AM.

Configure Connection from AM to UCMDB

To configure the connection from AM to UCMDB:

1. Log on to **UCMDB**.
2. From the left-hand navigation pane, select **Data Flow Management > Integration Studio**.
3. In the Integration Point pane, click the **New Integration Point**  button. The New Integration Point dialog box opens.

   Enter the following information:

Name	Recommended Value	Description
Integration Name	AM Push Integration	The name you give to the integration point.
Adapter	AM Push Adapter	Select the Push Integration.
Is Integration Activated	Selected	Select this check box to create an active integration point.

4. Click the **Adapter** button to open **Content Help** for this adapter.

   a. Navigate to **HP Universal CMDB Discovery and Integration Content Guide > Integrations > HP Asset Manager Push Integration > How to Integrate UCMDB and Asset Manager > Set Up UCMDB**.

   b. Follow the steps provided.

5. In the **Adapter Properties** fields, fill in the relevant details.

Name	Recommended Value	Description
Hostname/IP	<user defined>	Type the hostname of the database server.
Database Type	<user defined>	Select the database type—Oracle or SQL.
DB port	<user defined>	Type the database default port for Oracle 1521 and SQL 1433.
DB Name/SID	<user defined>	Type the database name (MSSQL) or SID (Oracle) of the database.
Credentials ID	<user defined>	Click the **Add new connection details for selected protocol type** button. Enter the following information: ■ Select the database type. ■ Type the port number. ■ In **User name**, type the schema user of AM. ■ In **DB password**, type the password of the schema.
AM Version	<user defined>	Select the AM version.
Data Flow Probe	<user defined>	Select the right Probe from the drill down list.

6. Copy the following .dll files from **<Asset Manager Installation folder>\x64 to <UCMDB Installation folder>\DataFlowProbe\lib**:

   ■ aamapi93.dll

   ■ amjni93.dll

- libeay63.dll
- oldap.dll
- ssleay64.dll

7. Click **Test Connection** and **OK**.

Verify AM to UCMDB Configuration

Note: On first use, run the full population job. After any changes are made, only run the **Delta Synchronization** population job.

To verify the AM to UCMDB Configuration:

1. Log on to UCMDB.
2. From the left-hand navigation pane, select **Data Flow Management > Integration Studio**.
3. Select the **AM Push Integration** adapter.
4. In the Integration Jobs, click the **AM Push** integration.
5. Click the **Full Synchronization**  button.
6. When the Confirm synchronizing window appears, click .
7. Click the Refresh  button and wait until the **Succeeded** message appears in the **Status** tab. The updated synchronization status appears.
8. From the left-hand navigation pane, select **Modeling > IT Universe Manager**.
9. Select the **Search CIs** tab.
10. In the CI type, select **Node** and click **Enter**.
11. Confirm that all CIs from UCMDB appear in AM.

Note: If Universal Discovery is used with Discovery Agent (previous functionality enabled by the DDMi product), UCMDB will push a lot of details about CIs into Asset Manager.

Troubleshooting

This section contains the following topics:

UCMDB Fails to Create an Integration Point in Front of AM

Problem: UCMDB Test Connection in front of Asset Manager fails due to **Unable to load dynamic library (libeay64.dll)** error.

The Microsoft Visual C++ 2008 Ridistributable package (x64) is not installed and required to run the libeay64.dll.

Solution: Download and install (both in UCMDB and Asset Manager) the **Microsoft Visual C++ 2008 redistributable** package as referenced in this knowledge article: Unable to load dynamic library (libeay64.dll) (http://support.openview.hp.com/selfsolve/document/KM1328658)

UCMDB Fails to Push Updated CIs/Assets to AM and Displays an Error

When UCMDB fails to push updated CIs/Assets to AM and displays an error that contains this reference:

```
Caused by: com.peregrine.ac.AmException: Error (12,001): ODBC error: [Micros
oft][ODBC SQL Server Driver][SQL Server]Snapshot isolation transaction aborted
due to update conflict. You cannot use snapshot isolation to access table
'dbo.amCounter' directly or indirectly in database 'AM932_BTO81' to update,
delete, or insert the row that has been modified or deleted by another trans
action. Retry the transaction or change the isolation level for the
update/delete statement. SQLSTate: 37000 ('Line 1 of script ''Default value' of
field 'Reference (Ref)' in table 'Workflow instances (amWfInstance)''')

SQL statement 'execute up_GetCounterVal N'amWfInstance_Ref', 1' could not be
executed ('Line 1 of script ''Default value' of field 'Reference (Ref)' in table
'Workflow instances (amWfInstance)''')

Counter 'amWfInstance_Ref' unknown ('Line 1 of script ''Default value' of field
'Reference (Ref)' in table 'Workflow instances (amWfInstance)''')

Agent 'CWorkEvtAgent' returned error : '12001'

An integrity was not correctly applied (no additional information available).
```

The cause of this error is a wrong counter setting in Asset Manager.

To resolve this error:

1. Start the Asset Manager Windows client.
2. Select **File > Import**.
3. Click the **Execute a script** button.
4. Select and import the **<AM installation folder>/datakit/standard/counters.scr** file.
5. After the import is finished, retry **UCMDB > AM push**.

Chapter 7: AM and SM Integration (via CIT)

This chapter includes:

Overview

This chapter describes the necessary steps to configure and verify the integration between HP Asset Manager (AM) and HP Service Manager (SM) via HP Connect-It (CIT). This integration sets up the synchronization of reference data between SM and AM. This data includes information about People, Places, Things (not configuration items), commonly referred to as PPT in the description described in this chapter. Depending on the current customer implementation phase, the master data source can be either Service Manager or Asset Manager— or each product will contain master data for specific record types.

By default, the provided CIT scenarios transfer the same PPT types from AM to SM and from SM to AM. You cannot implement the scenarios as they are, because data replication would circle back and forth. Thus you must decide whether the AM or SM database will store the reference data for each of the PPT types:

- Companies
- Vendors
- Locations
- Departments
- Contacts
- Models
- Stock rooms

Integrating AM with SM via CIT

To integrate AM with SM via CIT:

1. Install **CIT version 9.50**.
2. Download the HP Service Asset and Configuration Management (SACM) Solution version 9.30 content pack from HP Live Network (HPLN) (https://hpln.hp.com/node/13253/attachment-) and unzip it to **C:\SACM-9.30**.
3. Browse to **C:\SACM-9.30**.
4. Select one of the following scenarios:

   If the reference database for all PPT types is AM:

   - Use **amsm-ppt.scn** to transfer the PPTs from AM to SM.
   - Do not use **amsm-ci-ppt-link.scn** because links between configuration items (CIs) and Contact, Model, Vendor, Location and Department are managed by the **amsm-ppt.scn** scenario.

   If the reference database for all PPT types is SM:

   - Use **smam-ppt.scn** to transfer the PPTs from AM to SM.
   - Use **smam-wo.scn** to transfer changes and tasks.

   If the reference database for PPT types is a mixed solution between AM or SM according to PPT type:

   - Customize **smam-ppt.scn** so that PPTs referenced in SM are transferred to AM.
   - Customize **amsm-ppt.scn** so that PPTs referenced in AM are transferred to SM.
   - Do not use **amsm-ci-ppt-link.scn** because links between CIs and Contact, Model, Vendor, Location and Department are managed by the **amsm-ppt.scn** scenario.
   - Use **smam-wo.scn** to transfer changes and tasks.
5. For each scenario, define the AM details and SM details.
6. After all the details are defined in the components, click  .

Add the SACM Integration Web Service

The CIT scenarios depend on the SACM Integration Web Service. You need to add this Web service to SM.

To add the SACM Integration Web Service:

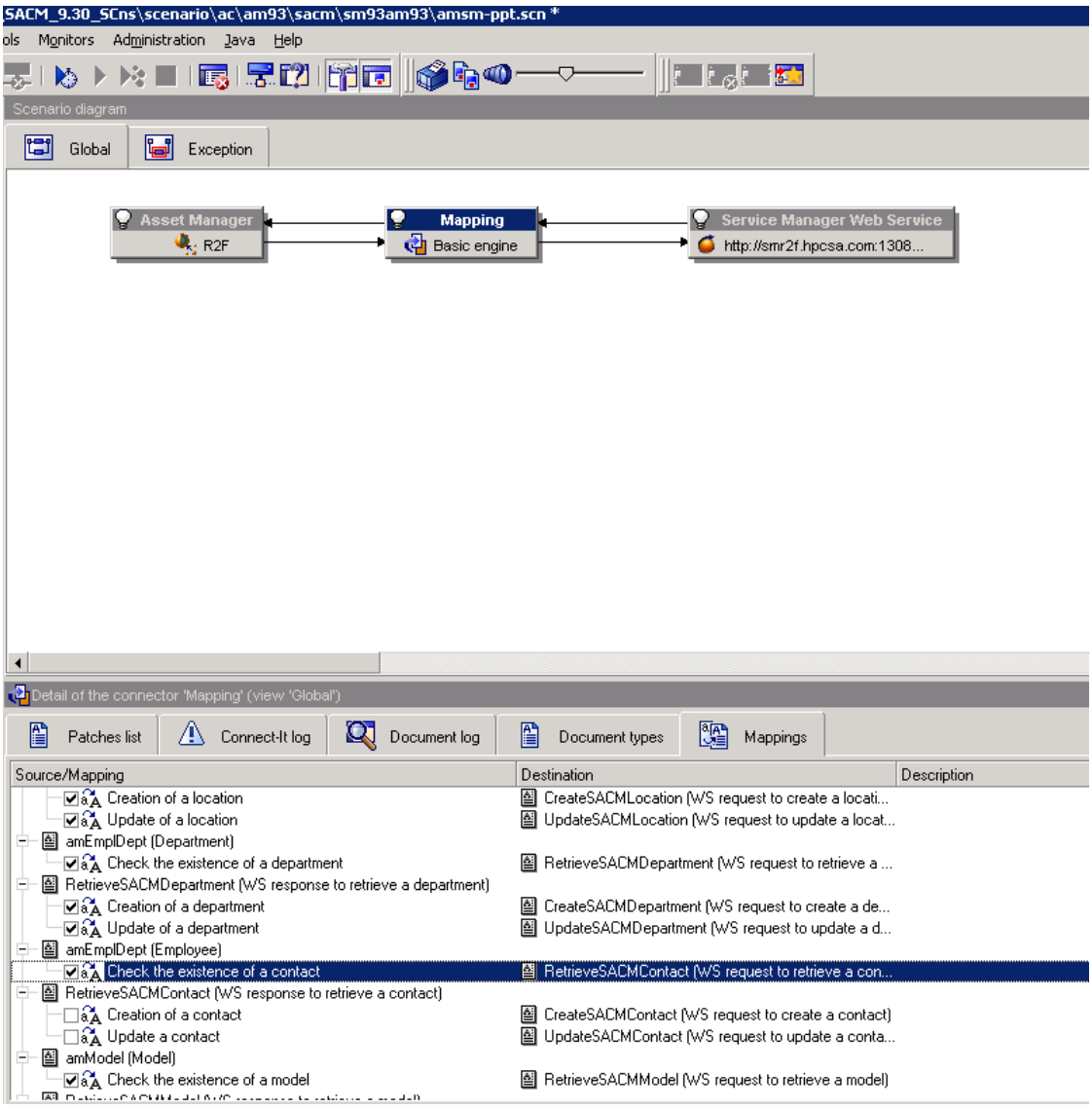
1. Start the HP Service Manager client.
2. Select **Menu Navigation > Tailoring-Database Manager** in the navigation pane.
3. Right-click the screen in the right pane and select **Import/Load**.
4. In the **File Name** field, enter **<HP Connect-It installation folder>\datakit\sc\sm93\SACMintegration.unl**.
5. Click **Load FG**.
6. In the navigation pane, select **Menu Navigation> Tailoring > Web Services-WSDL Configuration**.
7. In the **Service Name** field, enter **SACM Integration**.
8. Click **Search**.

Disable Contacts Synchronization

In an environment where an Employee Self Service (ESS) Catalog integration is planned (as described in "AM Web Configuration" on page 72), it is necessary to disable Contact synchronization in order to prevent possible data duplication.

To disable the synchronization of Contact records:

1. Open the amsm-ppt.scn Connect-It scenario.
2. In the Scenario diagram pane, select the **Mapping** box, and then select the **Mappings** tab as shown in the following diagram:



3. In the Detail of the connector 'Mapping' pane, uncheck **Creation of a contact** and **Update a contact**
4. Save the changes and exit the scenario.

Verify AM to SM Configuration

To verify the AM to SM configuration:

1. Log on to SM and open a new change request.
2. Browse to **Changes > Open New Change**.
3. Enter all relevant data and mandatory fields.
4. Click **Save**.
5. Log on to CIT.
6. Use the **scenario smam-wo.scn**.
7. Fill the relevant parameters for each product.
8. Click **Produce Now**  .
9. Log on to AM.
10. Browse to **Asset Lifecycle > Work Orders > Work Orders**.
11. Confirm that AM received the change request.

Note: This out-of-the-box integration synchronizes all **Change** and **Change Tasks** records from Service Manager to Asset Manager. In the production environment, the user may want to limit the scope for specific **Change** categories. To achieve this, there is a need to modify the **smam-wo.scn** scenario.

Chapter 8: AM Web Configuration

This chapter includes:

Overview

This section describes the necessary steps to configure and verify the HP Asset Manager (AM) Web Configuration. It is described here since it is a prerequisite for the HP Service Manager (SM) – AM integration described in "AM and SM Integration (via CIT)" on page 67.

Prerequisites

1. Install **JDK 6** and configure the environment variable of the **JAVA_HOME** to **JDK** folder—for example, **C:\Program Files\Java\jdk1.6.0_24**.
2. Install **Apache Tomcat 6.0.36**.
3. In order for some required libraries to be found by AM Web, make sure **<Asset Manager Installation folder>\bin** and **<Asset Manager Installation folder>\bin\x64** is in an environment variable of Path.

Implementing AM Automated Process Manager in Windows

To implement AM Automated Process Manager in Windows:

1. Browse to **Start > Run**.
2. Type **services.msc**.
3. Select AM Automated Process Manager 9.3 and change the start-up type to **automatic**.
4. Click **Start** and **OK**.
5. Browse to **Start > Programs > HP > Asset Manager 9.32 en > Automated Process Manager**.
6. Click **File connect to new database**.
7. Select the relevant database and type the credentials.

Tomcat Configurations

Note: These configurations must to be done just for Tomcat 6.

1. Browse to **<Apache Installation Folder>\Tomcat 6.0\bin**.

   For example, **C:\Program Files\Apache Software Foundation\Tomcat 6.0\bin)**
2. Right click **tomcat6w.exe** and select **Open**. The Apache Tomcat 6 Properties window opens.
3. Select the **Java** tab.
4. In the Java options window, insert the line **-Dsun.lang.ClassLoader.allowArraySyntax=true**.
5. Click **OK**.

AM Web Service package.properties Parameters

Note: Before editing the property file, make sure to:

- Make a backup copy of the file.
- If your application server is started, stop it.

To set the AM Web Service package.properties parameters:

1. Browse to **<Asset Manager Installation folder>\websvc**.
2. Edit the parameters in the **package.properties** file.

Parameter	Description	Value
DB.engine	Database engine that is used by this installation of AM.	For example, **ORACLE**
DB.datasource	Name of the database server.	For example, **labm3amdb35**
DB.login	Database engine log on of AM schema.	
DB.password	Password of AM schema.	
DB.library.path	Path to the aamapi93 library.	For example, **C:\Program Files\HP\Asset Manager9.30xx\bin\aamapi93.dl**
AssetManager.UserLogin	AM user log on to be used by the WebService.	For example, **Admin**
AssetManager.UserPwd	AM Password log on to be used by the WebService.	
encrypt	When this parameter is set to **true**, the user needs to enter a password in unencrypted format.	

Update Archive File Using Deployment Script

To update the archive file using a deployment script:

1. Click **Start > Run**.
2. Type **cmd**.
3. Browse to **<Asset Manager Installation folder>\deploy**—for example, **C:\Program Files\HP\Asset Manager 9.32 en\deploy**.
4. Type the command **deploy.bat ..\websvc\package.properties**.
5. Type the command **deploy.bat ..\webtier\ package.properties**.

Install AM Web Service

To install AM Web Service:

1. Copy **<Asset Manager Installation folder>\websvc\AssetManagerWebService.war** to **<Apache Installation Folder>\Tomcat 6.0\webapps**.
2. Browse to **<Apache Installation Folder>\Tomcat 6.0\bin**.
3. Right click **tomcat6w.exe** and select **Open**. The Apache Tomcat 6 Properties window appears.
4. Select the **Java** tab.
5. Insert the line **-Djava.library.path= <Asset Manager Installation folder>\bin**—for example, **C:\Program Files\HP\Asset Manager 9.32 en\bin**.
6. Start **Apache Tomcat 6**.

Test for AM Web Service Successful Deployment

To test for AM Web Service's successful deployment:

1. Open **Internet Explorer**.
2. Browse to **http://<Name of the Asset Manager Web Service server>:8080/AssetManagerWebService**.

3. Verify the following page appears:

If an error message appears—for example, **Unable to connect the database to retrieve the version…**—do the following:

a. Browse to **<Apache Installation Folder>\Tomcat 6.0\webapps\AssetManagerWebService\WEB-INF**.

b. Search for **AssetManager.DB.Name** and check that only the name of the AM schema is shown there.

```
<env-entry>
    <description>AssetManager Database name</description>
    <env-entry-name>AssetManager.DB.Name</env-entry-name>
    <env-entry-type>java.lang.String</env-entry-type>
    <env-entry-value>TEST</env-entry-value>
</env-entry>
```

Chapter 9: SM and AM Integration

This chapter includes:

Overview

This chapter describes the necessary steps to configure and verify the integration between HP Service Manager (SM) and HP Asset Manager (AM) following a request from the catalog. This integration enables the Employee Self Service (ESS) user of SM to create a request which will be transferred to AM and will be processed there until completion.

A typical request handled by this integration includes the procurement of new IT assets—such as the purchase of a new laptop computer for an employee or a new server for a data center.

Integrating SM with AM Pursuant to Request from Catalog

To integrate SM with AM pursuant to a request from the catalog:

1. Run an SM client.
2. Connect to the SM database.
3. In the browser, select **Menus > Service Catalog > Approval Activities**.
4. Select the first line in the **General Approval** table.
5. Click the **Remove Approval Activity** link.
6. Click **Finish**.
7. Select **Menu Navigation > Tailoring > Database Dictionary** in the navigation pane.
8. Enter **svcDisplay** in the **File Name** field.
9. Select the descriptor entry in the table (first line in the table).

10. Click the **New Field/Key** button.
11. Populate the **Name** field with the optionList value, the **Type** field with the character value, and click **OK**.
12. Edit the optionList entry in the table to populate the **SQL Name** field with **OPTIONLIST**, SQL Type with **IMAGE**, and SQL Table with **m1**.
13. Click **OK**.
14. Click **SM Alters**.
15. Select the descriptor entry in the table (first line in the table) again.
16. Click the **New Field/Key** button.
17. Populate the **Name** field with the **optionOptions** value, the **Type** field with the character value, and click **OK**.
18. Edit the optionOptions entry in the table to populate the **SQL Name** field with **OPTIONOPTIONS**, SQL Type with **IMAGE**, and SQL Table with **m1**.
19. Click **OK**.
20. Click **SM Alters**.
21. Select **Menu Navigation > Tailoring > Database Manager** in the navigation pane.
22. Right click the **Database Manager** screen and select **Import/Load** in the contextual menu.
23. In the **File Name** field, select the **<Asset Manager Installation folder>\esscat\sc\sm71\SCR42940.unl** file.
24. Click the **Load FG** button.
25. Right click the **Database Manager** screen and select **Import/Load** in the contextual menu.
26. In the **File Name** field, select the **<Asset Manager Installation folder>\esscat\sc\sm71\QC8955.unl** file.
27. Click the **Load FG** button.
28. Select **Tailoring > Web Services > WSDL Configuration** from the navigation bar.
29. In the **Service Name** field, enter **ServiceCatalog**.
30. Click **Search**.
31. Select the **ServiceCatalog** entry in the list of results.

32. In the details of the **ServiceCatalogWeb** service, select the **Fields** tab.
33. At the end of the list of fields, add a new entry with the following information:
    - Field: **detailedDescription**
    - Caption: **DetailedDes**
    - Type: **StringType**
34. Click **Save** and **OK**.
35. In the **Service Name** field, enter **ServiceDesk**.
36. Click **Search**.
37. Select the **ServiceDesk** entry in the list of results.
38. In the details of the **ServiceDeskWeb** service, select the **Fields** tab.
39. At the end of the list of fields, modify the resolution field with the following information:
    - Caption: **Resolution**
    - Type: **StringType**
40. In the same list, modify the **resolution.code** field with the following information:
    - Caption: **ResolutionCode**
41. Connect to CIT.
42. Click **File > open**.
43. Browse to **<HP Connect-It installation folder>\scenario\ac\ac93\esscat**.
44. Run the following scenarios:
    - users.scn
    - sso.scn
    - categories.scn
    - catalogitems.scn
    - status.scn

45. In the Scenario diagram window, modify the configuration of the SM Web Service connectors:
    a. Right-click the **SM Web Service connector(s)** and select **Configure connector ...**. The Configure the connector wizard opens.
    b. Click **Next**.
    c. Populate the **Define the connection parameters** page.
    d. Click **Finish**.
46. Return to the Scenario diagram window and modify the configuration of the AM connector:
    a. Right-click the **AM connector** and select **Configure connector ...**.
    b. Click **Next**.
    c. Populate the Define the connection parameters page.
    d. Click **Finish**.
47. Use the **File/Save** menu to save your changes.
48. Install **apache-tomcat-6.0.36**.
49. Change the name of the folder to TomcatESS.
50. Browse to **C:\TomcatESS\conf\server.xml**.
51. Change the port to a different port of AssetManagerWebService—for example, **7080**.

```
<Connector port="7080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
```

52. Deploy **ServiceCatalog.war** to **C:\TomcatESS\webapps**.
53. Log on to **SM**.
54. Browse to **Service Catalog > Catalog** Connectors menu.
55. Select the connector named **Open a Standard Request** in AM.
56. On the **Expressions** tab, enter the hostname and port for the Esscat Web service.
57. Start the Tomcat configuration console **(Start > Programs > Apache Tomcat 6.0 > Configure Tomcat)**.

58. Select the **Java** tab.
59. Add the following line to the Java Options section:

    -XX:MaxPermSize=256m
60. Quit the Tomcat configuration console.
61. Browse to **Tailoring > Web Services > Run WSDL to JS** in the system navigator panel.
62. Enter the URL for the WSDL of the AM Web Service proxy. The format is:

    http://AMProxyServer:8080/Service Catalog/wsdl/ServiceCatalog.wsdl
63. Click **Proceed**. A window with the new Java script corresponding to the Web Service Proxy is displayed.
64. Click **Replace**. The following message appears:

    Successful compilation of JavaScript function or expression.
65. Enter **status** in a SM command prompt.
66. Check that linker appears in the list.
67. If the linker scheduler already appears in the list, restart it:
    a. In the Command column of the linker line, enter **K**.
    b. Click the **Execute Commands** button.
    c. Repeat this action until the linker line disappears.
    d. Click the **Start Scheduler** button.
    e. Double-click linker-startup in the list.

Verify SM to AM Configuration

To verify the SM to AM configuration:

1. Connect to SM with the following link: **http://hostname of SM:8080/webtier-9.32/ess.do**
2. Log on to SM with the user that you created in AM.
3. Click **order from catalog** from the left pane.
4. Choose the product that appears in the SM catalog.

5. Click **Add to cart**.
6. Click the **Checkout** link.
7. Click **submit request**.
8. Complete the purpose tab and select the Urgency.
9. Click **Submit** and **OK**
10. Log on to AM.
11. Browse to **Asset Lifecycle > Procurement Lifecycle > Requests > purchase requests**.
12. Find the request in the list. It should begin with **ESS-SD XXX**.

Troubleshooting

This section contains the following topics:

ESS Catalog Tomcat Console Displays Errors About “PermGen space”

If the ESS catalog to the Asset Manager purchase request integration does not work, and ESS Catalog Tomcat console displays errors about PermGen space, update the JVM memory settings—such as adding this line to Tomcat/bin/catalina.bat:

```
set JAVA_OPTS=%JAVA_OPTS% %LOGGING_CONFIG% -server -Xms512m -Xmx512m -
XX:PermSize=512M -XX:MaxPermSize=512M.
```

Chapter 10: CI's Reconciliation Priority

This chapter includes:

Overview

From the ITPS Suite perspective, HP Universal CMDB (UCMDB) is the center configuration item (CI) repository. As such, it is populated with CI information from various HP and third-party products. Therefore, UCMDB must decide which source is more reliable and which source has the most accurate information.

UCMDB uses internal out-of-the-box reconciliation rules that make sure no duplications are created and the CI information is accurate. In addition, it also uses the Reconciliation Priority module that gives the Configuration Manager the power to determine for UCMDB which integration points are more reliable for which CI Types or Attributes. For more information, see Chapter 16, Reconciliation Priority in the *HP Universal CMDB version 10.01 Data Flow Management Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00245427?lang=en&cc=us&hpappid=OSP).

In the Request to Fulfill Value Stream, UCMDB is populated with CI information from two products—AM and SM.

For Best Practice guidelines and configuration instructions for how to prioritize the information received from HP Asset Manager (AM) and HP Service Manager (SM) into UCMDB in order for your UCMDB to contain the most accurate CI information, see the *HP Service Asset and Configuration Management (SACM) Solution version 9.30 Configuration Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00749032).

Chapter 11: Execute HP OO Flows from SM

This chapter includes:

Overview

HP Operations Orchestration (HP OO) software automates simple tasks such as auto archiving, and complex tasks such as disaster recovery planning. It provides the means to automate processes that include managing and provisioning a virtual infrastructure. The HP OO flows communicate and document procedures, decreasing dependencies on individuals or groups. Refer to HP OO documentation for more information.

When integrated with HP Service Manager (SM), HP OO shares information between monitoring and automation systems and the Help desk. Incident Management processes are enhanced by linking Knowledge documents with HP OO flows, allowing technicians to triage, diagnose, and resolve incidents more quickly and efficiently. Web client users have access to HP OO flows from Knowledge Management (KM). They can view, add, update, or delete HP OO flows; link HP OO flows to Knowledge documents; execute flows from related Knowledge documents for an incident; and view HP OO flow execution results attached to an incident as historic activities.

Enable HP OO Flows from SM – KM Module

This task lists the steps necessary to enable HP OO flows from the SM – KM module.

Prerequisites

1. Before the integration can be configured, install and enable the KM Engine that comes on separate installation media.
2. After it is installed on your local/remote server, and its service is running, start it using the command: **Search Engine installation folder>\startup.cmd**—for example, **C:\Program Files (x86)\HP\Service Manager 9.30\Search_Engine\startup.cmd**
3. In SM, navigate to **Knowledge Management > Configuration > Configure Search Servers**.
4. In the **Server Name** field, enter a valid name for the search server and click the **Add** button.
5. Enter the following details:

Name	Recommended Value	Description
hostname	<user defined>	Host name of search server.
port	<user defined>	C:\Program Files\HP\Service Manager 9.30\Search_ Engine\tomcat\conf\server.xml: **Connector port="8083" protocol="HTTP/1.1" ConnectionTimeout="20000" redirectPort="8443")** C:\Program Files\HP\Service Manager 9.30\Search_ Engine\tomcat\conf\server.xml: **Connector port="8083"protocol="HTTP/1.1" ConnectionTimeout="20000"redirectPort="8443")**
Service type	<user defined>	Select **master**.

6. Click **Verify Server**. Success message appears.
7. Verify the knowledge base is online as follows:
   a. In **SM**, **Knowledge Management > Configuration > Knowledgebases**, click **Search**.
   b. In **KM**, confirm the status is **online**. If not, click **Full Reindex**.

Configure SSL on HP OO

To configure SSL on HP OO:

1. Install **OpenSSL** on the **Operations Orchestration** server.
2. Append the **OpenSSL** bin folder to PATH system environment variable.
3. Locate the **openssl.cnf** file in your **OpenSSL** installation, and create a system environment variable called **OPENSSL_CONF**.
4. Verify that a folder with java tool **keytool.exe** is included in **PATH env.variable**.

   Note: The **keytool.exe** java tool is usually found in a **jdk/jre** bin folder such as **C:\Program Files\Java\jre7\bin**.

5. Before you start configuring SSL in HP OO, make a backup copy of the following folder:
   - **<OO_HOME>\Central\var\security**
6. Generate a private/public key pair for Root Certificate Authority.
   a. Change to the following directory: **<OO_HOME>\Central\var\security**
   b. Run the following command:

   ```
   openssl genrsa -des3 -out cakey.pem 2048
   ```

   c. When prompted, enter the phrase for cakey.pem: **changeit**:

   ```
   openssl req -new -key cakey.pem -x509 -days 1095 -out mycacert.pem
   ```

   Examples of data to enter during the command execution that 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) []	FQDN of HP OO server
Email Address []	name@devlab.ad

7. Use the Java key tool to generate a request.

   a. Run the following command (use values from previous request to populate corresponding fields):

   ```
   keytool -genkey -alias sm -keyalg RSA -keystore key.store -storepass
   changeit -keypass changeit -dname "CN=<FQDN of OO server>, OU=SSG, O='HP
   Software', L=Yehud, ST=Israel,C=IL"
   ```

   b. Run the following command:

   ```
   keytool -certreq -keystore key.store -alias sm -storepass changeit -file
   req.crs   (when prompted enter password: changeit)
   ```

   c. Run the following command:

   ```
   openssl x509 -req -days 1095 -in req.crs -CA mycacert.pem -CAkey cakey
   .pem -CAcreateserial -out smcert.pem   (when prompted enter password:
   changeit)
   ```

8. Import the root CA and self-signed certificate to **key.store**.

   a. Run the following command:

   ```
   keytool -import -v -alias rootca -keystore key.store -storepass changeit
   -file mycacert.pem
   ```

   Note: The command window prompts the certificate information—such as Owner, Issuer, Serial number, Valid period, Certificate fingerprints, and Extensions.

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

   The following confirmation message appears:

   Certificate was added to keystore.

   [Storing key.store]

c. Run the following command:

```
keytool -import -v -alias sm -keystore key.store -storepass changeit  -
file smcert.pem
```

The following confirmation message appears:

Certificate reply was installed in keystore.

[Storing key.store]

9. Restart the **HP OO Central** service.

Configure SSL on SM

To configure SSL on SM:

1. Create a trust store for SM.

   a. Change to the following directory: **<SM_HOME>\Server\RUN**.

   b. Copy the generated **mycacert.pem** and **smcert.pem** from **<OO_ HOME>\Central\var\security to <SM_HOME>\Server\RUN**.

   c. Run the following command:

```
keytool -import -v -alias rootca -keystore smtrust -storepass changeit -
file mycacert.pem
```

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

   The following confirmation message appears:

   Certificate was added to keystore.

   e. Run the following command:

```
keytool -import -v -alias sm -keystore smtrust -storepass changeit -
file smcert.pem
```

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

The following confirmation message appears:

Certificate was added to keystore.

g. Verify that smtrust was created in **<SM_HOME>\Server\RUN**.

h. Add the following lines to **sm.ini**:

```
# Certificates
truststoreFile:smtrust
truststorePass:changeit
```

2. Restart the SM server.

Add an SMOO Integration Instance

To add an SMOO integration instance:

1. Navigate to **Tailoring > Integration Manager**. The Integration Instance Manager window opens.
2. Click the **Add** button.
3. Select **SMOO** from the Integration Template drop-down list.

Note: Do not select the **Import Mapping** check box.

4. Click **Next**. The Integration Instance Information pane appears.
5. Enter the following information:

Interval time	180 seconds
Log file folder	C:\Program Files\HP\Service Manager 9.30\Server\logs
Desired log level	WARNING
Max Retry Times	3

6. Click **Next**.
7. In the **General** tab and **Secure Parameters** tab, modify the values. Add your HP OO server host name and port, user name and password, and a base path such as **/Library/ITIL/Change Management;/Library/ITIL/Incident Management**.

8. Click **Next** two times.
9. Click **Finish**.

Enable an Integration Instance

To enable an integration instance:

1. From the System Navigator, navigate to **Menu Navigation > Integration Manager**. The Integration Instance Manager window opens.
2. Select a disabled integration instance from the table and click **Enable**.
3. In the prompt window, click **Yes**. The integration instance is enabled. It is seen as **Running** and then enters **Sleeping** mode.

Note: Only users with SysAdmin or programmer capability have access to the Manage OO Flows menu to view, create, update, and delete HP OO flows in SM.

Configure LWSSO in HP OO

To configure and enable Lightweight Single Sign-On (LWSSO) on HP OO:

1. Log on to **HP OO Central**.
2. Click the **System Configuration** button.
3. Select **Security > SSO**.
4. Select the **Enable** check box.
5. Enter the **InitString**.
6. Enter the **Domain**. This is the domain name of the network of the servers on which HP Cloud Service Automation (HP CSA) and HP OO are installed.
7. Click **Save**.

Chapter 12: Security Settings Configuration

This chapter includes:

Overview

Lightweight Single Sign-on (LWSSO) is modular framework that can bridge authenticated information in heterogeneous environments between applications.

LWSSO was implemented in HP Software Products to fulfill the need for SSO support between products in the same HP Software Products Center, as well as those in different HP Software Products Centers, plus support for third-party solutions.

Using LWSSO in a solution simplifies the user's work flow by avoiding the need to enter authentication details each time the flow passes between the value stream products.

Configure the SM Web Tier for LWSSO Support

To configure the HP Service Manager (SM) Web tier for LWSSO support, you must first configure the SM Web client for trusted sign-on and SSL support with the SM server. This involves generating and deploying certificates and modifying the **sm.ini** file on the SM server and **web.xml** on the Web client.

To configure the SM Web tier for LWSSO support:

1. In the Web tier's **web.xml** file:

   a. Uncomment the following filter elements to enable LWSSO as shown below—for example, **C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\webtier-9.31\WEB-INF\web.xml)**.

   ```
   <!-- LWSSO filter for integrations using HP lightweight single sign-on
   PLEASE NOTE: Uncomment this filter and the associated filte r-mapping,
               and see application-context.xml for additional configuration
   needed for LWSSO. -
   -> <filter>
             <filter-name>LWSSO</filter-name> <filter-
              class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter
   /filter-class>
   </filter>
   ...
   <!-- LWSSO filter-mapping, please read description for LWSSO
   filter ab ove before uncommenting this. -->
            <filter-mapping> <filter-
            name>LWSSO</filter-name> <url-
            pattern>/*</url-pattern>
            </filter-mapping>
   ```

   b. Set the following parameter to **false**.

   ```
   <init-param> <param-
             name>querySecurity</param-name>
             <param-value>false</param-value>
   </init-par
   ```

2. Locate the **isCustomAuthenticationUsed context-param** element in the Web tier web.xml. Make sure the param-value element is set to **false**. It should look like the following:

```
<context-param> <param-
         name>isCustomAuthenticationUsed</param-name>
         <param-value>false</param-value>
</context-parm>
```

3. Modify the **application-context.xml** file located in the WEB-INF\classes folder of the SM Web tier deployment.

   a. Locate the **filterChainProxy** bean element. Add the lwSsoFilter to the value element.

```
<bean id="filterChainProxy"
class="org.acegisecurity.util.FilterChainProxy">
         <property name="filterInvocationDefinitionSource">
         <value> CONVERT_URL_TO_LOWERCASE_BEFORE_COMPARISON

       PATTERN_TYPE_APACHE_ANT
...
/**=httpSessionContextIntegrationFilter,lwSsoFilter,
anonymousProcessingFilter
         </value>
         </property>
</bean>
```

   b. Uncomment the **lwSsoFilter** bean, as shown below.

```
<!-- 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.LwSsoPr
eAuthenticationFilter">
 <property name="authenticationManager">
 <ref bean="authenticationManager"/> </property>
 <property name="defaultRole">
 <value>ROLE_PRE</value>
 </property>
</bean>
```

Note: The following two lines must be added to the file:

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

4. In the **lwssofmconf.xml** file located in the WEB-INF\classes folder of the SM Web client deployment, set the following parameters.
   - Set the value of enableLWSSOFramework to true (default is false).
   - **<*domain*>.** Domain name of the server where you deploy your Web tier. For example, if your Web tier's fully qualified domain name is mywebtier.example.com, then the domain portion is example.com.
   - **<*initString*>.** Password used to connect HP products (minimum length: 12 characters)—for example, smintegrationlwsso. Make sure that this value is the same as that used in the LWSSO configurations of the other HP applications (such as HP OO and BSM) that you want to connect via LWSSO.
   - **<*multiDomain*>.** The <multiDomain> element should include the domain names (DNSDomain), server names (NetBiosName), IP addresses (IP), fully-qualified domain names (FQDN) of the SM Web tier server and other product servers.

     Note: The multi-domain functionality is relevant only for user interface LWSSO (not for Web services LWSSO). In addition, you must set the multiDomain element in each product for which you want to support LWSSO.

5. Check the **secureHTTPCookie** value (default: true). If you set secureHTTPCookie to true (default), you must also set secureLogin in the **web.xml** file to true (default). If you set secureHTTPCookie to false,you can set secureLogin to true or false.

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config
xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/2.0">
 <enableLWSSO
  enableLWSSOFramework="true"
  enableCookieCreation="true
 cookieCreationType="LWSSO"/>
```

```
 <webui>


  <validation>

   <in-ui-lwsso>

    <lwssoValidation id="ID000001">

     <domain>example.com</domain>

      <crypto cipherType="symmetricBlockCipher" engineName="AES" padding
ModeName="CBC" keySize="256"

       encodingMode="Base64Url" initString="This is a shared secret pass
phrase"/>

    </lwssoValidation>

   </in-ui-lwsso>


    <validationPoint

     enabled="false"

     refid="ID000001"


authenicationPointServer="http://server1.example.com:8080/bsf"/>


    </validation>


    <creation>

     <lwssoCreationRef useHTTPOnly="true" secureHTTPCookie="true

      <lwssoValidationRef refid="ID000001"/>

      <expirationPeriod>50</expirationPeriod>

     </lwssoCreationRef>

    </creation>


    <logoutURLs>

      <url>.*/goodbye.jsp.*</url>
```

```
      <url>.*/cwc/logoutcleanup.jsp.*</url>
    </logoutURLs>

    <nonsecureURLs>
      <url>.*/images/.*</url>
      <url>.*/js/.*</url>
      <url>.*/css/.*</url>
      <url>.*/cwc/tree/.*</url>
      <url>.*/sso_timeout.jsp.*</url>
    </nonsecureURLs>

     <multiDomain>
      <trustedHosts>
       <DNSDomain>example.com</DNSDomain>
       <DNSDomain>example1.com</DNSDomain>
       <NetBiosName>myserver</NetBiosName>
       <NetBiosName>myserver1</NetBiosName>
       <IP>xxx.xxx.xxx.xxx</IP>
       <IP>xxx.xxx.xxx.xxx</IP>
       <FQDN>myserver.example.com</FQDN>
       <FQDN>myserver1.example1.com</FQDN>
      </trustedHosts>
     </multiDomain>
</webui>

<lwsso-plugin type="Acegi">
 <roleIntegration
   rolePrefix="ROLE_"
   fromLWSSO2Plugin="external"
   fromPlugin2LWSSO="enabled"
   caseConversion="upperCase"/>
```

```
 <groupIntegration
   groupPrefix=""
   fromLWSSO2Plugin="external"
   fromPlugin2LWSSO="enabled"
   caseConversion="upperCase"/>
 </lwsso-plugin>
</lwsso-config>
```

6. Restart your Tomcat server.
7. On the SM server side, go to:

   <SM installation folder>\RUN\lwssofmconf.xml

   (For example, go to **C:\Program Files (x86)\HP\Service Manager 9.32\Server\RUN\lwssomconf.xml)**.

   Update this file as described in step 4.
8. Restart the SM server.

Verify SM – HP OO Flow

Since there is no direct flow invocation of HP OO flows from incidents, it is possible to run flows attached to KM articles.

To verify that flows have been successfully launched from the SM Incidents module:

1. Open the **SM web client**.
2. In the **Knowledge Management** module, **Published** documents, select any article.
3. Edit the article.

   Note: Remember the article's name.
4. In the edit form, select the **OO Flow Links** tab.
5. Click the drop-down arrow and select any available flow.
6. Click the **Add Link** button.

7. Click the **Add** button again, and then click **Save** to save the record.
8. Click either the **Approve External** or **Approve Internal** buttons to approve the article.
9. Open a new incident.
10. Click the **More** button and select **Search Knowledge**.
11. Search for the title of the **Knowledge** article that you selected in Step 2.
12. Open the article and click the **Execute OO Flow** button.
13. Fill in the required parameters and click **Next > Yes** to view the HP OO execution report. The Incident record is updated in Journal Updates with the HP OO flow execution result.

Configure LWSSO in UCMDB

To configure LWSSO in UCMDB:

1. Access the JMX console by entering the following address into your Web browser:

   http://<server_name>:8080/jmx-console, where <server_name> is the name of the machine on which HP Universal CMDB is installed.
2. Under **UCMDB-UI**, click the **name=LW-SSO Configuration** to open the Operations page.
3. Set the init string using the **setInitString** method.
4. Set the domain name of the machine on which UCMDB is installed using the **setDomain** method.
5. Invoke the method **setEnabledForUI** with the parameter set to **True**.
6. To view the LW-SSO configuration as it is saved in the settings mechanism, invoke the **retrieveConfigurationFromSettings** method.
7. To view the actual loaded LWSSO configuration, invoke the **retrieveConfiguration** method.
8. Restart the UCMDB.

Chapter 13: Launch HP OO Flows from HP CSA

This chapter includes:

Overview

This task lists the steps necessary to launch HP Operations Orchestration (HP OO) flows from HP Cloud Service Automation (HP CSA).

Prerequisites

Make sure you have completed the following:

- HP Cloud Service Automation is up and running.
- HP Operations Orchestration is up and running, and contains relevant CSA Content Pack flows as described in the *HP Cloud Service Automation version 4.10 Configuration Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01061716) and in this chapter.

Configure HP CSA – HP OO Integration

This task lists the steps necessary to configure the HP CSA – HP OO integration, as well as to import HP OO flows into your HP CSA Service Design model. This enables HP CSA to launch the HP OO flows.

This section contains the following topics:

Step 1: Add a JRE to the System Path

The HP CSA flows that are imported require that a Java Runtime Environment (JRE) be included in the system path on the system running HP CSA.

For Windows:

1. Open the Environment Variables dialog box:
   a. Right-click **Computer** and select **Properties**.
   b. Select **Advanced system settings**.
   c. Click **Environment Variables**.
2. Select the **Path** system variable and click **Edit**.
3. At the end of the value for **Variable**, add a semicolon "**;**" and the following path:
   - If HP OO and HP CSA are installed on the same system:

     ```
     <OO_HOME_DIR>\java\bin
     ```

     OR

- If HP OO and HP CSA are installed on different systems:

  ```
  <csa_jre>\bin
  ```

4. Click **OK** and close all windows.

For Linux:

- Open a shell and enter the following command:
  - If HP OO and HP CSA are installed on the same system:

    ```
    export PATH=$PATH:$ICONCLUDE_HOME/java/bin
    ```

    OR
  - If HP OO and HP CSA are installed on different systems:

    ```
    export PATH=$PATH:$CSA_JRE_HOME/bin
    ```

Note: By setting the system path, all applications (that require a JRE) use the JRE that is installed with HP OO (if it is the only path or the first path set to a JRE in the system path). If you need to run another JRE with an application, you must type in the relative path to that JRE in order to run it (for example, when you configure SSL).

Step 2: Configure Internal Users

Internal users can be used to configure HP OO for HP CSA.

To configure the internal users:

1. Log on to **HP OO Central**.
2. Click the **System Configuration** button.
3. Select **Security > Internal Users**.
4. Click the **Add**  button.

5. Enter the following information and click **Save**.

Field	Recommended Value
User Name	csaoouser
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

Note: The csaoouser user is used to import the HP OO flows. When importing flows, this user is configured in the HP OO input file used by the process definition tool.

6. Select the **Enable Authentication** check box. Authentication is enabled.
7. Click **OK** in the confirmation dialog box.
8. Click the **Add**  button.
9. Enter the following information and click **Save**.

Field	Recommended Value
User Name	admin
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

Note: The admin user is used with HP Single Sign-On (LWSSO). When HP OO is launched from the Cloud Service Management Console, this user allows access to HP OO without having to log on.

10. Select the **Enable Authentication** check box. Authentication is enabled.
11. Select **OK** in the confirmation dialog box.
12. Log out of HP OO Central and log back in as the **csaoouser**.

Step 3: Set Up System Accounts for the HP CSA Content Pack

To set up the system accounts for the HP CSA content pack:

1. Log on to **HP OO Central**.
2. Click the **Content Management** button.
3. Select **Configuration Items > System Accounts**.
4. Click the **Add**  button.
5. Enter the following information if it is not already configured and click **Save**.

Field	Recommended Value
System Account Name	CSA_REST_CREDENTIALS
User Name	ooInboundUser
Password	cloud

Note: The User Name configured for the CSA_REST_CREDENTIALS System Account setting must match the Override Value (HP OO version 10.x) configured for the CSA_OO_USER System Property setting.

6. Click the **Add**  button.
7. Enter the following information if it is not already configured and click **Save**.

Field	Recommended Value
System Account Name	CSA_SERVICEMANAGER_CREDENTIALS
User Name	falcon
Password	<SM 'falcon' password>

Step 4: Set Up System Properties for the HP CSA Content Pack

To set up the system properties for the HP CSA content pack:

1. Log on to **HP OO Central**.
2. Click the **Content Management/Workspace** (depending on which HP OO version is being used) button.
3. Select **Configuration Items > System Properties**.
4. Click the **Add**  button.
5. Enter the following information if it is not already configured and click **Save**.

Field	Recommended Value
Name	CSA_REST_URI
Override Value	https://<csa_hostname>:8444/csa/rest

Step 5: Configure HP OO Properties in the csa.properties File

These properties are used to integrate with HP OO.

In the Cloud Service Management Console, for HP OO version 10.10, in the subscription event overview section of the **Operations** area, selecting the Process ID opens HP OO to the detailed page of the selected process when these properties are configured.

- Edit the `%CSA_HOME%\jboss-as-7.1.1.Final\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` file and configure the following properties:

Property	Description
OOS_URL	The URL used to access HP OO Central. This is the HP OO used for provisioning topology designs (HP OO version 10.10). Set this URL to the system on which HP OO version 10.10 is installed—for example, `https://<hostname>:8443`.
OOS_ USERNAME	The username used to log on to HP OO Central. Set this username to **admin**.

Property	Description
OOS_ PASSWORD	The encrypted password used by the user defined in `OOS_USERNAME` to log on to HP OO Central. Set this property to the encrypted value of the user defined in `OOS_USERNAME`. For more information about encrypting passwords, refer to the *HP Cloud Service Automation version 4.10 Configuration Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01061716)

Step 6: Configure SSL Between HP CSA and HP OO

For each system running HP CSA, import the root certificate of each HP OO Certificate Authority.

To import HP OO's Certificate Authority root certificate into HP CSA:

Note: First export HP OO's certificate from HP OO's truststore and then import it into HP CSA's truststore.

1. On the system running HP OO, open a command prompt and change the directory to `<OO_HOME>`.
2. Run the following command:

   For Windows.

   ```
   .\java\bin\keytool -export -alias tomcat -file C:\oo.crt -keystore
   .\Central\var\security\key.store -storepass changeit
   ```

   For Linux.

   ```
   ./java/bin/keytool -export -alias tomcat -file /tmp/oo.crt -keystore
   ./Central/var/security/key.store -storepass changeit
   ```

   Where: `C:\oo.crt` and `/tmp/oo.crt` are examples of file names and locations used to store the exported root certificate.

   Note: You can choose a different filename and location.

3. If HP OO is not running on the same system as HP CSA, copy `oo.crt` from the HP OO system to the system running HP CSA (in this example, the file is copied to `C:\`).

4. On the system running HP CSA, run the following command:

   For Windows.

   ```
   "<csa_jre>\bin\keytool" -importcert -alias tomcat -file C:\oo.crt -keystore
   <csa_jre>\lib\security\cacerts -storepass changeit
   ```

   For Linux.

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias tomcat -file /tmp/oo.crt -keystore
   $CSA_JRE_HOME/lib/security/cacerts -storepass changeit
   ```

5. When prompted to trust the certificate, enter **yes**.

6. Restart the HP CSA services.

   For Windows.

   a. On the server that hosts HP CSA, navigate to **Control Panel > Administrative Tools > Services**.

   b. Right-click on the **HP Cloud Service Automation** service and select **Restart**.

   c. Right-click on the **HP Marketplace Portal** service and select **Restart**.

   For Linux.

   a. `service csa restart`

   b. `service mpp restart`

Step 7: Import HP OO Flows to HP CSA

This section includes the following topics:

Overview

HP OO flows can be executed by HP CSA life cycle actions or used to submit delegated approvals. Before executing flows through HP CSA, they must be imported into HP CSA by running the Process Definition Tool. The Process Definition Tool creates an HP CSA process definition for every imported HP OO flow. The process definitions are associated with a process engine and that process engine corresponds to the HP OO system containing the imported flows.HP OO flows can be executed by HP CSA life cycle actions or used to submit delegated approvals. Before executing flows through HP CSA, they must be imported into HP CSA by running the process definition tool. The process definition tool creates an HP CSA process definition for every imported HP OO flow. The process definitions are associated with a process engine and that process engine corresponds to the HP OO system containing the imported flows

Create a Database Properties File

Note: HP recommends that you generate sample database properties files and input file by doing the following:

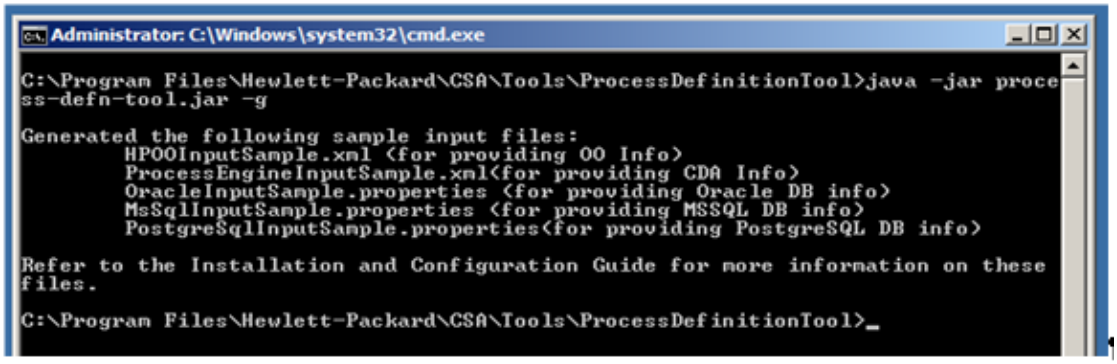
1. Navigate to the **%CSA_HOME%\Tools\ProcessDefinitionTool** directory.
2. Run the following command:

   ```
   ..\..\jre7\bin\java -jar process-defn-tool.jar -g
   ```

   In this section, **%CSA_HOME%** is the directory in which HP Cloud Service Automation is installed.

1. Select a system and working directory from which to run the Process Definition Tool. You can run the Process Definition Tool on the same system on which HP CSA is installed from the **%CSA_HOME%\Tools\ProcessDefinitionTool** directory. Or, you can run the Process Definition Tool on a different system by copying **%CSA_HOME%\Tools\ProcessDefinitionTool\process-defn-tool.jar** to a working directory on that system. The examples in this section show the tool being run on the same system on which HP CSA is installed.

Output:



2. Edit the database properties file. Use the file type according to your system's database—MSSQL, ORACLE, or Postgres. The following is an example for ORACLE database content:

Property Name	Description
db.type	The database used by HP Cloud Service Automation. **Example.** **db.type=oracle**
db.url	The JDBC URL. **Example.** **db.url=jdbc:oracle:thin:@127.0.0.1:1521:XE**
db.user	The user name of the database user you configured for HP CSA after installing the database.
db.password	The encrypted password for the database user. For more information, see "Encrypting a Password Using the Process Definition Tool" on page 112 later in this chapter for instructions on encrypting passwords. An encrypted password is preceded by **ENC** without any separating spaces and is enclosed in parentheses. While you may enter a password in clear text, after you run the Process Definition Tool, the clear text password is automatically replaced by an encrypted password. **Example.** **db.password=ENC(fc5e38d38a5703285441e7fe7010b0)**

Outcome:

```
db.type=oracle
db.url=jdbc:oracle:thin:@127.0.0.1:1521:XE
db.user=csa
db.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

Create a HP OO Input File (Defines the Flows to be Imported)

In the working directory, if you generated the sample HP OO input file, make a copy of the `HPOOInputSample.xml` file, rename it to `HPOOInfoInput.xml`, and update the attributes and values, described below, as needed. The `HPOOInfoInput.xml` file is formatted as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

</ooengines>

<ooengine name="<CSA_process_engine>" uri="https://<OO_
server>:8443/PAS/services/WSCentralService" username="<OO_user>"

password="<encrypted_password>" truststore="<location_of_truststore>"
truststorePassword="<truststore_encrypted_password>"

[accessPointType="URL" | "EXTERNAL_APPROVAL"] [update="true" | "false"]
[delete="true" | "false"] >

<folder path="<path_name>" [flow="true" | "false"] [recursive="true" | "false"]
[regex="<regular_expression>"] [update="true" | "false"] />

</ooengine>

</ooengines>
```

See the following example of `HPOOInfoInput.xml` content, which Imports the flows named **stop_request and start_job**:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<ooengines>

<ooengine name="oo-instance-1"
uri="https://127.0.0.1:8443/PAS/services/WSCentralService" username="admin"
password="ENC(a3pGFPJQFwwXwtBBdpYktg==)" truststore="C:/Program Files/Hewlett-
Packard/CSA/jre/lib/security/cacerts" truststorePassword="ENC
(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)">

<folder path="/Library/ITIL/Change Management/stop_request" flow="true" />

<folder path="/Library/ITIL/Change Management/start_job" flow="true" />

</ooengine>

</ooengines>
```

For the full description of `HPOOInfoInput.xml` file attributes, see the *HP Cloud Service Automation version 4.10 Installation Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01061713).

Run the Process Definition Tool

To run the Process Definition Tool, in the working directory, run the following command—for example:

```
"%CSA_HOME%\jre7\bin\java" -jar process-defn_tool.jar -d
OracleInputSample.properties -i HPOOInfoInput.xml
```

After the process definition tool is run, the total number of imported flows is displayed (depending on the number of flows imported, this may take some time to complete). If more than one HP OO system is specified in the HPOOInfoInput.xml file, flows are imported sequentially by system (that is, the flows from the first HP OO system listed are imported; once these flows have been imported/updated in HP CSA, the flows from the next HP OO system are imported).

Review the log file, `process-defn-tool.log`, for any error messages.

Note: The following options are available in the Process Definition Tool:

Option	Description
-d <filename>	Required. The name and location of the database properties file. **Example** `-d OracleInputSample.properties`
-i <filename>	Required. The name and location of the HP OO input file. **Example** `-i HPOOInfoInput.xml`
-e <password>	Optional. Encrypt a password. Use to encrypt a password that is entered as an attribute value in the `HPOOInfoInput.xml` file. You can also use the `passwordUtil.jar` utility to encrypt passwords.

-g	Optional. Generate example files:
	`MsSqlInputSample.properties,`
	`OracleInputSample.properties,`
	`PostgreSqlInputSample.properties,`
	`ProcessEngineInputSample.xml, and`
	`HPOOInputSample.xml.`
	The sample `HPOOInputSample.xml` file can be used to import all the flows whose associated process definitions are referenced in the out-of-the-box resource offerings and service designs provided with HP CSA.

-h	Optional. List the options available in this tool.
-v <filename>	Optional. Validate the HP OO input file. **Example** `-v HPOOInfoInput.xml`

Encrypting a Password Using the Process Definition Tool

Encrypt a password by using the encryption option in the Process Definition Tool. In the working directory, run the following command:

```
"%CSA_HOME%\jre\bin\java" -jar process-defn-tool.jar -e <password>
```

Chapter 14: Cloud Billing Management (HP CSA – AM Integration)

HP Cloud Service Automation (HP CSA) is the HP's solution for automating the request management and the deployments of internal cloud services.

HP Asset Manager (AM) is HP's solution for asset life cycle management, which includes capabilities such as asset tracking, software compliance management, financial management, and so on.

The HP CSA – AM integration imports cloud services (services that are provisioned using the cloud) from HP CSA to AM, thus allows AM to perform asset tracking, compliance auditing and billing for cloud services. The integration is achieved via HP Connect-It (CIT) scenarios.

Note: Cloud Billing Package version 2.2 does not formally support AM version 9.32. However, it performed as expected in the tests we executed in our lab. We recommend using AM version 9.40 if you plan on implementing the Cloud Billing Package.

This chapter includes:

Overview

This chapter lists the steps necessary to implement the cloud billing integration (CSA – AM) based on the *Cloud Billing Best Practice Package version 2.2*.

Note: This chapter describes the steps of this integration on a high level.

For complete instructions for this integration (including Cloud Billing prerequisites, limitations, known issues, and practices), see:

- *Cloud Billing Best Practice Package version 2.2 Content Pack*. See **Downloads > Cloud Billing Package > CloudBillingBestPracticePackageV2.2.zip**.

The content pack installer, along with the **CB22-ReleaseNotes-EN.pdf** and **Integrating AM with CSA White Paper**, are embedded inside this zipped content pack file.

Prerequisites

- HP Asset Manager is installed, and up and running.
- HP Connect-It is installed, and up and running.
- HP Cloud Service Automation is installed, and up and running.

Install the CloudBillingBestPracticePackageV2.2

The Cloud Billing Content Package is installed on top of the existing Asset Manager database. It modifies the out-of-the- box database structure to enrich its functionality.

Caution: Make sure you have fully tested the installation on a test database which is copied from the production database before you implement it in production.

Always make a full backup of your database before installing the Cloud Billing Content Package to the production environment.

To install the CloudBillingBestPracticePackageV2.2:

1. Run the installer. The welcome page displays introductory information about the Cloud Billing Content Package.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. Select a connection from the list of available connections and enter the password for the log on Admin.
5. Click **Next**.
6. Click **Finish**.

Note: After installing the Cloud Billing Content Package, disconnect Asset Manager Automated Process Manager from the database and then reconnect.

Two CSA connector configuration files (offering.xsd and subscription.xsd) are updated in the Cloud Billing package version 2.2, which are located in the **<Cloud Billing installation folder>\integration\config** folder. When integrating with CIT, you must copy them to the **<Connect-It installation folder>\config\csa\xsd\response** folder and overwrite the old files. Without this step, you may encounter unexpected errors when using the Cloud Billing Content Package.

Integration Steps

1. Configure the connectors for each CIT scenario.

   For details, refer to the HP Connect-It documentation.

   In the *HP Connect-It version 9.50 Connector Guide*, see the sections for the corresponding connectors; in particular, **Chapter 5, Hewlett-Packard Connectors > Configuring the HP Cloud Service Automation Connector > Specify the server information** on page 79, and populate the fields as follows:

Field	Value in CSA connector	Value in AM connector
Server	<IP address or domain name of the CSA server>:<port>/csa/rest	<Your AM database name>
Login	Admin	Admin
Password	Password for admin	Password for admin
Organization Name	CSA-Provider	N/A
User Name	Admin	N/A

   Refer to the following section on page 34 of the *HP Connect-It version 9.50 Connector Guide* for how to populate the **SSL Configuration** page:

   Configuring Connectors > Configuring Advanced Mode Settings > Configuring SSL > For Java connectors

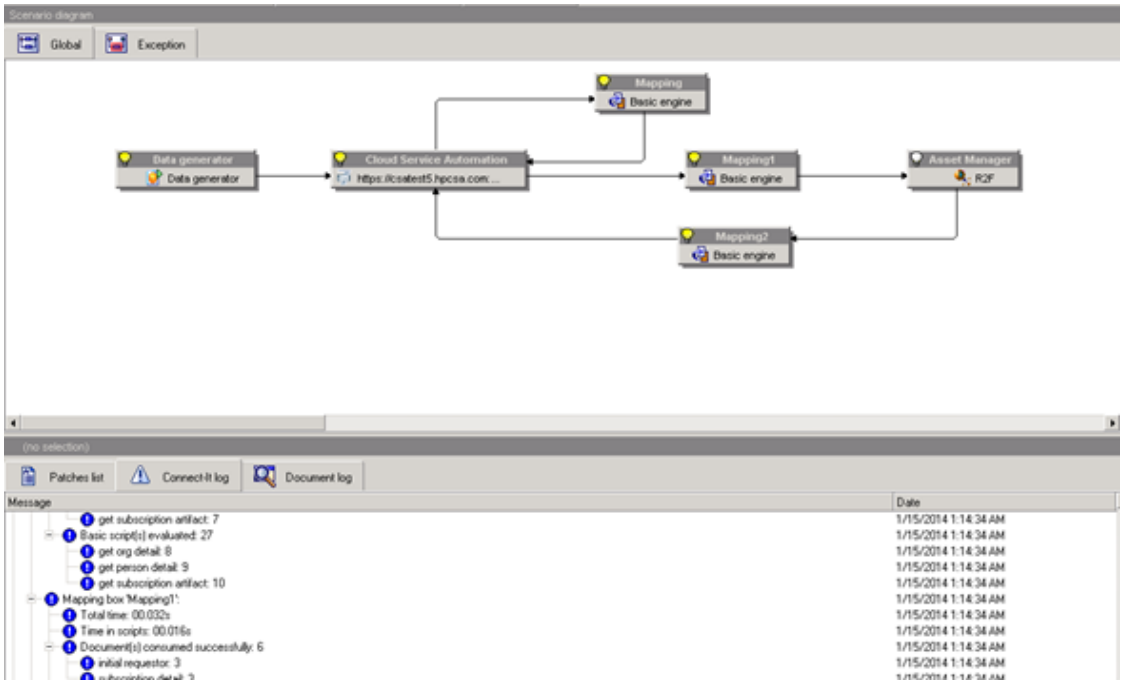
2. Schedule the scenarios to run in the following order:

   a. **catalog.scn.** This Connect-It scenario imports CSA Catalogs and Service Offering.

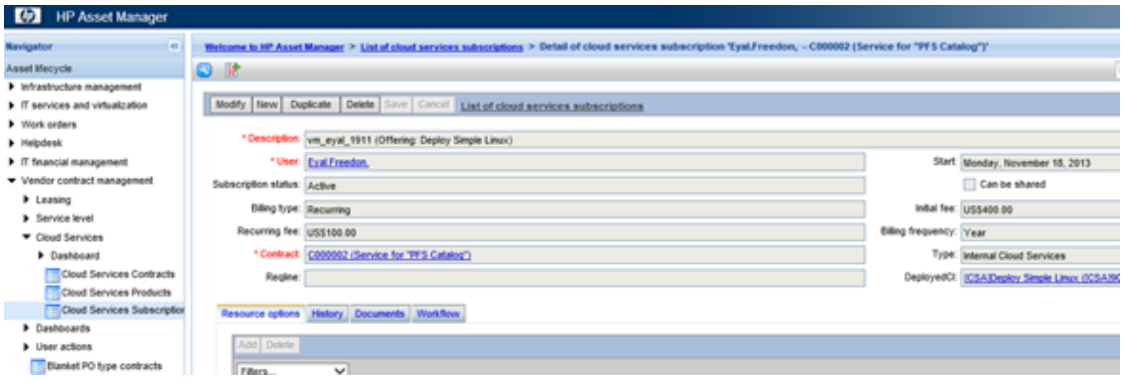
   b. **subscription.scn.** This Connect-It scenario imports CSA subscriptions and its status.

   c. **serviceinstance.scn.** This Connect-It scenario creates and updates the layered Business services and the related client-resource relationship.

3. Check the **Connect-it log** tab for any errors:



4. Log on to Asset Manager. Check the populated Offering, Subscriptions, Assets and Billing info.



Chapter 15: “Sanitize” Server Automation Agent (Virtual Machine Template)

This chapter includes:

Overview

This chapter goal is to prepare the Server Automation (SA) agent on a virtual machine template in order it to be able to install and register a new virtual machine with Server Automation when you create a new clone.

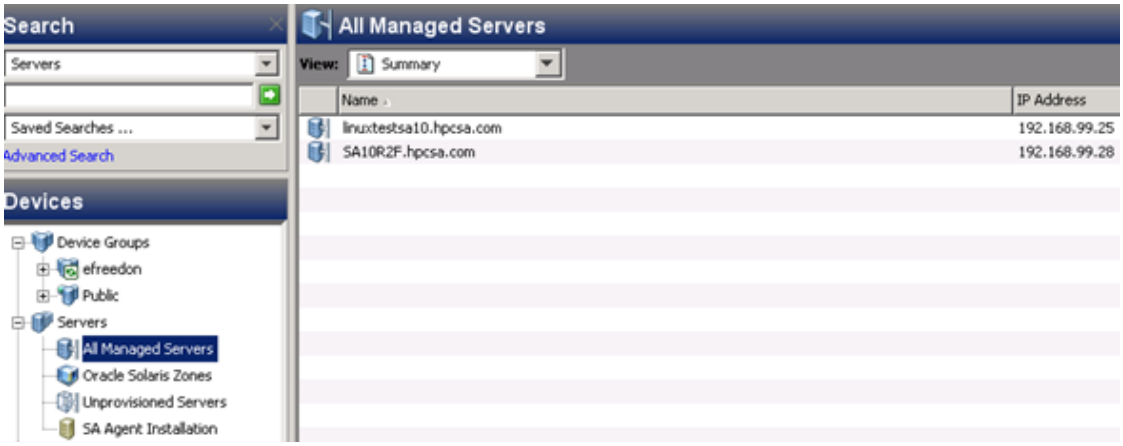
Prerequisites

- HP Server Automation is up and running.
- VMWare VCenter is up with free Disk/RAM resources.

“Sanitation” Steps

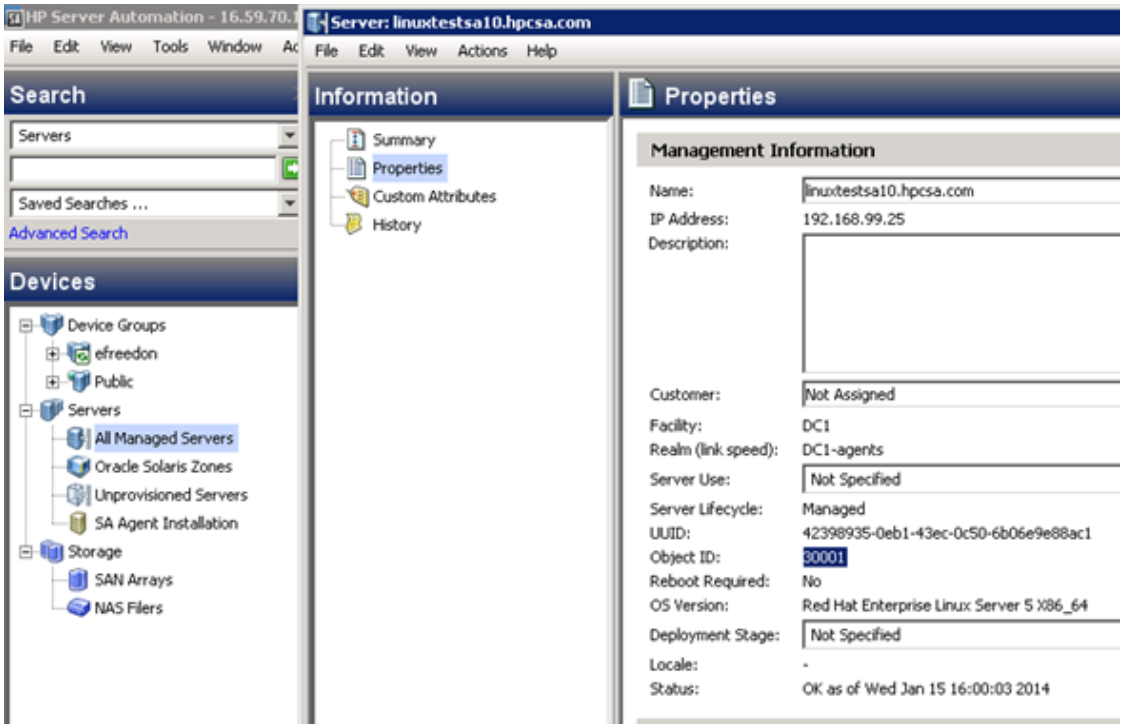
1. Create a virtual machine with the appropriate Operating System Image. Verify its IP address.
2. Launch the **SA Client** and log on to the SA core.
3. Go to **SA Agent Installation** and scan for the IP address of your specific target virtual machine.
4. Right-click on the virtual machine host name and select **Install SA Agent**. Supply the relevant credentials.

5. Verify the target virtual machine is now under the management of SA:



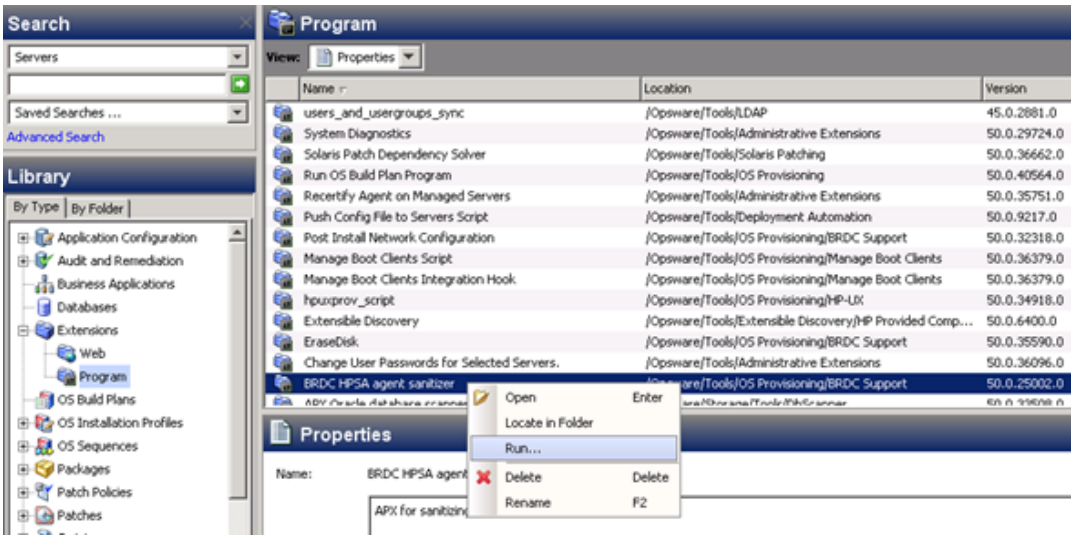
6. Open the Device Explorer of the target virtual machine server and view the server **Properties**.

7. Record the **Object ID** value (use the copy command so you can paste it later).

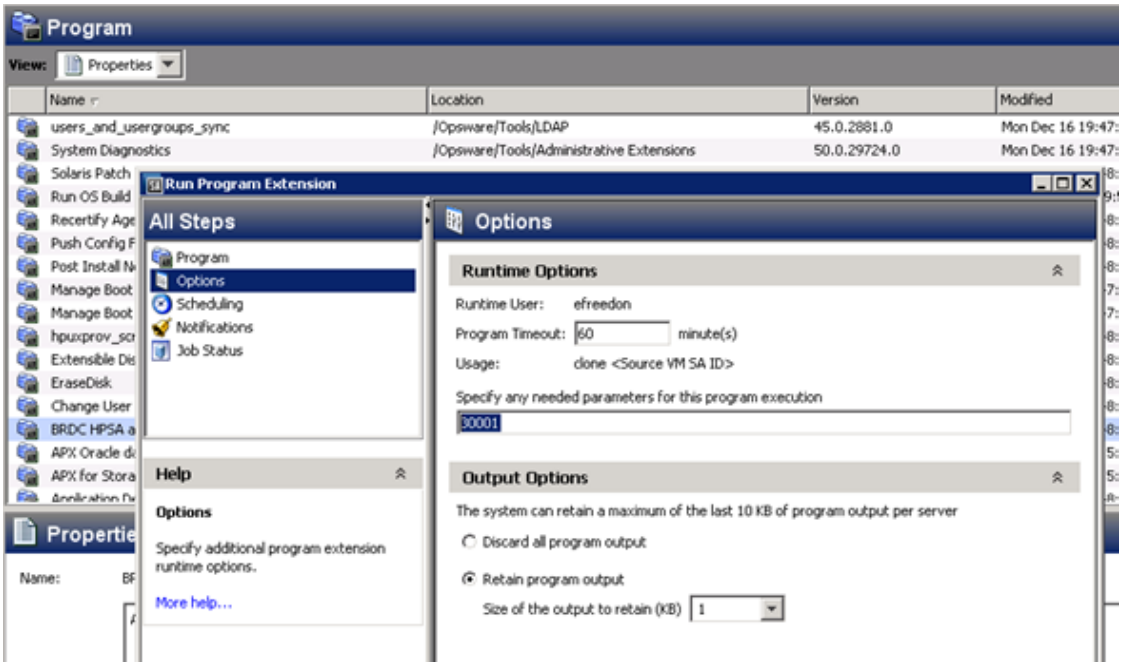


8. Close the Device Explorer.

9. From the SA Library, run the **BRDC HPSA agent sanitizer** Program APX.
   a. In the **Library** tab, navigate to **Extensions > Program**.
   b. Locate the program, right-click, and select **Run…**.

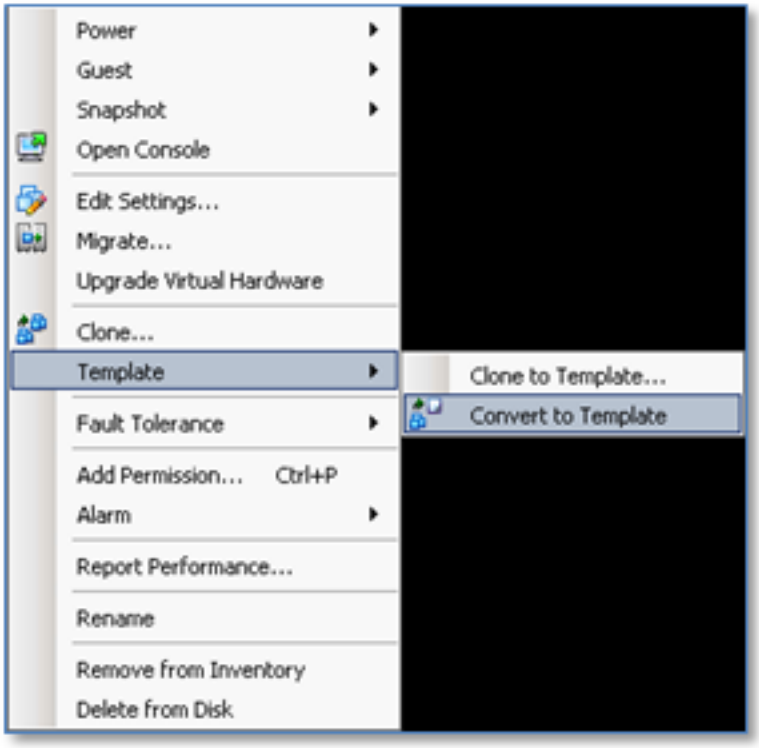


10. In the Options step of the APX, enter the **Object ID** of the target virtual machine server.



11. Wait for the job to complete before shutting down the target virtual machine.
12. Shut down the virtual machine (do not reboot or start).

13. Return to the **vSphere Client** and shut down your target virtual machine using the console.
14. Your virtual machine is now ready to convert into a virtual machine template. When the virtual machine template is cloned and powered on, the SA agent will then register automatically with the core as a new managed server.
15. Return to the vSphere Client. Select your target virtual machine.
16. Right-click and select **Template** and then **Convert to Template**:



Your virtual machine template is now ready to use within HP Cloud Service Automation (HP CSA).

Chapter 16: SA – UCMDB Integration

This chapter includes:

Overview

This section describes how to synchronize HP Server Automation (SA) with HP Universal CMDB (UCMDB) based on the SA – UCMDB connector.

Prerequisites

- HP Server Automation is up and running. Includes managed (provisioned) servers.
- HP Universal CMDB is up and running.

Enabling and Starting the SA – UCMDB Connector

To enable and start the SA – UCMDB connector:

1. Run the **enable** command to configure the SA – UCMDB Connector with the new UCMDB server.

   The following is a simple example of this command: (Run from: /opt/opsware/tell/bin)

   ```
   ./enable --host <UCMDB FQDN> --port <UCMDB Port> --user <UCMDB Admin user> -
   -password <UCMDB Admin password>
   ```

   Note: For more information about the complete enable command set of parameters, syntax, and options, see HP Server Automation version 10.0x All Manuals download (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417676) and select the *HP Server Automation version 10.0 Integration Guide*.

2. Run the start command to restart the SA-UCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

3. Optionally check the status of the SA-UCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

Note: For customizing the SA – UCMDB connector, see HP Server Automation version 10.0x All Manuals download and select the *HP Server Automation version 10.0 Integration Guide*.

Chapter 17: Connecting HP CSA to SX

This chapter includes:

Overview

This section describes how to connect HP Service Exchange (SX) to additional HP Cloud Service Automation (HP CSA) instance.

Prerequisites

- Both HP Service Exchange and Catalog are configured and running.
- HP Cloud Service Automation is configured, and up and running.

Adding Additional HP CSA Instances

During installation, the `installer.properties` file adds one HP CSA instance to the appropriate configuration JSON file. However, it is possible to connect any number of instances of HP CSA to SX. To add additional HP CSA instances, the following file must be edited manually:

`[%SX_HOME%] /WEB-INF/classes/config/csa/instances.json`

Required fields: **endpoint**, **loginName**, and **password**.

Assuming **CSAEurope1** was added through the `installer.properties` file during installation, add additional instances as in the following **CSAEurope2** example.

Note: Enter your unique instance names, URLs, loginNames, and passwords in place of the values in italics in the following **SAEurope2** example.

CSAEurope2 example:

```
{
        "CSAEurope1": {
        "endpoint": "https://example1.com:8444/csa",
        "user": {
        "loginName": "johndoe",
        "password": "mypassword"
},
"organization": "CSA_CONSUMER"
},
"CSAEurope2": {
        "endpoint": "https://example2.com:8444/csa",
        "user": {
        "loginName": "janedoe",
        "password": "my2password"
},
"organization": "CSA_CONSUMER"
}
```

Caution: For a specific module to use the correct instance, relevant configuration files must be edited to include the appropriate HP CSA instance names.

Configure HP CSA to Use LDAP

To configure HP CSA to use LDAP:

1. Log on to HP CSA.
2. Select **Organizations**.
3. Select **HP CSA Consumer**.
4. Select the **LDAP** section.
5. Fill in your LDAP server information and click **Save**.
6. Select the **Access Control** section.

7. Click A**dd-On**.
8. Fill in the AC Config and click **Update**.

Configure HP CSA Approval settings

To configure HP CSA approval settings:

1. Log on to **HP CSA**.
2. Select **Catalogs**.
3. Create a new catalog.
4. Go to the **Approval Policies** section of the new catalog.
5. Fill in **Name**, select a **Template** (that is, Named Approver Template) and add **Approver**.
6. Save the policy

Note: Once HP CSA is added, the HP Propel certificate must be imported into the HP CSA system's trust store. For details, see "SSL Configuration for HP CSA Integration" in the *HP Propel version 1.10 Installation and Configuration Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01315852).

Chapter 18: Connecting SX to SM

This chapter includes:

Overview

This section describes how to connect HP Service Exchange (SX) to an additional HP Service Manager (SM) instance.

Prerequisites

- Both HP Service Exchange and Catalog are configured and running.
- HP Service Manager is up and running.

Adding SM Instances

During installation, the `installer.properties` file adds one SM instance to the appropriate configuration JSON file. However, it is possible to connect any number of instances of SM to SX. To add additional SM instances, the following file must be edited manually:

`[%SX_HOME%] /WEB-INF/classes/config/sm/instances.json`

Required fields: **endpoint**, **loginName**, and **password**

Note:

- Instances of SM with Process Designer installed must have the `withProcessDesigner` parameter set to **true**.
- The following example uses the default port number that HP Propel uses to communicate with SM. If you changed the port number, specify yours in the endpoint address in place of 13080.
- For more information, see "Setting up SX to Use LWSSO" on the next page concerning the `"useLwsso": true` line in the example.

Assuming **SMEurope1** was added through the `installer.properties` file during installation, add any additional SM instances as in the following *SMEurope2* example. Replace the values in italics with your unique URLs, names, and passwords.

SMEurope2 Example:

```
{
        "SMEurope1":{
        "endpoint":"http://sm1.example.com:13080/SM",
        "user": {
        "loginName": "johndoe",
        "password": ""
        },
        "withProcessDesigner": true
},
        "SMEurope2":{
        "endpoint":"http://sm2.example.com:13080/SM",
        "user": {
        "loginName": "janedoe",
        "password": ""
        },
        "useLwsso": true
        }
}
```

Caution: For a specific module to use the correct instance, relevant configuration files must be edited to include the appropriate SM instance names.

Setting up SX to Use LWSSO

The previous example shows that SX is configured to access the **SMEurope2** instance via LWSSO. Note that it is not necessary to supply the password in this case. However, to make the LWSSO communication work, it is necessary that the file `[sx.war]/WEB-INF/classes/config/lwssofmconf.xml` contains a proper LWSSO configuration that matches the target SM instance. In particular:

- The domain element must contain the common domain for SX and the target SM instance (default: hpswlabs.adapps.hp.com.)
- The initString attribute of the crypto element must contain the same passphrase as the SM instance.

Configure for Ticketing

Users of a particular organization are only able to manage tickets on systems configured for that organization.

For ticketing REST API to use a certain instance, edits need to be made to the following file:

`[%SX_HOME%]/WEB-INF/classes/config/tenantInstanceMappings.json`

In `tenantInstanceMappings.json`:

- The `backendSystemType` and `instanceName` field values have to be set for each organization in the file.
- The DEFAULT values need to be added for all users whose organization is not specifically defined elsewhere in the file.

Example:

```
{
        <ORGANIZATION_NAME>: {
        "backendSystemType": "SM",
        "instanceName": "SMInstance1"
},
        "DEFAULT": {
        "backendSystemType":"SM",
        "instanceName":"SMInstance2"
        }
}
```

In this example, **SMInstance1** and **SMInstance2** need to be the unique names previously defined in `instances.json`, and used for identifying these SM instances in other configuration files.

Chapter 19: Customize SM to Work with SX

This chapter includes:

Overview

HP Service Exchange (SX) requires the HP Service Manager (SM) instances to have specific customizations applied in order to enable SX functionality. This chapter describes the needed steps for customizing SM.

Prerequisites

- Both HP Service Exchange and Catalog are configured and running.
- HP Service Manager is up and running.

Import SX Unload Scripts

Necessary customizations of SM are performed by SM unload files.

For the complete list of unload files, see "SX Unload Files" on the next page.

To import unload files into SM:

1. In your SM instance, go to **System Administration > Ongoing Maintenance > Unload Manager > Apply Unload**.
2. Select the **Unload File**—for example, **{ path-to-unload-file }**

3. Select **Backup To**—for example, **{ path-to-unload-file }.backup**
4. Click **Next**.

If there is a conflict with an entry, double-click that entry to see the details, and refer to the "**Possible conflicts applying unload scripts**" chapter in the *HP Propel version 1.10 Installation and Configuration Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01315852).

SX Unload Files

The following unload files contain fundamental SM customizations that are needed for SX to integrate with your SM instance.

Note:

- For full details of each unload file, refer to the *HP Propel version 1.10 Installation and Configuration Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01315852).
- Since Case Exchange is not part of the Request to Fulfill official use cases, its unloads are not described here. If case needed, refer to the *HP Propel version 1.10 Installation and Configuration Guide*.
- The unloads can be found in the SX file system under: **/opt/hp/propel/jboss-as/standalone/deployments/sx.war/contentStorage/…**

1. **SXBaseCustomizations.unl**

   Description: Customize operator "joe.manager".

2. **SXBaseDB.unl**

   Description: The triggers in the following entities:

   - cm3r (changes)
   - subscription:
     - SX.subscription.delete
   - incidents
     - SX.incidents.after.add

- SX.incidents.after.update
- SX.incidents.after.delete

3. **SXBaseExtAccess.unl**

   Description: Provides remote interfaces (SOAP/REST) for:

   - Change detection (see SXBaseDB.unl)
   - Other functionality that is shared for Quotes, Changes and Ticketing features

4. **SXTicketing.unl**

   - **Description:** Changes for Ticketing feature. Customizes SOAP/REST interfaces:
     - SXGlobalLists
     - SXActivityServiceMgt
     - SXTicketInteraction

   The goal of the following three unloads is to support the **Changes** feature. However, changes are not part of the Request to Fulfill official use cases which are only based on SM **Quotes** (see Unload 8 and later).

5. **SXChangesCustomizations.unl**

   Description: Changes feature support:

   - Subscription Approval setup (sets **joe.manager** as the only approver, simplifies change category **Subscription** to two phases).
   - Change catalog item "Custom desktop Provisioning" (changes connector, adds user Options).

6. **SXChangesDB.unl**

   Description: Database triggers for SX **Changes** support.

7. **SXChangesExtAccess.unl**

   Description: SOAP/REST API updates SXSubscription and SXChange endpoints creation which are needed for the **Changes** feature.

8. **SXQuotesCustomizations.unl**

Description: Quotes feature support:

- Sets joe.manager as the only approver of **Manager Approval**
- Customizes approval process/life cycle of **Quotes**:
  - Removes **Financial department approval** from the first phase (Front Line Management Approval).
  - Removes 'Manager approval' from the last phase (Customer Follow-up.)
- Interaction Approval testing item (Performance Desktop) and Approval Process (SVC Off Catalog Request Approval).

9. **SXQuotesDB.unl**

   Description: Database triggers for SX **Quotes** support.

10. **SXQuotesExtAccess.unl**

    Description: SOAP/REST interfaces for SX **Quotes** support:

    - Adds **SX_CloseQuote** Script Library. This script does the Quote Item closing.
    - Adds **SX.CloseQuote** External Access Action. Adds CloseQuote action into SX/Quote remote interface. This action only executes CloseQuote Script Library.
    - Adds SOAP/REST interface for SX/Quote - ocmq (Quote) SM Item access for SX.

11. **SXQuotesTest.unl**

    Description: Data for Quotes feature testing:

    - ScriptLibrary SX_MoveQuoteToCustFollowUpPhase and extractions id="SX.MoveQuoteToCustFollowUpPhase" - Force sets "Customer Follow-up" phase.
    - SOAP/REST interface SX/SXQuoteForTests - remote interface for Quotes Testing, which includes Customer Follow-up phase enforcing.

SM Process Designer – Additional Manual Configuration

This section contains the following topics:

Configuration for Ticketing

This task describes how to change/customize the **SXTicketInteraction Web Service**—specifically how to change the **Expression** tab code by removing the **$G.ess=true** line.

Note: This is relevant for SM with Process Designer Only.

To customize the SX Web Service in SM with Process Designer:

1. Go to **Tailoring > Web Services > Web Service Configuration**.
   a. In the **Object Name** field, add the string **SXTicketInteraction** and click **Search**. The **SXTicketInteraction** settings will load.
   b. Open the **Expressions** tab (click the button).
2. Remove the `$G.ess=true` string.
3. Click **Save**.

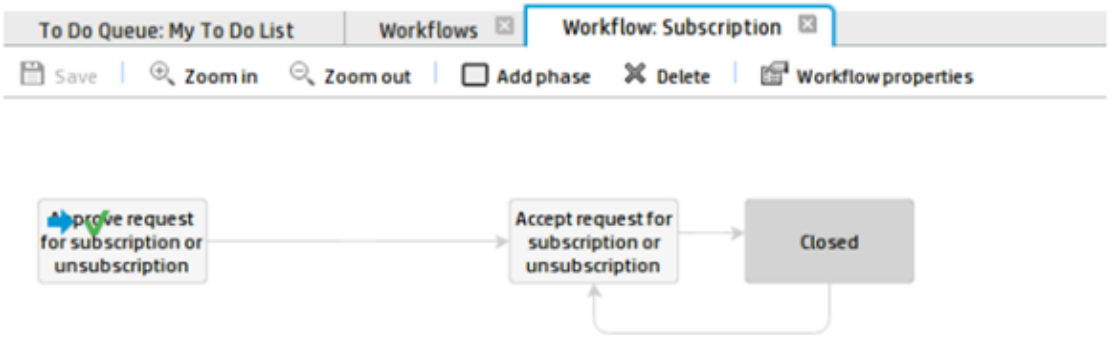
Configuration for Change R2F

Note: This is relevant for SM with Process Designer Only.

To customize the SM Change Workflow for SM with Process Designer:

1. Log on to your Web client.
2. Go to **Change Management > Configuration > Change Workflows**.
3. Select **Subscription** from the list.
4. Remove the second phase from the diagram.
5. Connect the first and third phases by relation.

6. Click to the new relation.
7. Fill in the Command Name **nextphase**. Your window looks as follows:



Apply R2F Unload Scripts

This section contains the following topics:

Unload Scripts

Apply the following Request to Fulfill unload scripts:

1. SXR2FCustomizations.unl
2. SXR2FDB.unl
3. SXR2FExtAccess.unl
4. SXTest.unl

Manual Configuration – R2F

Note: Execute the following manual steps only after the R2F unloads are applied.

To execute the R2F unload scripts:

1. Customize the approval process/life cycle of **Quotes**:
   a. Go to **Request Management > Quotes > Quote Categories**, click **Search** and select the **Customer** record.
   b. Click the first phase box (**Front Line Management Approval**) and remove **Financial Approval** on the **Approvals** tab. Click **OK**.

      Note: If the **Select Event For New Phase** tab opens, click the **Back** button.

   c. Click the last phase (**Customer Approves Delivery of Item**) and remove **Manager Approval** on the **Approvals** tab. Click **OK**.

      Note: If the **Select Event For New Phase**t ab opens, click the **Back** button.

2. Rebuild the **Extaccess Actions** Global List:

   Note: For this step, use the HP Service Manager (SM) client directly (not the Webtier).

   a. Go to **System Definition > Tables > globallist** and open it.
   b. Click **View all records in the table**.
   c. Select the line **Extaccess Actions**.
   d. Right-click anywhere in the bottom part of the screen (the Item View panel), and select **Rebuild Global List**.
   e. Click **Save**.

3. Modify the **DEFAULT** profile:

   Note: This step will not work if you have Process Designer installed.

   a. Go to **System Administration > Ongoing Maintenance > Profiles > Service Desk Profiles**.

   b. Click **Search** and select the **DEFAULT** profile.

   c. Check the **Close** check-box.

   d. Click **Save**.

Manual Configuration – Approvals

This section contains the following topics:

Note: The following configuration is not needed if the HP SM instance is accessed via LWSSO.

Modify Change and Request Profiles Used by Approvers

To modify change and request profiles used by your approvers:

1. Log on as **Admin**.
2. Go to **System Administration > Ongoing Maintenance > Operators**.
3. Enter the log on name and click **Search**.
4. Click the **magnifying glass**  button next to **Change Profile**.
5. Select the **Approvals/Groups** tab.
6. Check **Can Delegate Approvals**.
7. Click **OK**.

8. Click the **magnifying glass**  button next to **Request Profile**.
9. Change to **Alert/Approval** tab.
10. Check **Delegate Approvals**.
11. Click **OK**.
12. Select the **Startup** tab.
13. Change the parameter values in the first table as follows:
    a. name = MAIN MENU
    b. prompt =
    c. string1 = HOME
14. Click **OK**.

Delegate Change Approval

Note: Request to Fulfill official use cases are based on Service Manager's (SM) **Quotes** only. Perform this procedure only if you are going to implement a Request to Fulfill flow that is based on SM Subscription Changes.

To delegate change approval:

1. Go to **System Administration > Operators**.
2. Fill in the log on name: as **joe.manager**, and click **Search**.
3. Add the **change approver** Security Role to **joe.manager**.
4. Click **Save**.
5. Go to **System Administration > Security > Roles**.
6. Select the **change approver** and click **Search**.
7. Click the **Change** row.
8. Under **Settings**, check **Can Delegate Approvals**.
9. Click **Save**.

Set Up Approval Delegation for Each Approver

To set up approval delegation for each approver:

1. Log on as the **Approver**.
2. Go to **Miscellaneous > Approval Delegation**.
3. Click **Add New Delegation**.
4. Select **Delegate Selected Approvals**.
5. Click **Next**.
6. Select the **Request Management** module.
7. Click **Next**.
8. Move **jane.doe** to the right column.
9. Click **Next**.
10. Delegate to **johndoe**. Fill in the **Start** and **End** dates.
11. Click **Next**.
12. Click **Finish**.
13. Repeat for the **Change Management** module.

Manual Configuration – Ticketing

Note: This task only necessary for Process Designer-enabled SM.

To manually configure ticketing:

1. Log on as **Admin**.
2. Go to **Tailoring > Tailoring Tools > Display Options**.
3. In the **Unique ID** field, enter **db.view_add**.

4. Change the condition from:

   ```
   evaluate(add in $L.env) and filename($L.filed)~="dbdict" and
   nullsub($L.io.cond.flag, true)
   ```

   to

   ```
   (evaluate(add in $L.env) or evaluate(new in $L.env)) and
   filename($L.filed)~="dbdict" and nullsub($L.io.cond.flag, true)
   ```

5. Click **Save**.

Part IV: Appendix

Appendix A: Catalog Aggregation

This appendix contains:

Overview

In the HP Propel Management Console, use the Aggregation tile to create and aggregate catalogs from HP Cloud Service Automation (HP CSA) and HP Service Manager (SM).

First, add an adapter so that HP Propel communicates with either HP CSA or SM and its cataloging functions. After the adapter is created, you can aggregate the adapter so that the service and product offerings from HP CSA or SM are made available in an aggregated catalog. The catalog and its offerings are then available in HP Propel and specific organizations can have access to the offerings.

Prerequisites

- HP Propel is configured and integrated with HP Cloud Service Automation and HP Service Manager.

Step 1: Import Web Services into SM

Import web services into SM. An out-of-the-box web service is provided with HP Propel.

1. Transfer the `HPPropelAggregation.unl` Web service file from the HP Propel Portal virtual machine (VM) to the SM system. This file is located in the `/opt/hp/propel/jbossas/standalone/deployments/aggregation.war/WEB-INF/classes/sm-webservice` directory on the HP Propel File system.

2. Start SM. In the left pane of SM, navigate to **System Administration > Ongoing Maintenance > Unload Manager > Apply Unload**. The Unload Manager window is displayed.

3. In the **Unload File** field, browse to the `HPPropelAggregation.unl` web service file.

4. In the **Backup To** field, type a name for the file to be stored as a backup and click **Next**.

   Note: The name for the backup file can be any name you choose.

5. In the dialog that appears for applying the Unload file, click **Yes**. A confirmation message **Hotfix was successfully applied** appears .
6. Click **Finish**.

Step 2: Verify Success of Web Services Import

1. In SM, navigate to the **Tailoring** menu and select **Web Services > Web Service Configuration**.
2. Run a search for:
   - **Service Name:** HPPropelAggregation
   - **Name:** joinsvcdisplay
   - **Object Name:** HPPropelCatalogItem

In the search results, the HPPropelAggregation Web service appears in the External Access Definition window with a list of associated fields.

Step 3: Add an Adapter

HP Propel catalog aggregation provides the HP CSA and SM adapters as available types of default adapters.

1. Log on to the **HP Propel Management Console** and click the **Aggregation** file. The list of available adapters is displayed.
2. To add an adapter, click **Add Adapter**. The Add Adapter window opens.
3. Select the **Adapter Type** you want to add—**HP CSA** or **SM**.
4. Add the **HostName**, **UserName**, and **Password**.
5. Most of the Adapter Properties are preset, but you must edit the following properties:
   - **Required for HP CSA and SM.** Initially, provide a password to the **central-password** field (for the central-user).
   - **Required for HP CSA only.** Initially,provide a user name for the **csa-user** field.

- **Optional for SM only.** You can also edit fields such as **service-catalog-language**, **servicemanager-default-currency-code**, **service-manager-host-protocol**, and **service-manager-port**.

6. When you finish, click **Save**. The new adapter appears in the **Available Adapters** list.

Step 4: Create a New Aggregated Catalog

After you add an adapter, you can aggregate the adapter and create a new catalog, which will populate the catalog's offerings with new products and services in HP Propel.

1. From the HP Propel Management Console, click the **Aggregation** file. The Available Adapters window opens.

2. Select the adapter from which you want to create an aggregated catalog and click **Create**. The available Catalogs window opens, showing which catalogs are available to aggregate.

3. Enter the name of the Destination Catalog for the catalog you want to aggregate, and then select the associated Destination Organization from the list. When you are finished, click **Aggregate**.The color of the **Aggregate** button changes from green to gray, and the status **Pending** appears.

4. To verify that the aggregation is complete, click the **Refresh** button in the Available Adapters window. Aggregation is complete when the Status shows **AGGREGATED**.

To view a newly created catalog and its offerings:

1. In the HP Propel Management Console, navigate to **Catalogs**.

2. Select the catalog you created and click the **Offerings** tab. The items from the newly-added catalog appear as new choices for the consumer.

> **Note:** The next time you log on to the HP Propel Marketplace portal, the newly added catalog items appear as choices in the **New Releases** view.

Appendix B: Integrate DMA with SA (Optional)

Note: This section should be performed by an HP Server Automation (SA) administrator with SA administrator privileges and access.

This appendix contains:

Overview

This section describes the integration of HP Database and Middleware Automation (DMA) with HP Server Automation (SA).

DMA uses SA as an agent infrastructure. DMA integrates with SA to authenticate users, associate users with groups, and determine user privileges. DMA uses SA to acquire knowledge of servers and to send requests to execute workflows on servers. Before DMA can actually work, you have to perform a series of integration steps on your SA system as well as on your new DMA server.

Integration Requirements

The following requirements must be met before integrating HP Database and Middleware Automation (DMA) version 10.21 with HP Server Automation (SA) version 10.01:

- Confirm that you have met all of the general DMA installation requirements
- DMA server software is installed and configured.
- DMA Application Server Provisioning Solution Pack is installed.
- DMA server software and the DMA Client for SA software are installed on the same system.

> **Note:** This system will be referred to as the DMA server in the following instructions.

Install the DMA Client for SA

This stage shows you how to install the DMA Client for SA on the DMA server.

> **Note:** The DMA Client for SA is used to create a DMA software policy in SA. This needs to be done once per SA mesh.

On the DMA server, get the **dma-sa-client-10.21-0.x86_64.rpm** file from the DMA version 10.21 installation media under the **DMA_10.21_Server_and_Client** folder, and then run the following commands as root:

```
$ cd DMA_10.21_Server_and_Client
$ rpm -ivh dma-sa-client-10.21-0.x86_64.rpm
```

Import the DMA APX

The following steps must be performed by an SA administrator.

The SA user (<SA_APX_User>) who imports the DMA APX must belong to a group with the following privileges:

- SA Global Shell (OGSH) permission to Launch Global Shell
- Manage Extensions (Read & Write) permission under Automation Platform Extension
- List, Read, and Write permission on the **/DMA_APX** folder

If the **/DMA_APX** folder does not yet exist, this user must have List, Read, and Write permission on the **/** (root) folder, where the **/DMA_APX** folder will be created.

1. Work with the DMA user with root-level access to the DMA server (or the user that installed the RPMs on the DMA server) to do the following:

   On the DMA server, copy the DMA APX to the SA server Global Shell—For example:

   ```
   $ scp -P 2222 /opt/hp/dma/server/client_bits/westapx.zip
   <SA_APX_user>@<SA_Server>:westapx.zip
   $ scp -P 2222 /opt/hp/dma/server/client_bits/updateWinAdmin.zip
   <SA_APX_user>@<SA_Server>:updateWinAdmin.zip
   ```

2. Log on to the SA server Global Shell and install the DMA APX using the defaults—for example:

   ```
   $ ssh -p 2222 <SA_APX_user>@<SA_Server>
   $ apxtool import westapx.zip
   $ apxtool import updateWinAdmin.zip
   ```

   By default, this places the APX in /DMA_APX. If you want to place it somewhere else, use the **-f <folder>** option.

   To skip the prompts, add **-F** to the end of the command or respond **Y** to all Y/N prompts.

   Note: This creates the **/DMA_APX** (or <folder>) folder.

Install the DMA Client Files Policy

This topic shows you how to install the DMA Client Files policy on the SA server and then to attach and remediate the DMA Client Files policy on all SA managed servers that will be used as DMA targets.

Tip: The following steps must be performed by an SA administrator.

The SA user (<SA_Policy_User>) who installs the policy must belong to a group with the following privileges:

- **Manage Software Policy.** Read & Write under Policy Management.
- **Manage Package.** Read & Write under Package Management.
- List, Read, Write, and Execute permissions on the folder (**/DMA_Client**) that will contain the DMA packages and policy.

Note: The following instructions assume that the DMA Client for SA is installed on the DMA server.

To install the DMA Client Files policy on your SA server, <SA_Server>:

1. In the SA Client, create a **/DMA_Client** folder.
2. As root on the DMA server, go to the **client_bits** folder and run the **dma_upload** script using your <SA_Policy_User> account. For example:

```
$ cd /opt/hp/dma/server/client_bits
$ sh ./dma_upload.sh -host <SA_Server> -user <SA_Policy_User>
-password <SA_Policy_Password>
-keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/publicKey
-folderName /DMA_Client
```

   Note: If you omit the password option (- password), you will be prompted for the password.

3. *Optional:* To verify that the policy has been properly uploaded, perform the following steps in the SA Client:

   Go to **Library > By Folder >** `DMA_Client`.

   The `DMA_Client` folder should be populated. Verify that the DMA Client Files policy is included.

4. For each server that will be used as a DMA target, attach and remediate the DMA Client Files policy.

Set Up the SA Groups and Users

This topic shows you how to set up the necessary SA groups and users for DMA.

This section contains the following topics:

Note: The following steps must be performed by an SA administrator.

Your SA administrator may have a security model that is more finely grained. Follow your SA policies for naming and granting permissions to groups.

DMA User Groups

The following table provides examples of the types of user groups that you will need to use and manage DMA in your environment.

Group Type	Example Name	Capability Require	Description
DMA administrators	DMA Admins	Administrator	Users in this group will perform DMA administrative duties.
Users who will create DMA workflows	DMA Workflow Creators	Workflow Creator	Users in this group will have the ability to create DMA workflows. **Note:** Once a workflow is created, it can be modified using Role Based Access (RBAC) as needed.
Users who will run DMA workflows	DMA Workflow Runners	Login Access	Users in this group will have the ability to run DMA workflows.

To set up your DMA user groups:

1. On the SA server to which DMA will connect, create each of the groups listed in the table and any additional groups that you need.
2. Grant the following permissions to each group:
   - **List**, **Read**, and **Execute** permission for the **/DMA_APX** folder
   - Managed Servers and Groups
   - READ access to all managed servers that will be added to DMA

   In order to add servers to DMA organizations, a user must also have permission to see those servers in SA. This requires either **Read** permission on the pertinent customer or facility or **Read** permission on the device group or groups where the servers reside, depending on how your SA administrator manages permissions.

   Note: Use the SA Client to grant these permissions.
3. Add at least one user to each group.

Later, you will register these groups as DMA roles and assign each role the appropriate DMA capability.

DMA Connector User

An additional SA user, <dma_connector_user>, is required to configure the DMA connector to SA.

Note: This user does not need to be a member of any of the SA groups that you just created.

This user will be used by DMA to connect to SA whenever a specific, personalized SA account cannot be used—for example, to verify whether a log on is allowed.

To create the DMA connector user:

1. On the SA server to which DMA will connect, create a new SA user (for example: dma_connector_user).
2. Grant this new user the following permissions:
   - **List**, **Read**, and **Execute** permission for the **/DMA_Client** folder
   - **List** permission for all parent folders of the **/DMA_Client** folder
   - Managed Servers and Groups
   - Manage Software Policy (READ)
   - READ access to all managed servers that will be added to DMA

This requires either Read permission on the pertinent customer or facility or Read permission on the device group or groups where the servers reside, depending on how your SA administrator manages permissions.

Start the DMA

The first time you start DMA, you must log on as the default initial DMA administrator (dma_initial_admin) to configure the operating environment.

1. As root, start the **DMA version 10.21** server—for example:

   ```
   $ service dma start
   ```

2. Use a Web browser to connect to the DMA server:

   ```
   https://<dma_server>:8443/dma
   ```

   Here, <DMA_Server> is the fully qualified host name of your DMA server.

3. Accept the certificates. The **DMA version 10.21** installation page appears.

4. Enter an initial password for the **dma_initial_ admin** user, retype the password, and then click **Submit**.

5. To log on, enter the user name **dma_initial_admin**, the new password for the password, and then click **Login**.

Configure the Connector

This topic shows you how to configure the connector that enables DMA and SA to communicate.

To configure the connector that enables DMA and SA to communicate:

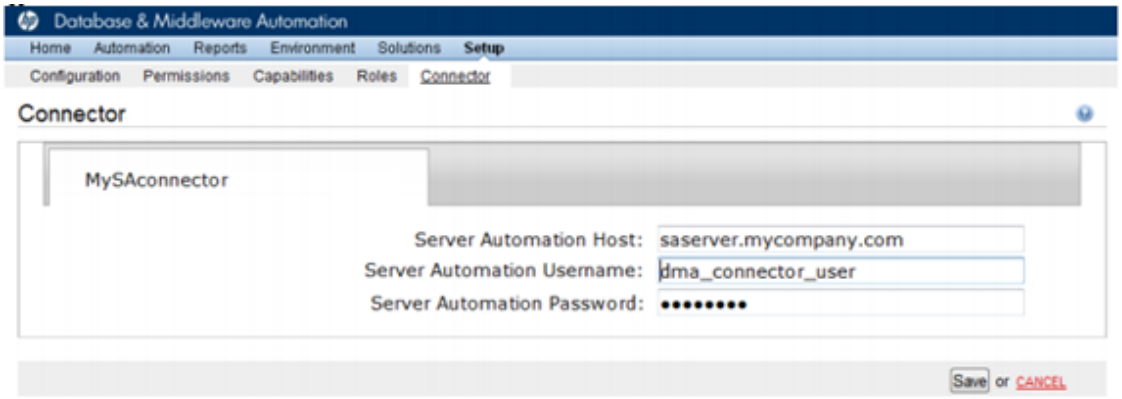
1. Log on as **dma_initial_admin**.

2. On the **Setup > Connector** page, in the lower right corner, click the **Add Connector button.**

3. Specify a name for your connector, and click **Enter**.

4. Specify the **Server Automation Host**, **Server Automation Username**, and **Server Automation Password** for your connector:

   The Server Automation Username is the SA user that you created in "Set Up the SA Groups and Users" on page 148—for example, **dma_connector_user**.



5. Click **Save**. A Successful Configuration message appears.

6. As root, restart the DMA version 10.21 server—for example:

```
$ service dma restart
```

7. Use a Web browser to connect to the DMA server:

```
https://<dma_server>:8443/dma
```

   Here, <DMA_Server> is the fully qualified host name of your DMA server.

8. To log on, enter the username **dma_initial_admin**, your password, and then click **Login**.

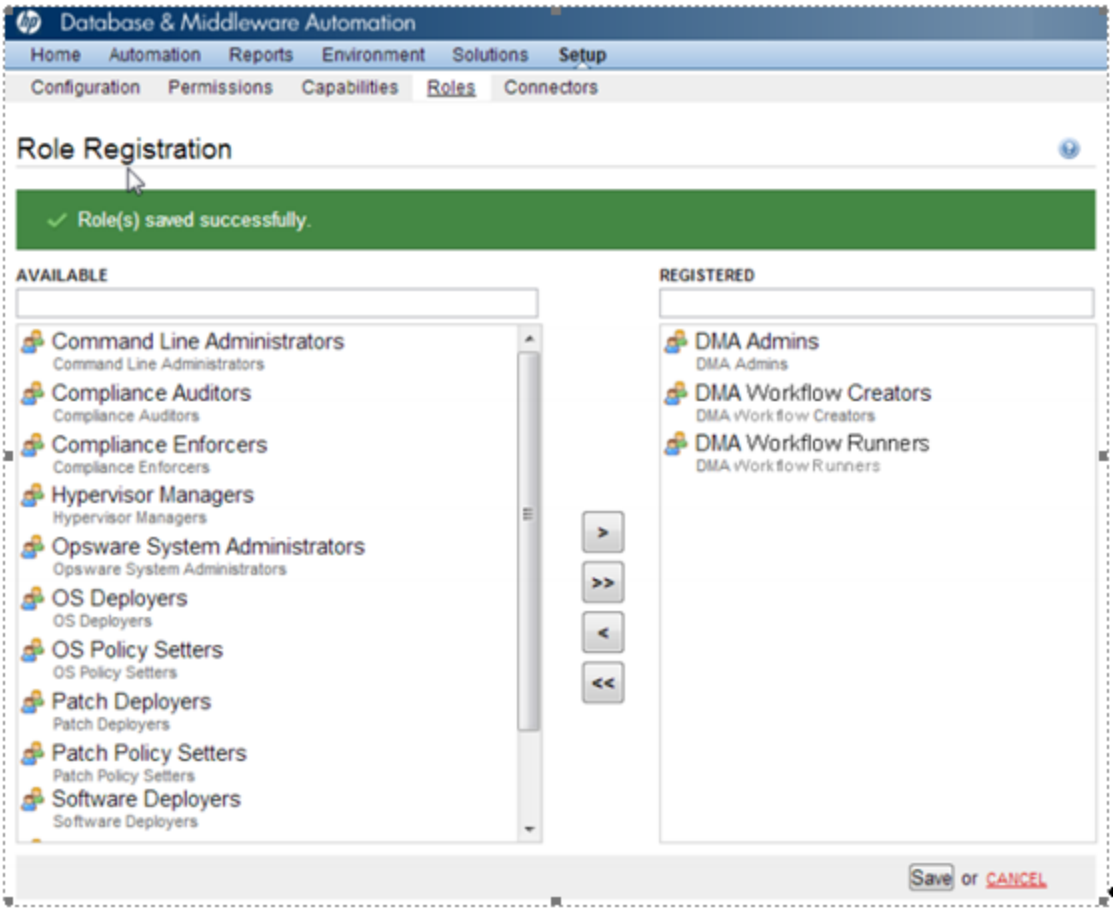
Register DMA Roles

This topic shows how to register DMA roles. DMA obtains the complete set of available roles from SA—including the groups that your SA administrator configured in "Set Up the SA Groups and Users" on page 148.

To register DMA Roles:

1. Log on as **dma_initial_ admin** and go to **Setup > Roles**. The roles that are available to be registered are listed on the left. The roles that are already registered are listed on the right.

2. Select a user group from the **AVAILABLE** list on the left side of the screen and then click the > button. The selected role moves to the **REGISTERED** list on the right.



3. Click the **Save** button to save your changes.

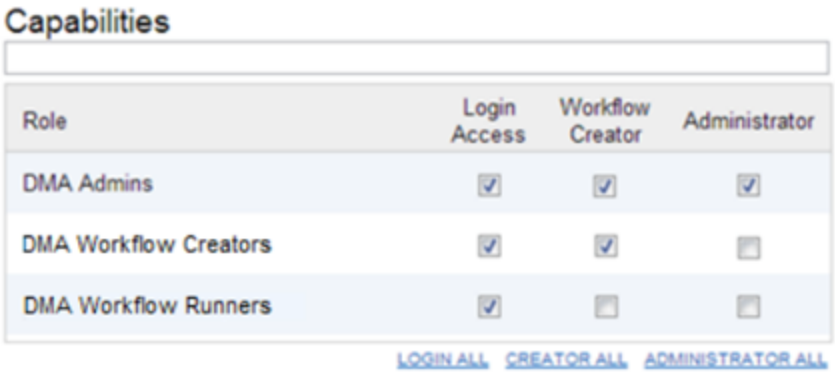
Assign DMA Capabilities

This topic shows you how to assign DMA capabilities. Capabilities are collections of related privileges. You must assign capabilities to each role that you registered in the previous step.

To assign DMA Capabilities:

1. Log on as **dma_initial_ admin**.
2. Go to **Setup > Capabilities**.

3. Select a role and check the desired capabilities for that role.



Note: Only users whose roles have Administrator capability can import solution packs.

4. In the lower right corner, click **Save**.
5. Log out of DMA.

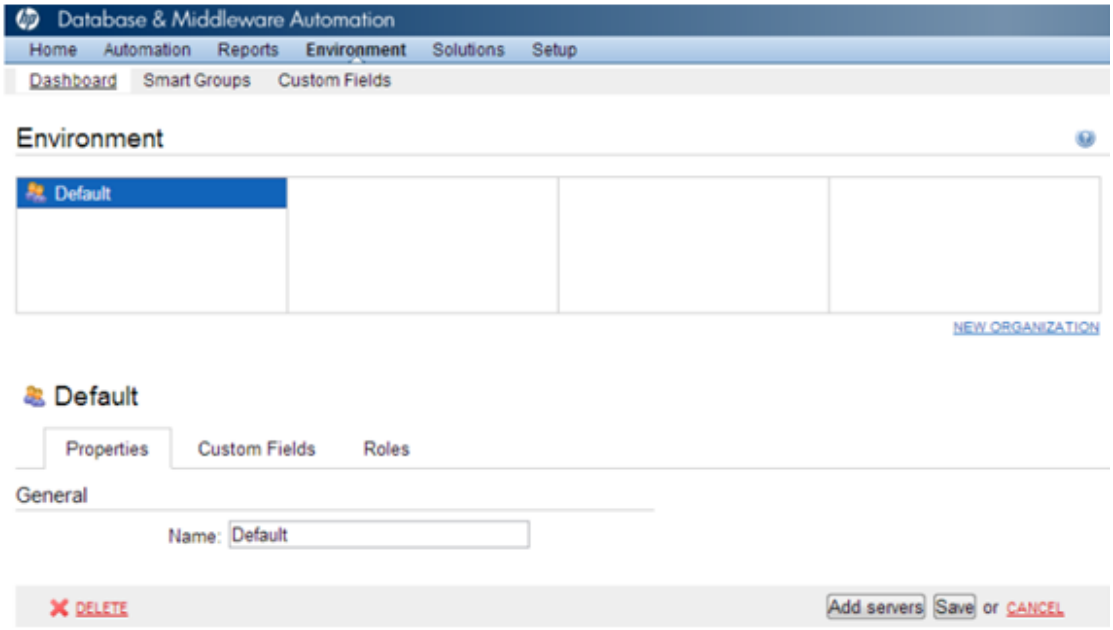
Add Available Targets

This topic shows you how to make target servers available to DMA users.

To add target servers:

1. Log on to DMA as a user with Administrator capability—for example, a user with the DMA Admins role—and go to the **Environment** page.

2. In the first **Environment** box, select **Default**.



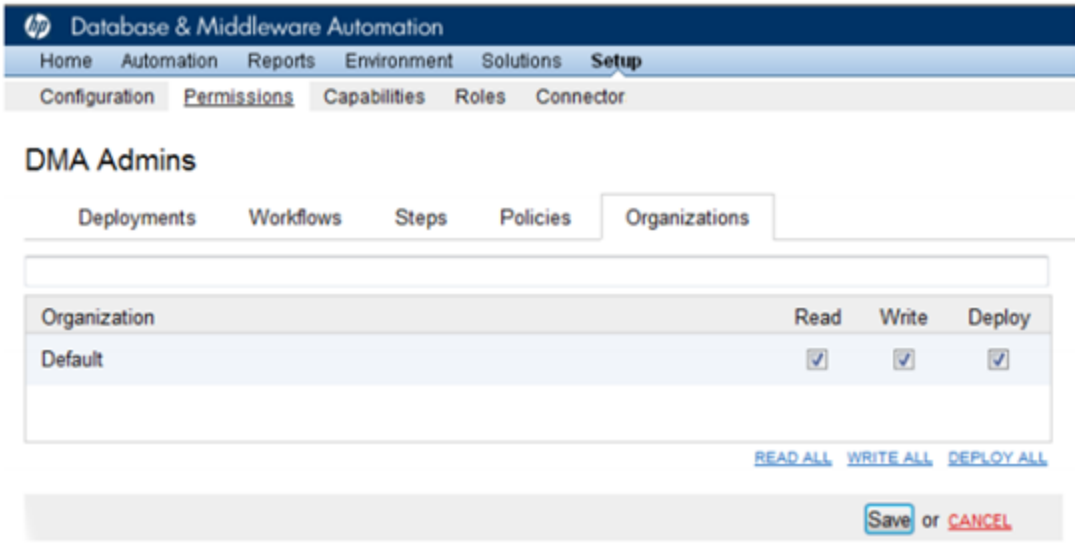
3. In the lower right-corner, click **Add servers**. The **Add servers to organization** dialog box appears.

4. Select any servers that you want to use as DMA targets.

5. Click **Add** and then click **Save** in the lower right-hand corner.

To grant user roles permission to access the servers:

1. Go to **Setup** > **Permissions**.
2. Select the name of the role to which you want to grant server permissions—for example, **DMA Admins**.
3. Click **Organizations**.
4. Select the appropriate permissions for this role—for example: **Read**, **Write**, and **Deploy**.



5. In the lower right-hand corner, click **Save**.

Import a DMA Solution Pack

This topic shows you how to import solution packs. These instructions apply to any solution pack.

The DMA version 10.21 installation media provides solution packs in the following folders:

- **DMA_10.21_Server_and_Client** contains the Discovery solution pack (Discovery.zip).
- **DMA_10.21_Database_Solution_Packs** contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- **DMA_10.21_Middleware_Solution_Packs** contains all of the application server solution packs (provisioning, patching, configuration management, and release management).

To import the solution pack:

1. Log on to DMA as a DMA administrator—that is, a user who has at least one role with Administrator capability.
2. On the **Solutions** > **Installed** tab, click the **Browse** button in the lower right-hand corner. The Choose File dialog box opens.
3. Locate and select the desired solution pack ZIP file—either from the DMA version 10.21 installation media or from HP Software Support Online (https://softwaresupport.hp.com/group/softwaresupport/home)—and then click **Open**.
4. Click **Import solution pack**.

Note: Import the Discovery solution pack first. It is not automatically installed in DMA. You must import it if you want to use the discovery workflows.

For more information and troubleshooting information, refer to the *HP Database and Middleware Automation version 10.21 Installation Guide* (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00997087).