

HP Value Stream

Software Version: 1.2

Detect to Correct Concept and Configuration Guide

Document Release Date: December 2014



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

© Copyright 2005 - 2014 Hewlett-Packard Development Company, L.P.

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

Welcome to This Guide	8
How This Guide is Organized	8
Who Should Read This Guide	8
Additional Online Resources	10
Part I: Detect to Correct Concept Guide	11
Chapter 1: Detect to Correct Value Stream Concepts	12
Overview	12
HP Detect to Correct Value Stream Diagram	14
Detect to Correct Functional Components	16
Detect to Correct Artifacts	18
Use Cases	20
Terms and Definitions	22
Part II: Detect to Correct Configuration Guide	25
Chapter 2: Detect to Correct Value Stream Configurations	26
Overview	26
Prerequisites	27
Users and Permissions	27
Hardware and Software Requirements	28
Supported Versions	28
Enterprise Hardware and Software Requirements	29
HP Business Service Management – Overview	29
HP Application Lifecycle Management – Overview	30
HP Service Manager – Overview	30
HP Universal CMDB – Overview	30
HP Operations Orchestration – Overview	31
HP Release Control – Overview	32
Chapter 3: Detect to Correct Monitoring	33
Overview	33
Chapter 4: BSM – SM Incidents Exchange Integration	36
Overview	36
Configure Connection from BSM to SM	36
Add an OMi – SM Integration Instance	40

Verify BSM to SM Configuration	43
Chapter 5: BSM – SM Business Impact Report Integration	45
Overview	45
Access Business Impact Report via SM User Interface	45
Verify Business Impact Report Integration	47
Chapter 6: UCMDB – SM Integration Configuration	48
Overview	48
Set Up UCMDB for Integration with SM Using ServiceManagerAdapter9-x	48
Prerequisites	49
Configure SM Adapter in UCMDB	49
Create a New Integration Point	49
Set Up the Data Push Job	50
Run the Data Push Jobs	51
Set Up SM for Integration with UCMDB	51
Prerequisites	51
Add the UCMDB Connection Information to the System Information Record	51
Verify UCMDB – SM Integration	53
Set Up UCMDB for Integration with SM Using ServiceManagerAdapter7-1	54
Prerequisites	54
Configure SM Adapter in UCMDB	54
Create a New Integration Point	54
Set Up the RMI Job	56
Set Up the Changes Job	56
Run the Data Push Jobs	56
Set Up SM for Integration with UCMDB	58
Prerequisites	58
Add the UCMDB Connection Information to the System Information Record	58
Verify UCMDB – SM Integration	58
Chapter 7: UCMDB – BSM Integration Configuration	60
Overview	60
Create UCMDB to BSM Integration Point in BSM	60
Deploy Package CMS_to_RTSM_Sync.zip on UCMDB	60
Enable the CMDB 9.x Integration Point	61
Configure BSM 9.x Integration Point	63
Deploy Package CSM_to_RTSM_Sync.zip on BSM	63
Enable the CMDB 9.x Integration Point	64
Verify UCMDB – BSM Configuration	67
Chapter 8: Execute HP OO Flows from SM	68
Overview	68

Enable HP OO Flows from SM – KM Module	68
Prerequisites	68
Configure SSL on HP OO	70
Configure SSL on SM	74
Add an SMOO integration instance	75
Enable an Integration Instance	76
Configure LWSSO in HP OO	76
Chapter 9: Execute HP OO Flows from BSM	79
Overview	79
Execute HP OO Flows from BSM User Interface	79
Configure the Link Between BSM and HP OO	79
Import HP OO Server Certificates to BSM	80
Permissions	81
Chapter 10: Security Settings Configuration	82
Overview	82
Configure the SM Web Tier for LWSSO Support	83
Configure LWSSO in BSM	89
Verify SM – HP OO Flow	90
Verify BSM – HP OO Run Book Invocation Integration	91
Configure LWSSO in UCMDB	91
Configure LWSSO in RC	92
Chapter 11: UCMDB – RC Integration Configuration	93
Overview	93
Set Up UCMDB for Integration with RC	93
Prerequisites	93
Deploy the RC Integration Package	93
Set Up RC for Integration with UCMDB	94
Chapter 12: SM – RC Integration Configuration	95
Overview	95
Set Up SM Integration with RC	95
Prerequisites	95
Add RC Integration Instance	96
Set Up RC for Integration with SM	96
Verify SM – RC Integration	99
Chapter 13: SM – ALM/QC Integration	100
Overview	100
HP Application Lifecycle Management	101
HP Service Manager	106

HP ALM Synchronizer	114
Part III: Appendix	121
Appendix A: Importing Unload Files into HP Service Manager	122
Importing Unload files into Service Manager	122
Appendix B: Downtime Management	124
Downtime Management – Overview	124
Prerequisites	127
Users and Permissions	127
Global ID Generator	127
Downtime Management Solution Diagram	128
Integration Flow	129
A. To create a SMIS SMBSM_DOWNTIME integration	129
B. To integrate SM RFC downtimes with UCMDDB	131
C. To integrate SM downtimes with BSM (via UCMDDB)	132
D. To send BSM downtime start/stop events ("Off" by default)	133

Welcome to This Guide

Welcome to the HP Detect to Correct Value Stream Concept and Configuration Guide. The Detect to Correct Value Stream is focused on IT activities such as event detection, diagnostics, incident management, change and problem management (including synchronization with ALM as defect manager), and remediation. The user decides how many configurations are implemented to achieve the management level required.

This chapter includes the following topics:

How This Guide is Organized	8
Who Should Read This Guide	8
Additional Online Resources	10

How This Guide is Organized

This guide contains the following parts:

Part I: "Detect to Correct Concept Guide" on page 11

Describes the Detect to Correct Value Stream concepts

Part II: "Detect to Correct Configuration Guide" on page 25

Describes the Detect to Correct Value Stream configurations

Part III: "Appendix" on page 121

- Defines how to import Unload files into HP Service Manager
- Provides information about setting up Downtime Management for the Detect to Correct Value Stream

Who Should Read This Guide

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 Best Practices 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/hpsupport.

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.

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://support.openview.hp.com/sc/solutions/index.jsp>.

Part I: Detect to Correct Concept Guide

Chapter 1: Detect to Correct Value Stream Concepts

This chapter includes the following topics:

Overview	12
HP Detect to Correct Value Stream Diagram	14
Detect to Correct Functional Components	16
Detect to Correct Artifacts	18
Use Cases	20
Terms and Definitions	22

Overview

The Detect to Correct (D2C) Value Stream provides a framework for integrating the monitoring, management, remediation and other operational aspects associated with realized services and/or those under construction. It also provides a comprehensive overview of the business of IT operations and the services these teams deliver. Anchored by the service model, D2C delivers new levels of insight which help improve understanding of the interdependencies among the various operational domains; including event, incident, problem, change, and configuration management. It also provides the business context for operational requests and new requirements. D2C is designed to accommodate a variety of sourcing methodologies across services, technologies, and functions.

Detect to Correct connects the various functions involved in service operations to enhance results and efficiencies. Today, most teams work in isolation because they lack visibility to key artifacts and lack a common taxonomy to facilitate collaboration and sharing. When attempts are made to resolve this issue using a process-led approach, they are often too difficult and/or complex to finish or there is a technology or organization shift that invalidates the result. Using the service model and value stream, the functional components and data exchanges that comprise D2C remain consistent regardless of changes in technology, organization structure, process and/or methodologies.

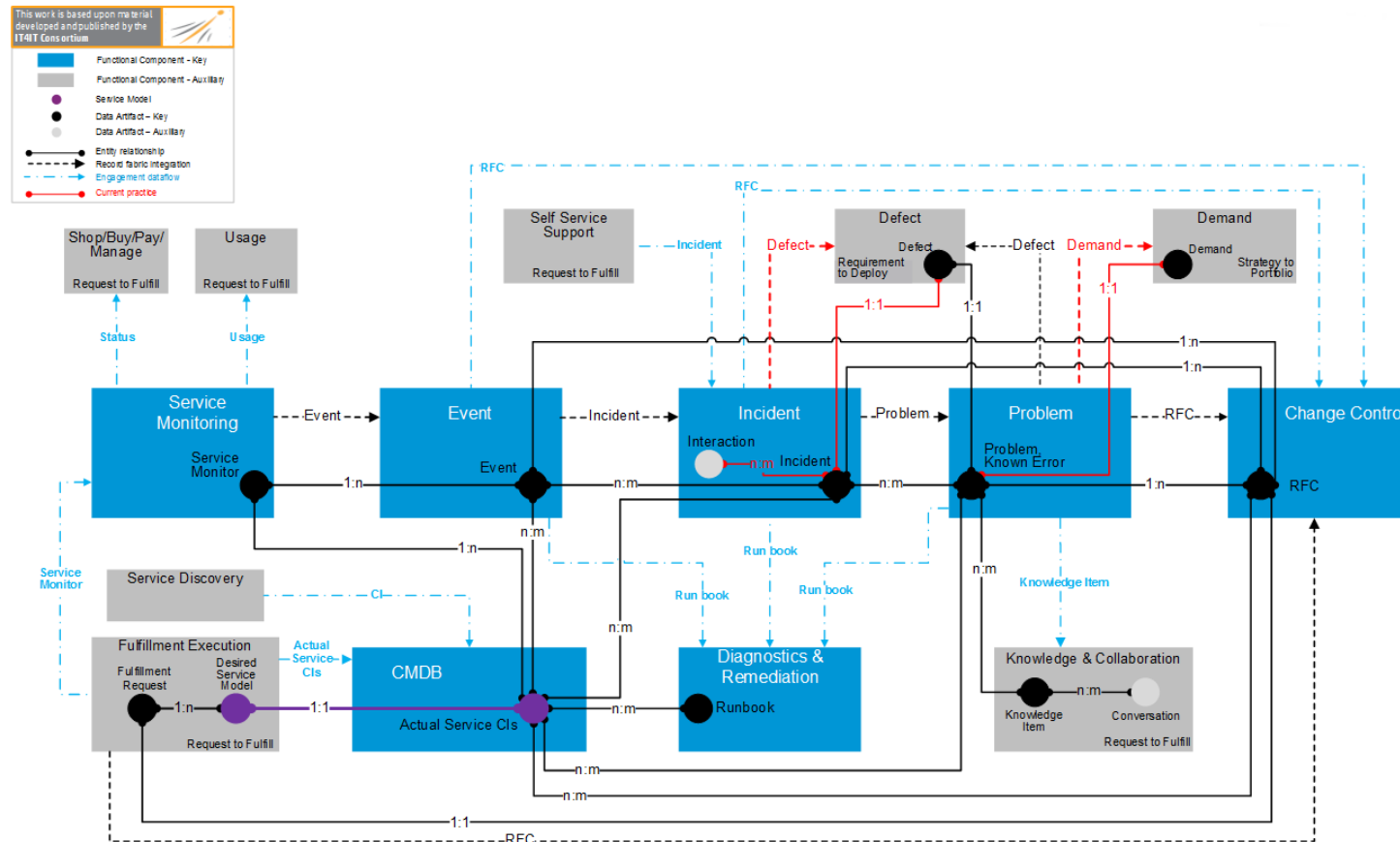
Today, all IT organizations have the capability to address operational issues, but suffer from the following limitations:

- Timely identification, impact analysis, prioritization and remediation of issues
- Complexity of service delivery across multiple internal and external functions makes getting things done difficult
- End-to-end traceability of incidents and events (all the way back to the original requirements) is virtually impossible
- Inability to keep the service model data current (for example, topology/CMDB)

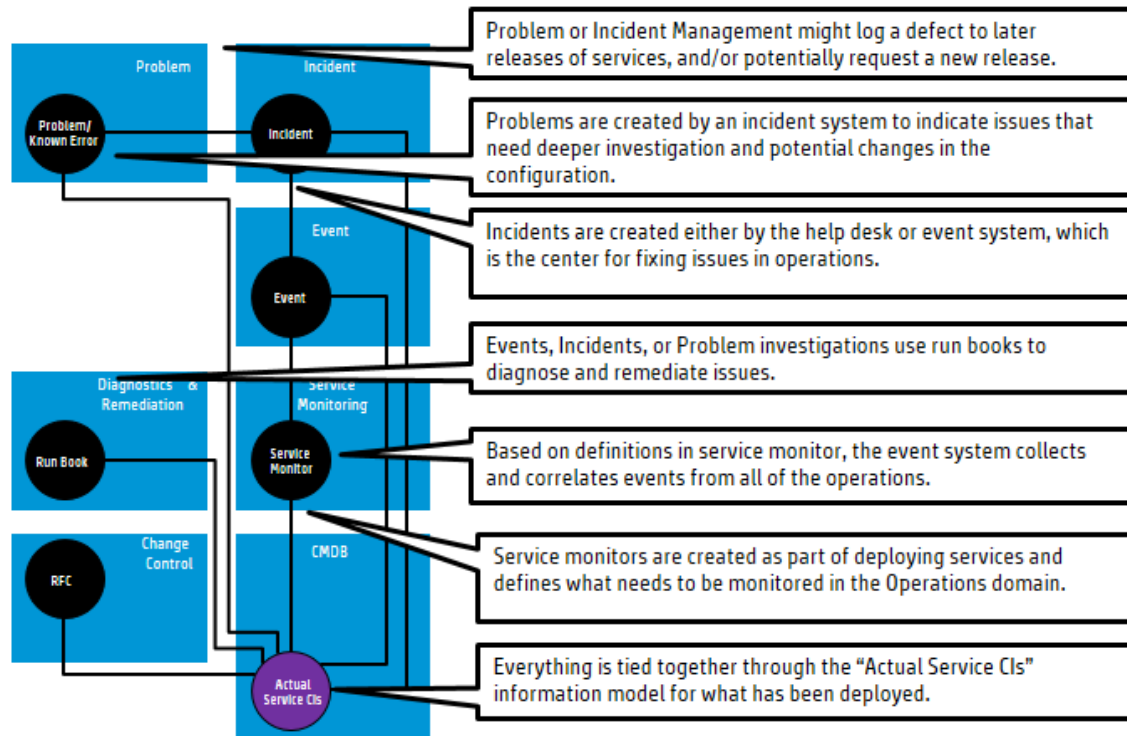
The role of IT operations becomes more complex with each technology disruption. New solutions are consistently introduced faster than the retirement of the old which compounds the degree of difficulty of managing services in a cost-effective manner. The emergence of cloud-sourcing has added a new dimension to this problem by limiting the operational visibility into services. D2C provides the framework for maximizing visibility, promotes consistency and responsiveness, and brings together the various IT functions and suppliers involved regardless of sourcing strategy.

HP Detect to Correct Value Stream Diagram

The following diagram illustrates the Functional Components and Artifacts that comprise the Detect to Correct Value Stream, as described in version 1.1 of Reference Architecture.



Detect to Correct Functional Components



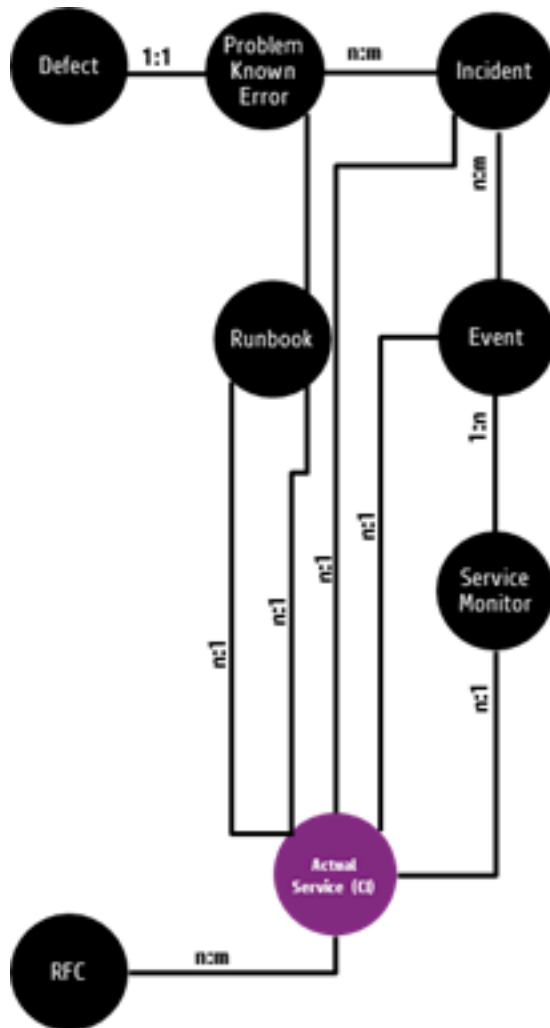
The functional components for this value stream are:

- **Service Monitoring.** Performs the monitoring of all aspects of a service, including infrastructure, applications, information and security.
- **Event Management.** Receives events and performs categorization, correlation and prioritization on them.
- **Incident Management.** Restores normal service operations as quickly as possible and minimizes the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
- **Problem Management.** Responsible for managing the life cycle of all problems. The primary objectives of problem management, from an ITIL viewpoint, are to prevent incidents from occurring and to minimize the impact of incidents that cannot be prevented.
- **Configuration Management.** Identify, control, record, report, audit and verify service configuration items; including versions, baselines, constituent components, their attributes and relationships. It is focused on the configuration management aspect of the ITIL Service Asset and Configuration Management within the IT service management area.

- **Diagnostics and Remediation.** Through the use of manual and automated run books, provides diagnostic information and/or remediation steps to shorten the mean-time-to-repair.
- **Change Management.** Ensures standardized, auditable methods and procedures are used for efficient and prompt handling of all changes to minimize overall business risk.

Detect to Correct Artifacts

The Detect to Correct Value Stream contains both key and auxiliary artifacts that interact with the configuration items that comprise the physical service model.



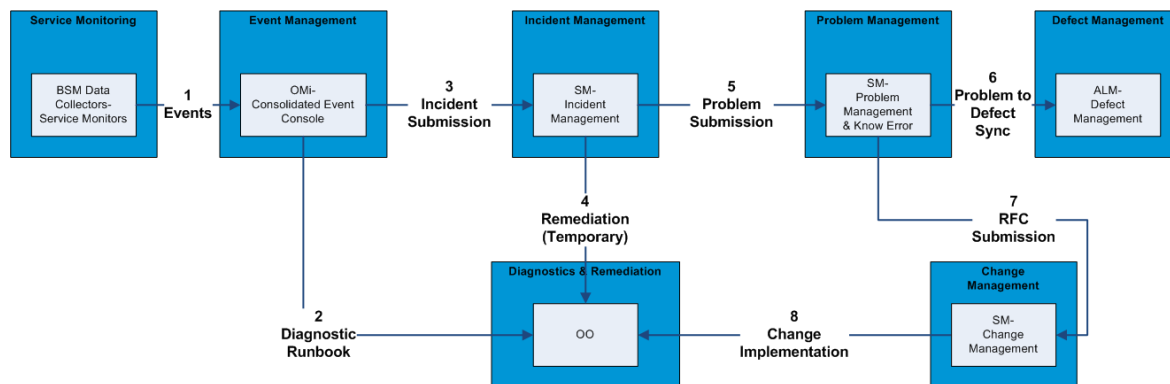
The artifacts for this value stream are:

- **Service Monitor.** Specifies the monitoring of a configuration item or a service in order to maintain visibility to and understand the current operational status. The service monitor supports the concepts of active and passive monitoring.
- **Event.** A change of state that has significance for the management of a service or configuration item. The term is also used to mean an alert or notification created by any service, configuration item, or monitoring tool. Events typically require IT personnel to take actions, and often lead to incidents being logged.

- **Incident.** An unplanned interruption or reduction in the quality of a service. Failure of a configuration item that has not yet affected service is also an incident—for example, failure of one disk from a mirror set.
- **Problem, Known Error.** A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation. Known errors are problems that have documented root cause and workarounds already captured.
- **Defect.** A shared artifact. A flaw in a component or system that can cause the component or system to fail to perform its required function—for example, an incorrect statement or data definition. A defect, if encountered during execution, may cause a failure of the component or system.
- **Run Book.** Is a compilation of the routine remediation actions to be taken by the administrator or operator of the service. A run book can be either a set of manual steps or an automated script.
- **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.
- **Usage.** An auxiliary artifact (not pictured) that was previously defined in the Request to Fulfillment (R2F) Value Stream. In this context, it is the active measurement of service usage.
- **Interaction.** An auxiliary artifact (not pictured) that is a record of any end-user contact with the service desk agents. In some cases, the interaction can be resolved by either the agent or self-service knowledge without creating an incident. In other cases, an interaction can be associated with an existing incident or used to create a new one.
- **Knowledge item.** A shared artifact (not pictured) that was previously defined in R2F. In this context, it may be used to solve a problem and may also create new knowledge items as a result of problem management activities.

Use Cases

The following diagram and description provide a high level data flow for the main use case of the Detect to Correct Value Stream. This describes how artifacts are created and maintained between the various HP Products that implement the Functional Components described in ["Detect to Correct Functional Components" on page 16](#).



The following prerequisite must be met before implementing the use case main flow:

- Discovery populates HP Universal CMDB (UCMDB) and UCMDB syncs the CIs to HP Service Manager (SM) and HP Business Service Management (BSM).

Use case main flow:

1. The monitors report their data into BSM and the events are correlated to causal and symptom events..
2. HP Operations Orchestration (OO) is used (from BSM) to run diagnostics and check the status of the service.
3. An Incident is opened from the causal event.
4. OO is fired from the Incident through the SM Knowledge Management (KM) to automate a workaround fix like restart.
5. A problem is opened from the incident in SM.
6. A defect is opened to address the root cause of the problem.
7. To apply the permanent fix, a Request for Change (RFC) is opened from the problem in SM.
 - a. The RFC goes through the change life cycle (using HP Release Control (RC) to evaluate, assess, and schedule the Change Implementation).

- b. Downtime (DT) is created in BSM so that the monitoring team is aware that the system will be down for planned maintenance.
- 8. In order to automate the Change Implementation, OO is invoked.

Terms and Definitions

- **Actual State**

Current physical and logical state of the IT infrastructure.

- **Affected CI(s)**

CI(s) that are impacted by the issue at hand. In most implementations, affected business CI(s) will give greater value to the operation's organization.

- **Authorized State**

Physical and logical state of the IT infrastructure expected by the organization.

- **Business Impact**

Composed of associated business services and applications, the status of Service Level Agreements (SLAs), the current operational state of the business services and applications.

- **Change Advisory Board (CAB)**

Group of people that advises the Change Manager in the assessment, prioritization, and scheduling of changes. This board is usually made up of representatives from all areas within the IT service provider, the business, and third parties such as suppliers.

- **Change Conflicts**

When two or more changes require the same resources, such as people or components of the IT infrastructure, or that impact the same CIs in a given time frame.

- **Configuration Item (CI)**

Any component that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the Configuration Management System and is maintained throughout its life cycle by Configuration Management.

Configuration Items typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLAs.

- **Deployment Release**

The implementation of a change into an environment (either test or production).

- **Desired Unplanned Change**

A configuration change that:

- Does not have an RFC
- Does not cause a policy breach
- Can be kept and authorized

- **Emergency Change Advisory Board (ECAB)**

A sub-set of the Change Advisory Board who make decisions about high impact emergency changes. Membership in the ECAB may be decided at the time a meeting is called, and depends on the nature of the emergency change.

- **Enterprise Operations Center (EOC)**

Central or regional location for monitoring the organization's IT operations.

- **Event Management**

Process responsible for managing events throughout their life cycle.

One of the main activities of IT operations.

- **Incident Management**

Process responsible for managing the life cycle of all incidents.

Primary objective of incident management is to return the IT service to users as quickly as possible.

- **Information Technology Infrastructure Library (ITIL)**

Collection of volumes intended to assist and promote effective and efficient Information Technology (IT) service management practices in organizations.

- **Operational Business Impact**

Issue assigned by BSM. The components of Business Impact pertain to the effect the issue has on the implementation of business processes.

Impact is often based on how service levels will be affected.

Impact and Urgency/Severity are used to assign priority.

- **Operational Severity**

Issue assigned by BSM. The components of Severity pertain to the seriousness of their effect on the quality of IT service(s) at hand (the affected CI(s)).

- **Planned Change**

A configuration change that is derived from an RFC.

- **Request For Change (RFC)**

An initial request that entails some form of modification, addition, or removal of CI(s). Once approved, these requests evolve into changes.

- **Suspect CI(s)**

Configuration Item(s) thought to be the cause of the issue at hand.

- **Target CI**

Configuration Item linked to the causal event/incident.

- **Undesired Unplanned Change**

A configuration change that:

- Does not have an RFC
- Causes a policy breach
- Will result in an RFC to roll back to the previous configuration

Part II: Detect to Correct Configuration Guide

Chapter 2: Detect to Correct Value Stream Configurations

This chapter includes the following topics:

Overview	26
Prerequisites	27
Hardware and Software Requirements	28
HP Business Service Management – Overview	29
HP Application Lifecycle Management – Overview	30
HP Service Manager – Overview	30
HP Universal CMDB – Overview	30
HP Operations Orchestration – Overview	31
HP Release Control – Overview	32

Overview

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

There are many ways to monitor the Detect to Correct (D2C) Value Stream. One example is described in the [HP End-to-End Service Monitoring and Event Management Best Practices v2.x](#).

End-to-End Service Monitoring in the IT Environment provides our suggested method for deploying and implementing smart end-to-end service monitoring solutions to ensure adherence to the level agreed upon between the service provider and the service consumer.

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:

- Comprehensive end-to-end service monitoring will benefit the event management process, especially in the detection and correlation phases.
- 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 Universal CMDB.** Server is installed. Data flow probe is connected and running (different server than BSM server).
- **HP Application Lifecycle Management.** Server, client, and the synchronizer package are installed.
- **HP Business Service Management.** Server, including the OMi application, are installed and running.

BSM machine has the DDM data flow probe connected and running.

- **HP Service Manager.** Server, Client, Help Server, Web Tier, and Knowledge Management are installed and running.
- **HP Operations Orchestration.** Central and Studio are installed and available for use.
- **HP Release Control.**

Users and Permissions

The same user name must be used on all the products (they can have different passwords). For example, user NocOperator1 must exist in both BSM and SM in order to drill down from OMi events into SM incidents. As well, the same user should exist in HP OO in order to execute HP OO run books on CIs.

Hardware and Software Requirements

This section includes the following topics:

Supported Versions	28
Enterprise Hardware and Software Requirements	29

Supported Versions

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

Product	Version	Instructions
Business Service Management	<ul style="list-style-type: none">9.21 Recommended. 9.21	For installation instructions, see the HP Business Service Management Deployment Guides Package .
Application Lifecycle Management	11.52 Recommended. 11.52	For installation instructions, see the HP Application Lifecycle Management Installation Guide .
Service Manager	<ul style="list-style-type: none">9.31 Recommended. 9.31	For installation instructions, see the HP Service Manager Interactive Installation Guide .
Universal CMDB	<ul style="list-style-type: none">10.01 Recommended. 10.01	For installation instructions, see the HP Universal CMDB Interactive Deployment Guide .
Operations Orchestration	<ul style="list-style-type: none">9.05 or later Recommended. 9.05	For installation instructions, see the HP Operations Orchestration Installation and Upgrade Guide .
Release Control	<ul style="list-style-type: none">9.20 Recommended. 9.20	For installation instructions, see the HP Release Control Deployment 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 Universal CMDB.** For more information, see the [HP Universal CMDB Support Matrix](#).
- **HP Application Lifecycle Management.** For more information, see the [HP Application Lifecycle Management Readme](#).
- **HP Business Service Management.** For more information, see [HP Business Service Management System Requirements and Support Matrixes](#).
- **HP Service Manager.** For more information, see the [HP Service Manager Support Matrix](#).
- **HP Operations Orchestration.** For more information, see the [HP Operations Orchestration System Requirements](#).
- **HP Release Control.** For more information, see the [HP Release Control Support Matrix](#).

HP Business Service Management – Overview

HP Business Service Management (BSM) helps businesses optimize the performance and availability of applications in production and proactively resolve problems when they arise, thus assisting critical production applications to perform as required and deliver business results.

BSM helps customers model their business processes and services by providing a framework for mapping the complex and dynamic dependencies between applications and their supporting infrastructure. BSM helps customers optimize business availability and event handling by proactively detecting problems in order to prioritize problem resolution based on business impact and service level compliance.

BSM consists of an integrated set of applications for real-time performance and availability monitoring from a business perspective—service level management, end-user management, event handling, system availability management, and custom reporting and alerting. BSM is based on a common foundation of shared workflow, administration and reporting services, shared assets, and expertise.

BSM helps customers to reduce mean time to detection (MTTD) and end-user downtime by proactively detecting application performance and availability problems—assisting in escalation of problems to the right department at the right priority, as well as resolution of performance problems before service-level objectives are breached. This helps organizations reach toward the goal of the maximization of value of IT operations and reduction of Total Cost of Ownership (TCO) of IT infrastructure.

HP Application Lifecycle Management – Overview

HP Application Lifecycle Management (ALM) empowers IT to manage the core application life cycle, from requirements through deployment, granting application teams the crucial visibility and collaboration needed for predictable, repeatable, and adaptable delivery of modern applications.

Application Lifecycle Management is a complex process. Whether your organization is predominantly Agile or you are using both iterative and sequential methods, the aim of effective life cycle management is greater predictability, heightened repeatability, improved quality, and a ready accommodation of change. Understanding project milestones, deliverables, and resource and budget requirements and keeping track of project health, standards and quality indicators, allow delivery managers to achieve these objectives.

ALM simplifies and organizes application management by providing you with systematic control over the process. It helps you create a framework and foundation for your Application Lifecycle Management workflow in a central repository.

HP Service Manager – Overview

HP Service Manager stores the managed or expected state of CIs and CI relationships as attribute values in a CI record. To be part of the integration, a CI attribute in your UCMDB system must map to a managed field in the 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 consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) 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 Release Control – Overview

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

Chapter 3: Detect to Correct Monitoring

This chapter includes the following topics:

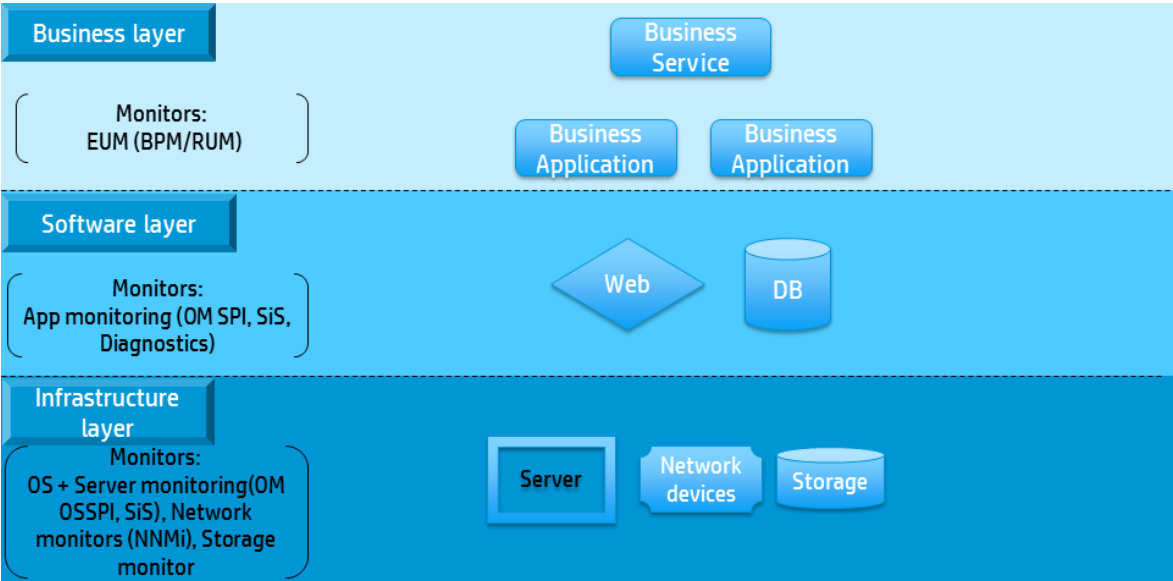
Overview 33

Overview

End-to-End Service Monitoring in the IT Environment provides our suggested best practices for deploying and implementing smart end-to-end service monitoring solutions to ensure adherence to the level agreed upon between the service provider and the service consumer. Feel free to use the entire best practice's solution, a mix of the various products, or just use a single product to address your monitoring needs.

Note: Comprehensive end-to-end service monitoring will benefit the event management process, especially in the detection and correlation phases.

The following diagram illustrates how an IT services environment might look—illustrating the complexity of a contemporary business service, relying/depending on multiple infrastructure and network components, as well as with the software running on top of it. The organization responsible for this service benefits greatly when it can monitor and assess the status and performance of the components.



A typical business service usually consists of the three layers as shown in the diagram. Each of those layers can be monitored separately, providing insight into the status and performance of the corresponding aspect. The best results are achieved when all monitors are implemented and the aggregated data is supplied to a central console to be accessible for further reporting and processing/analysis.

The central console is BSM OMi as part of the Service and Operations Bridge (SaOB).

- **Business layer.** In the Business layer, IT monitors the application itself, mainly by end-user monitoring (EUM). It contains line of business (LOB), business services, and complex business applications—for example, an email service is a Business Service and Microsoft (MS) Exchange Suite is a Business Application.
- **Software layer.** In the Software layer, IT monitors the software components that are installed on the servers that provide services to the application. It connects the business layer to the infrastructure layer, and contains all of the software components—for example, IIS software on a Client Access Server is a Web Application and MS SQL software on an MS Exchange mailbox server is a database.
- **Infrastructure layer.** In the Infrastructure layer, IT monitors the infrastructure that is used by the software layer—server, network, and other infrastructure services.
 - **Network Monitoring.** Network Monitoring is a major part of the IT infrastructure services that provides networking services to the IT environment—for example, network switch, routers, and so on. Most contemporary business services require an adequate network infrastructure to operate. This mandates special attention to the monitoring of network equipment and configuration to enable stable communications.

Each layer is divided into the following four sections:

- **Overview.** Overview of what is being monitoring and why it is being monitored
- **Tools.** List of tools to be used for this type of monitoring
- **Installation and Configuration.** Flow of actions for applying the monitoring solution; including characterizing and configuring the tools and monitors
- **Recommendations.** Set of field best practice recommendations to help in effectively applying the monitoring solution

For use cases and more information about End-to-End Service Monitoring Best Practices, see [HP End-to-End Service Monitoring and Event Management Best Practices v2.x](#).

Chapter 4: BSM – SM Incidents Exchange Integration

This chapter includes the following topics:

Overview	36
Configure Connection from BSM to SM	36
Add an OMi – SM Integration Instance	40
Verify BSM to SM Configuration	43

Overview

HP Business Service Management (BSM) Operations Management events, and their updates, can be automatically or manually forwarded to HP Service Manager (SM) as an incident. The Operations Management Event Browser shows what events have been forwarded, including detailed information about the corresponding SM incident, on the **Forwarding** tab of the corresponding events.

In addition, changes made to an Operations Management event are synchronized to the related SM incident, and vice versa.

Extended Incident Details view can be launched from the event record (opens the SM user interface in the correct context).

Extended Event Details view can be launched from the incident record (opens the BSM user interface in the correct context).


Optionally (and highly recommended), you can use Lightweight Single Sign-On (LWSSO) to bypass the log-on prompts. This is covered further in this guide.

Configure Connection from BSM to SM

Note:

- Before starting this procedure, create a user in SM that will be used for the integration and will have full administrative permissions. Remember these user details as you will need them in the following procedure.
- For instructions on how to create the user, see the Service Manager documentation.
- Be sure to modify **ServiceManagerAdapter.groovy** to support SM version 9.31.

To configure the SM server as a target connected server:

1. In the BSM console, navigate to **Admin > Operations Management > Setup > Connected Servers**.
2. In the Connected Servers page, click the **New Item**  button. The **Create New Server Connection** wizard opens.
3. In the **Display Name** field, enter a name for the target SM server. By default, the **Name** field is filled automatically.
4. Enter a description for the new target server.
5. Select the **Active** check box and click **Next**.
6. Select **External Event Processing** and click **Next**.
7. Enter the **Fully Qualified DNS Name** of the SM target server and click **Next**.
8. For the Integration type, select **Call Groovy Script Adapter** and select **sm:serviceManagerAdapter**.

Note: The default web tier value is **webtier-9.30**. If you are using another web tier version, update its name via the *Manage Scripts* wizard via the *Manage Scripts* link in this window.

9. Click **Manage Scripts**.
 - a. In the opened window, select **sm: ServiceManagerAdapter**.
 - b. Click the **Edit item** button, select the **Script** tab, and change the **SM_WEB_TIER_NAME** value to **webtier-9.31**.
 - c. Click **OK** to save this copy of the script and close the Manage Scripts dialog box.
10. Click **Next**. The Outgoing Connection pane appears.

11. Provide the following event forwarding credentials to the event forwarding user that you already created in SM.

Field	Sample Value	Description
Username	<Integration Username>	The user name for the integration user you set up previously.
Password	<password>	The password for the user you just specified.
Password (Repeat)	<password>	The password you just specified.
Port	<13080>	The port configured on the SM side for the integration with Operations Management. (See Note "To find the port number to enter:" on the next page.)
Use secure HTTP	<not selected>	Confirm this check box is not selected.
Supports Synchronize and Transfer Control	<selected>	<p>Confirm this check box is selected.</p> <p>When the Supports Synchronize and Transfer Control flag is set, an Operations Management operator is then able to transfer ownership of the event to the target connected server.</p> <p>If the Supports Synchronize and Transfer Control flag is not set, then the option Synchronize and Transfer Control does not appear in the list of forwarding types when configuring forwarding rules.</p> <p>If the Supports Synchronize and Transfer Control flag is not set for any target connected server, the Transfer Control option does not appear at all in the Event Browser context menu.</p> <p>If a specific server is configured without the Supports Synchronize and Transfer Control flag set, then that server is not available in the Event Browser context menu as a server to which you can transfer ownership.</p>

Note: To find the port number to enter:

- Navigate to the following file:

**<HP Service Manager root directory>/HP/Service
Manager<version>/Server/RUN/sm.ini**

- In the **sm.ini** file, you will find two port entries. If you want to use a secure HTTP connection, select the **httpPort** with the default port number **13080** or **httpsPort** with the default port number **13443**. The actual values for the ports can differ from these default values depending on how they are configured. Note that using HTTP/s in this integration is not covered by this guide and will require more configurations than listed here.

For details, see the *HP Business Service Management OMi Extensibility Guide*. It is recommended to use HTTP.

- Enter the appropriate value in the **Port** field.

12. Click the **Test connection** link located on the top of the window.
13. Click **Next**. The Event Drilldown pane appears.
14. In addition to forwarding events to SM, if you also want to drill down into SM, you need to specify the fully qualified DNS name and port of the SM web tier.

Note:

- To enable event drilldown to SM, you must install a web tier client for your SM server according to your SM server install/configuration instructions.
- In the Event Drilldown dialog box of the Connected Servers manager, configure the server where you installed the web tier client along with the configured port used.
- If you do not specify a server in the Event Drilldown dialog box of the Connected Servers manager, it is assumed that the web tier client is installed on the server used for forwarding events and event changes to SM, and receiving event changes returned from SM.
- If nothing is configured in the Event Drilldown dialog box, and the web tier client is not installed on the SM server machine, the web browser will not be able to find the requested URL.

Click **Next**. The Incoming Connection pane appears.

15. To enable event changes to be synchronized from SM to Operations Management, a new user is created. The new user is automatically created by the application.

- a. Define a new password.


Note: Take note of the given user name and password you defined. You will need to provide it later when configuring the SM server to communicate with the server hosting Operations Management.

- b. Click **Finish**. The target SM server appears in the list of Connected Servers.

Add an OMi – SM Integration Instance

Before you can use the OMi – SM integration, you must add an OMi – SM integration instance in SM's Integration Manager and enable it.

To add an OMi – SM integration instance:

1. In the SM console, navigate to **Tailoring > Integration Manager**. The **Integration Instance Manager** opens.
2. Click the **Add**  button. The **Integration Template Selection** wizard opens.

Note: There is no need to select the **Import Mapping** check box.

3. Select **SMOMi** from the Integration Template list, and click **Next**. The Integration Instance Information pane appears.
4. In the Integration Instance Information pane, select **Run at system startup**.
 - For **Interval Time (s)**, enter **150**.
 - For **Max Retry Times**, enter **3**.

Note: These fields are mandatory. Leave the other fields blank.

- Save the log files.

Note:

- The default location to save the log files is your **C:** directory, but it is suggested to save the log files in a drive that does not contain your operating system.
- Set your log level as **WARNING**.

5. Click **Next**. The Integration Instance Parameters pane appears.
6. On the General Parameters tab, complete the following fields as necessary:

Field	Sample Value	Description
omi.server.url	http:// <servername>:<port> >opr-gateway/rest/ synchronization/event/	URL address of the OMi Server RESTful web service. Replace <servername> and <port> with the BSM gateway host name and port number of your OMi server. Note: The default port is 80 .
username	<user defined by BSM>	User name used to access the OMi Server RESTful web service interface using Basic authentication. (See Step 15 in Configure Connection from BSM to SM)
http.conn.timeout	30	HTTP connection time-out setting in seconds.
http.rec.timeout	30	HTTP send time-out setting in seconds.
http.send.timeout	30	HTTP send time-out setting in seconds.

Field	Sample Value	Description
sm.mgr.id	<automatically created>	Universally Unique Identifier (UUID) automatically generated for this instance of SM. Note: The value of this field is automatically created each time you add an OMi – SM instance. Do not change the automatically created value or the integration will not work properly.
omi.reference.prefix	urn:x-hp:2009:opr:	Prefix of the BDM External Process Reference field that will be present in incoming synchronization requests from the OMi server. Note: This field has a fixed value. Do not change it.
sm.reference.prefix	urn:x-hp:2009:sm:	Prefix of the BDM External Process Reference field that will be present in outgoing synchronization requests from SM. Note: This field has a fixed value. Do not change it.
omi.eventdetail.base url	http://<servername>:<port>/opr-console/ opr-evt-details.jsp?eventId=	Basic URL address of the event detail page in OMi. Replace <servername> and <port> with the BSM gateway host name and port number of your OMi server.

- On the **Secure Parameters** tab, complete the following field:

Field	Description
Password	Password of the user name used to access the OMi Server RESTful web service interface using Basic authentication.

- Click **Next** twice, and then click **Finish**. The Integration Instance Manager window appears.
- To enable the integration, right-click the integration row and do not select an option.

10. Click the **Enable** option on the left side of the integration list. You will be prompted with an action verification.
11. Select **Yes**.
12. Click the **Enable** link.

Note: The OMi – SM integration does not use the settings on the **Integration Instance** fields and Integration Instance Mapping panes.

The OMi – SM integration instance is added enabling it to start working with the integration.

Verify BSM to SM Configuration

The BSM to SM integration enables the creation of SM incidents based on BSM events.

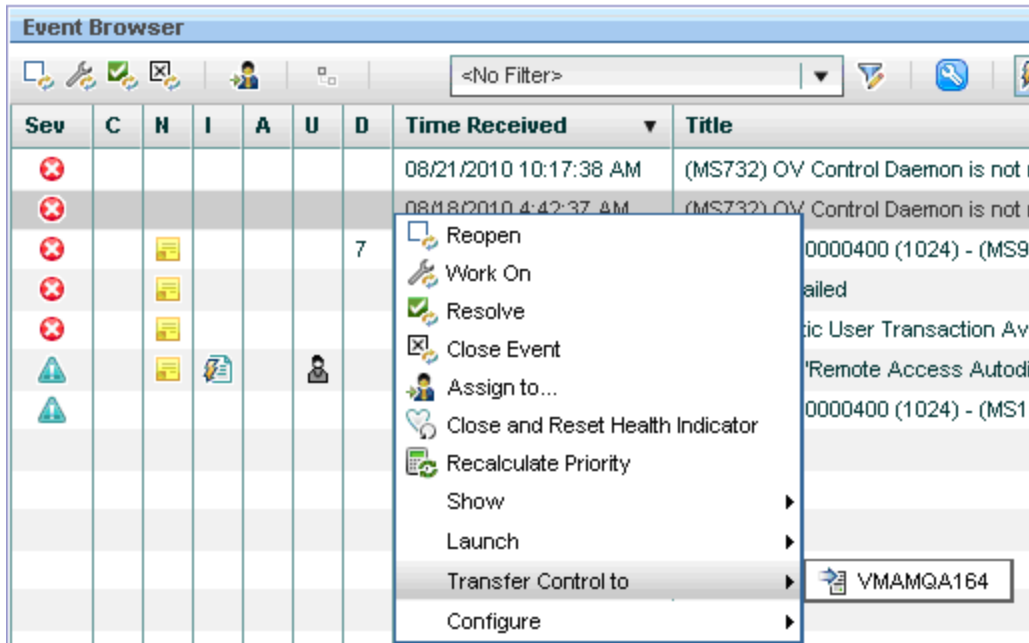
To verify the BSM – SM configuration:

1. Create a new event in BSM.

For example, use the event **submitEvents.bat** that resides in **<BSM Install folder>\opr\support** on the event generator, **submitEvents.bat -s WARNING -t Testing -d "This is a testing event"**.

2. In the BSM user interface, navigate to **Applications > Operations Management** and locate the newly created event.

- Right-click the newly-created event and select **Transfer Control To= >{Display name for SM server}**.



- Double-click the event to show its details. The **Forwarding** tab shows details about the opened incident.

Note: Remember the Incident ID for the following steps.

- In the SM user interface, navigate to the **Incident Management** module and click the **Search Incidents** option.
- In the Search window, use the incident ID to find the incident from the previous step. The relevant incident is populated and the correct event data appears.

Chapter 5: BSM – SM Business Impact Report Integration

This chapter includes the following topics:

Overview	45
Access Business Impact Report via SM User Interface	45
Verify Business Impact Report Integration	47

Overview


HP Business Service Management (BSM) includes impact reports that you can use to help evaluate the impact of incidents on your business. A Business Impact Report (BIR) shows information about how a configuration item (CI) impacts the business services it belongs to. Data about the effect of Business Service, Application, and Business Process CIs includes KPI data, over-time data, and SLA data. For example, if the status for a host CI is critical, you can use the report to show the status of the Business Service CIs to which the host CI is attached.

When deployed as part of the BSM solution, Incident Management users can launch an impact report from an incident in context with the incident's affected CI. Service Desk Agents can validate the updated status of the business impact to categorize and prioritize the incident.

Access Business Impact Report via SM User Interface

To use the BSM Business Impact Report integration, you must add and enable an instance of this integration in Integration Manager.

To add a BSM Business Impact Report integration instance:

1. Log on to the HP Service Manager (SM) management console with a System Administrator account.
2. Navigate to **Tailoring > Integration Manager**. The Integration Instance Manager window opens.
3. Click the **Add**  button. The Integration **Template Selection** wizard opens.

4. Select **SMBIR** from the Integration Template list.

Note:

- Do not select the **Import Mapping** check box.
- Only one instance of the BSM Business Impact Report integration is allowed. If an instance of this integration already exists in Integration Manager, the SMBIR template becomes unavailable.

5. Click **Next**. The Integration Instance Information pane appears.
6. Update the following fields:

Note: Only **Name** and **Version** are required fields. This integration does not use the **Interval Time(s)** and **Max Retry Times** fields as it is based on the user interface.

Name	Recommended Value	Description
Name (required)	<user defined>	Name of the integration instance (default: SMBIR).
Version (required)	<user defined>	Version of the integration template (default: 1.0).
SM Server	<SM server name>	Display name of the SM server machine.
Endpoint Server	<BSM server name>	Display name of the BSM server machine.
Run at system startup	Select	Select this check box if you want this instance to be automatically enabled when the SM server starts.

7. Click **Next**. The Integration Instance Parameters pane appears.
8. On the **General Parameters** tab, replace **BSM_host** in the **baseurl** parameter with the host name of the BSM Gateway server.
9. Click **Next** twice.

Note: Leave the Integration Instance fields and Integration Instance Mapping panes.

10. Click **Finish** to exit the wizard.

11. Click **Control +** and the line of the new integration you created.
12. Click the **Enable** link.
13. Click **Yes**.

Verify Business Impact Report Integration

The BSM and SM integration enables launching the BSM Business Impact Report directly from the SM web user interface.

To verify the integration is working:

1. In SM, there should already be an incident opened from a BSM event. (For details, see ["Verify BSM to SM Configuration" on page 43.](#))
2. In the Incident Details window, click the **More** button and select **Launch Business Impact Report**. The BSM logon window opens.

Note: This does not happen if LWSSO is already configured on both systems and the same currently logged in user exists in both.

3. Enter the BSM logon details to log on to BSM. A BSM Business Impact Report appears in the context of the relevant CI (affected CI in the Incident record).
4. A BSM Business Impact Report also appears when you right-click the corresponding event in the Operations Management console and select **Show= > "Business Service Impact for Related CI"**.

Chapter 6: UCMDB – SM Integration Configuration

This chapter includes the following topics:

Overview	48
Set Up UCMDB for Integration with SM Using ServiceManagerAdapter9-x	48
Set Up SM for Integration with UCMDB	51
Verify UCMDB – SM Integration	53
Set Up UCMDB for Integration with SM Using ServiceManagerAdapter7-1	54
Set Up SM for Integration with UCMDB	58
Verify UCMDB – SM Integration	58

Overview

This section 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.

Beginning with UCMDB version 9.05, a new SM adapter is supplied with UCMDB out of the box (also known as ServiceManagerAdapter9-x, which is an enhancement of ServiceManagerAdapter7-1). Even though ServiceManagerAdapter9-x is the more recommended adapter, the legacy ServiceManagerAdapter7-1 adapter is also supported, although it will not provide the same out-of-the-box content as the newer adapter.

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	49
Configure SM Adapter in UCMDB	49
Create a New Integration Point	49
Set Up the Data Push Job	50

Run the Data Push Jobs	51
------------------------------	----


Prerequisites

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

Configure 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

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.
Adapter	<user defined>	Select the appropriate adapter for the version of SM that you are using.

Name	Recommended Value	Description
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>	<p>If SM credentials appear in the Credentials column, select them.</p> <p>If no SM credentials appear, select Generic Protocol and click the Add new connection details for selected protocol type  button.</p> <p>Enter the following information:</p> <p>Description. Enter Service Manager.</p> <p>User Name. Enter the SM user name. The default value is falcon.</p> <p>User Password. Enter and confirm a password.</p>
Probe Name	<user defined>	The probe is selected from a drop-down list. This is the same probe that is being used for the UCMDB – BSM integration.

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

- 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 **Synchronize All**  to run the push job.
- 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.

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	51
Add the UCMDB Connection Information to the System Information Record	51

Prerequisites

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

Add the UCMDB Connection Information to the System Information Record

- 1. Log on to your Service Manager system as an administrator.
- 2. Navigate to **System Administration > Base System Configuration > Miscellaneous > System Information Record**.


3. Select the **Active Integrations** tab.
4. Select the **HP Universal CMDB** option. The form appears in 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

1. Browse to your UCMDB server.
2. Navigate to **Managers > Modeling > CI Type Manager**.
3. Under **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.

Set Up UCMDB for Integration with SM Using ServiceManagerAdapter7-1

This task lists the steps necessary to configure UCMDB in order to perform the integration with SM using ServiceManagerAdapter7-1.

This task includes the following steps:

Prerequisites	54
Configure SM Adapter in UCMDB	54
Create a New Integration Point	54
Set Up the RMI Job	56
Set Up the Changes Job	56
Run the Data Push Jobs	56

Prerequisites

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

Configure 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 **ServiceManager Adapter7-1** and expand it.
5. Expand the **configuration files** item.
6. Select **ServiceManagerAdapter7-1/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

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.
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>	<p>If SM credentials appear in the Credentials column, select them.</p> <p>If no SM credentials appear, select Generic Protocol and click the Add new connection details for selected protocol type  button.</p> <p>Enter the following information:</p> <p>Description. Enter Service Manager.</p> <p>User Name. Enter the SM user name. The default value is falcon.</p> <p>User Password. Enter and confirm a password.</p>

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

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

Set Up the RMI Job

To replicate the relations from UCMDB to SM:

1. Edit the **SM Topology Comparison Push** job.
2. Select **Scheduler Definition**.
3. For the **Repeat** field, select **interval**.
4. Set the **Repeat Every** field to **1 Day**.
5. Click **OK**.

Set Up the Changes Job


To replicate CIs from UCMDB to SM:

1. Edit the **SM History-based Push** job.
2. Select **Scheduler Definition**.
3. For the **Repeat** field, select **interval**.
4. Set the **Repeat Every** field to **1 Day**.
5. Click **OK**.

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 **Synchronize All**  to run the replication job.
4. When the Confirm synchronizing window appears, click **Yes**.
5. Click the **Statistics** tab to view the progress of the synchronization.

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

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

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	58
Add the UCMDB Connection Information to the System Information Record	58

Prerequisites

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

Add the UCMDB Connection Information to the System Information Record

1. Log on to your Service Manager system as an administrator.
2. Navigate to **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
3. Select the **Active Integrations** tab.
4. Select the **HP Universal CMDB** option. The form appears in the UCMDB Web service URL field.
5. In the UCMDB Web service URL field, enter the URL to the HP Universal CMDB Web service API.


The URL has the following format:

http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService

6. In the UserId dialog box, enter your UCMDB user name and password and click **Save**.

Verify UCMDB – SM Integration

1. Browse to your UCMDB server.
2. Navigate to **Managers > Modeling > CI Type Manager**.
3. Under **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 7: UCMDB – BSM Integration Configuration

This chapter includes the following topics:

Overview	60
Create UCMDB to BSM Integration Point in BSM	60
Configure BSM 9.x Integration Point	63
Verify UCMDB – BSM Configuration	67

Overview


This configuration synchronizes the configuration item (CI) records between HP Universal CMDB (UCMDB) and Run-Time Service Model (RTSM). Apart from the convenience synchronizing the configuration between UCMDB and RTSM provides, we make sure that the CIs across all three systems (UCMDB, HP Service Manager (SM), and HP Business Service Management (BSM)) are identical and have the same GlobalID generated by UCMDB.

Create UCMDB to BSM Integration Point in BSM

This task includes the following steps:

Deploy Package CMS_to_RTSM_Sync.zip on UCMDB	60
Enable the CMDB 9.x Integration Point	61

Deploy Package CMS_to_RTSM_Sync.zip on UCMDB


1. Copy the file CMS_to_RTSM_Sync.zip located on the BSM-DPS machine file system under **HPBSM\odb\confactory_packages** to the file system on the UCMDB machine.
2. Open the UCMDB user interface.
3. Select the **Administration** tab.
4. Select **Package Manager**.
5. Select **Deploy Packages to server (from local disk)**.
6. Click the **Add**  button and select the file **CMS_to_RTSM_Sync.zip** through the file system



browser.

7. Select **Deploy**.

Enable the CMDB 9.x Integration Point

1. Open the BSM admin user interface and select the **RTSM Administration**.
2. Select the **Data Flow Management** tab.
3. Select **Integration Studio**.
4. Create a new **Integration Point** according to the following table:

Name	Recommended Value	Description
Integration Name	<user defined>	The name you give to the integration point.
Adapter	UCMDB 9.x	Select the adapter type from the drop-down list.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the UCMDB server.
Port	<user defined>	The port through which you access UCMDB.
Credentials	<user defined>	<p>If UCMDB credentials appear in the Credentials column, select them.</p> <p>If no UCMDB credentials appear, select Generic Protocol and click the Add new connection details for selected protocol type  button.</p> <p>Enter the following information:</p> <ul style="list-style-type: none"> ■ Description. Enter UCMDB. ■ User Name. Enter the UCMDB user name. The default value is admin. ■ User Password. Enter and confirm a password.
Probe Name	<user defined>	Select the probe you configured previously from the drop-down list.


5. Click the **Add**  button on the right side of the window and add Job definitions as follows:
 - a. Name the **Job definition**.
 - b. Select the **Allow Delete** check box.
 - c. Click the **Add**  button in the Job definition window.
 - d. From the pop up window, browse to **root - CMS sync** and select the **ActiveDirectory_sync** job and click **OK**.
 - e. Select the **Scheduler definition** check box.
 - f. In the Repeat window, select **Cron**.

Note: **Cron** refers to a Cron expression, which is a string composed of six or seven fields separated by white space. Six of the fields are mandatory, and one is optional.

For example, for the following expression: **0 15 10 * * ? 2011**, the task runs at 10:15 A.M. every day during the year 2011.

For more details, see the *UCMDB or BSM documentation*.

- g. For the Cron expression, enter the following string: *** 0/10 * * * ? ***.
- h. Adjust other settings as needed.
- i. When finished, click **OK** and save the integration.
- j. Repeat steps **a** to **i** and configure the following jobs:
 - **FailoverCluster_Sync**
 - **IIS_Sync**
 - **SOA_Sync**
 - **BusinessAndFacilities_Sync**
 - **ExchangeServer_Sync**
 - **Virtualization_Sync**
 - **Siebel_Sync**
 - **Credentials_Sync**
 - **Basicinfrastructure_Sync**

- **J2EE_Sync**
 - **SAP_Sync**
6. Browse to UCMDB on port 8080 (for example, <http://yourUCMDBhost.domain:8080>), and select the **JMX Console**.
 7. Log on to the JMX console.
 8. From the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.
 9. Invoke:
 - a. **setAsGlobalIdGenerator** and verify it succeeded.
 - b. **getGlobalIdGeneratorScopes** and verify it succeeded.
 10. Browse to your BSM administration user interface.
 11. Select the **Data Flow Management** tab.
 12. Select **Integration Studio** from the options.
 13. Select the **Integration Point** that you have configured.
 14. In the Job definition section, click **Synchronize All**  to run the synchronization.

The Integration Point should be active and the jobs appear properly.


Configure BSM 9.x Integration Point

This task includes the following steps:

Deploy Package CSM_to_RTSM_Sync.zip on BSM	63
Enable the CMDB 9.x Integration Point	64

Deploy Package CSM_to_RTSM_Sync.zip on BSM

1. Copy the file CSM_to_RTSM_Sync.zip located on the BSM-DPS machine file system under **HPBSM\odb\confactory_packages** to the file system on the BSM machine.
2. Open the BSM user interface.
3. Navigate to **Admin > RTSM Administration > Administration > Package Manager**.
4. Select **Deploy Packages to server (from local disk)**.


5. Click the **Add**  button and select the file **CMS_to_RTSM_Sync.zip** through the file system browser.
6. Click **Deploy**.



Enable the CMDB 9.x Integration Point

Note: Complete the following procedure in UCMDB version 9.0.

1. Open the UCMDB user interface.
2. Click the **Data Flow Management** tab.
3. Click **Integration Studio**.
4. Create a new **Integration Point** according to the following table:

Name	Recommended Value	Description
Integration Name	<user defined>	The name you give to the integration point.
Adapter	BSM Adapter	Select the adapter type from the drop-down list.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the BSM server.
Port	<user defined>	The port through which you access UCMDB.

Name	Recommended Value	Description
Credentials	<user defined>	<p>If UCMDB credentials appear in the Credentials column, select them.</p> <p>If no UCMDB credentials appear, select Generic Protocol and click the Add new connection details for selected protocol type  button.</p> <p>Enter the following information:</p> <ul style="list-style-type: none"> ■ Description. Enter UCMDB. ■ User Name. Enter the UCMDB user name. The default value is admin. ■ User Password. Enter and confirm a password.
Push Back IDs	Enabled	<p>Specifies whether to push back the global IDs after CIs are populated in the server.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: Relevant for UCMDB 9.x adapters.</p> </div>
Probe Name	<user defined>	Select the probe you configured previously from the drop-down list.

5. Click the **Add**  button on the right side of the window and add Job definitions as follows:
 - a. Name the **Job definition**.
 - b. Select the **Allow Delete** check box.
 - c. Click the **Add**  button in the Job definition window.
 - d. From the pop up window, browse to **root - CMS sync**, select the **ActiveDirectory_sync** job and click **OK**.
 - e. Select the **Scheduler definition** check box.

- f. In the Repeat window, select **Cron**.

Note: **Cron** refers to a Cron expression, which is a string composed of six or seven fields separated by white space. Six of the fields are mandatory, and one is optional.

For example, for the following expression: **0 15 10 * * ? 2011**, the task runs at 10:15 A.M. every day during the year 2011.

For more details, see the *UCMDB or BSM documentation*.

- g. For the Cron expression, enter the following string: *** 0/10 * * * ? ***.

- h. Adjust other settings as needed.

- i. When finished, click **OK** and save the integration.

- j. Repeat steps **a** to **i** and configure the following jobs:


- **FailoverCluster_Sync**
- **IIS_Sync**
- **SOA_Sync**
- **BusinessAndFacilities_Sync**
- **ExchangeServer_Sync**
- **Virtualization_Sync**
- **Siebel_Sync**
- **Credentials_Sync**
- **Basicinfrastructure_Sync**
- **J2EE_Sync**
- **SAP_Sync**

6. Browse to BSM on port 21212 (for example, <http://yourDPSHost.domain:21212>), and select the **JMX Console**.

Note: DPS represents the data processing server.

7. Log on to the JMX console.

8. From the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.

9. Invoke:
 - a. **setAsNonGlobalIdGenerator** for customer ID 1 and verify it succeeded.
 - b. **getGlobalIdGeneratorScopes** for customer ID 1 and verify it succeeded.
10. Browse to your UCMDB administration user interface.
11. Click the **Data Flow Management** tab.
12. Select **Integration Studio** from the options.
13. Select the integration point that you have configured.
14. In the Job definition section, click **Synchronize All**  to run the synchronization.

The integration point should be active and the jobs appear properly.

Verify UCMDB – BSM Configuration

1. Browse to your UCMDB server user interface.
2. In the CI Type manager window, locate the **Node** element.
3. Right-click a Node object and select **Show CIT Instances**. The CIT Instances window appears.
4. Right click on one of the CIs and select **Properties**.
5. Locate the Global ID and write down its value.
6. Browse to your BSM server user interface.
7. Repeat steps 2-4 and identify the value of **Global ID**.
8. Compare the IDs from steps 5 and 7 and verify that they are the same.

Chapter 8: Execute HP OO Flows from SM

This chapter includes the following topics:

Overview	68
Enable HP OO Flows from SM – KM Module	68

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. For more information, see the HP OO documentation.

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	68
Configure SSL on HP OO	70
Configure SSL on SM	74
Add an SMOO integration instance	75
Enable an Integration Instance	76
Configure LWSSO in HP OO	76

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 **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")
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

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\jre6\bin**.

5. Before you start configuring SSL in HP OO, make a backup copy of the following keystores:
 - <OO_HOME>\Central\conf\rc_keystore
 - <OO_HOME>\RAS\Java\Default\webapp\conf\ras_keystore.jks

- <OO_HOME>\Scheduler\conf\rc_keystore

- <OO_HOME>\Studio\conf\rc_keystore

6. Generate a private/public key pair for Root Certificate Authority.

a. Change to the following directory: %OO_home%\Central\conf

b. Run the following command:

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

c. When prompted, enter the phrase for cakey.pem: **bran507025**:

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

Examples of data to enter during the command execution follow:

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 rc_keystore -storepass  
bran507025-keypass bran507025 -dname "CN=<FQDN of OO server>, OU=SSG,  
O='HP Software', L=Yehud, ST=Israel,C=IL"
```

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

- b. Run the following command:

```
keytool -certreq -keystore rc_keystore -alias sm -storepass bran507025 -file req.crs
```

- c. Run the following command:

```
openssl x509 -req -days 1095 -in req.crs -CA mycacert.pem -CAkey cakey.pem -CAcreateserial -out smcert.pem
```

8. Import the root CA and self-signed certificate to rc_keystore.

- a. Run the following command:

```
keytool -import -v -alias rootca -keystore rc_keystore -storepass bran507025 -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 rc_keystore]

- c. Run the following command:

```
keytool -import -v -alias sm -keystore rc_keystore -storepass bran507025 -file smcert.pem
```

The following confirmation message appears:

Certificate reply was installed in keystore.

[Storing rc_keystore]

9. Configure SSL in HP OO RAS:

- a. Change to the following directory:

<OO_HOME>\RAS\Java\Default\webapp\conf.

- b. Copy the generated root CA **mycacert.pem** and self-signed certificate **smcert.pem** from **<OO_HOME>\Central\conf** to the current directory.
- c. Import the root CA **mycacert.pem** and self-signed certificate **smcert.pem** to **ras_keystore.jks** and run the following command:

```
keytool -import -v -alias rootca -keystore ras_keystore.jks -storepass  
bran507025 -file mycacert.pem
```

- d. Run the following command:

```
keytool -import -v -alias sm -keystore ras_keystore.jks -storepass  
bran507025 -file smcert.pem
```

10. Configure SSL in HP OO Scheduler:

Caution: If you install version 9.05 and have not previously installed version 9.04, the RSScheduler service is removed and unified with the RSCentral service.

- a. Change to the following directory: **<OO_HOME>\Scheduler\conf**.
- b. Copy the generated root CA **mycacert.pem** and self-signed certificate **smcert.pem** from **<OO_HOME>\Central\conf** to the current directory.
- c. Import the root CA **mycacert.pem** and self-signed certificate **smcert.pem** to **rc_keystore** and run the following command:

```
keytool -import -v -alias rootca -keystore rc_keystore -storepass  
bran507025 -file mycacert.pem
```

- d. Run the following command:

```
keytool -import -v -alias sm -keystore rc_keystore -storepass bran507025  
-file smcert.pem
```

11. Restart the **RSCentral** and **RSJRAS** services.

12. Configure SSL in HP OO Studio:

- a. Change to the following directory: **<OO_HOME>\Studio\conf**.
- b. Copy the generated root CA **mycacert.pem** and self-signed certificate **smcert.pem** from **<OO_HOME>\Central\conf** to the current directory.

- c. Import the root CA **mycacert.pem** and self-signed certificate **smcert.pem** to **rc_keystore** and run the following command:

```
keytool -import -v -alias rootca -keystore rc_keystore -storepass  
bran507025 -file mycacert.pem
```

- d. Run the following command:

```
keytool -import -v -alias sm -keystore rc_keystore -storepass bran507025  
-file smcert.pem
```

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\conf** to **%SM_home%/Server/RUN**.
 - c. Run the following command:

```
keytool -import -v -alias rootca -keystore smtrust -storepass bran507025  
-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 bran507025 -  
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:bran507025
```


2. Restart the SM server.

When using HP OO in High Availability (HA) mode, perform the following:

1. From the SM Server, export the certificate from the browser (Internet Explorer):
 - a. Browse to the HP OO load balancing URL (for example, **https://lbbto.devlab.ad:8444/PAS**).
 - b. Click **Continue to this website (not recommended)**.
 - c. Click the **Certificate Error** button and select **View certificates**.
 - d. Click the **Details** tab and then click **Copy to File...**
 - e. Click **Next**.
 - f. Select **DER encoded binary X.509** and click **Next**.
 - g. Enter the path and file name to where the certificate will be exported (for example, C:\oocert).
 - h. Click **Next** and then **Finish**.
2. Import the certificate to server keystore.

```
keytool - import -keystore smtrust -file "C:\oocert.cer" -alias oocert
```
3. Restart the SM server.

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

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

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

To configure LWSSO in SM, see ["Configure the SM Web Tier for LWSSO Support" on page 83](#).

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

To configure LWSSO in HP OO:

1. In %OO_HOME%\Central\WEB-INF\applicationContext.xml, enable the import between **LWSSO_SECTION_BEGIN** and **LWSSO_SECTION_END**.
2. In %OO_HOME%\Central\WEB-INF\web.xml, enable all the filters and mappings between **LWSSO_SECTION_BEGIN** and **LWSSO_SECTION_END**.
3. In %OO_HOME%\Central\conf\lwssofmconf.xml, enable LWSSO and edit the following two parameters:
 - **<domain>**. Domain name of the SM web tier server.
 - **initString**. Password used to connect HP products (minimum length: 12 characters)—for example, smintegrationlwssso. Make sure that this value is the same as that used in the LWSSO configurations of the other HP applications (such as your SM LWSSO configuration) that you want to connect via LWSSO.

For example:

```
<enableLWSSO
  enableLWSSOFramework="true"
  enableCookieCreation="true"
  cookieCreationType="LWSSO"/>
<webui>
  <validation>
    <in-ui-lwss>
      <lwssValidation id="ID000001">
        <domain>asia.hpqc.net</domain>
        <crypto cipherType="symmetricBlockCipher"
          engineName="AES" paddingModeName="CBC"      keySize="256"
encodingMode="Base64Url"
          initString="SMOOIntegration"></crypto>
      </lwssValidation>
    </in-ui-lwss>
  </validation>
  <creation>
    <lwssCreationRef id="ID000002">
      <lwssValidationRef refid="ID000001"/>
      <expirationPeriod>600000</expirationPeriod>
    </lwssCreationRef>
  </creation>
</webui>
```

4. Restart the HP OO services.

Chapter 9: Execute HP OO Flows from BSM

This chapter includes the following topics:

Overview	79
Execute HP OO Flows from BSM User Interface	79

Note: All previous relevant integrations must be fulfilled prior to executing this integration.

Overview

HP Operations Orchestration (HP OO) provides a simple way for customers to run scripts for automatic actions. The integration with HP Business Service Management (BSM) utilizes the HP OO capabilities for building investigation tools or service remediation scripts, providing the operators with a simple way to validate a problem, investigate it, or automatically correct it. A run book can be executed manually.

Execute HP OO Flows from BSM User Interface

This task describes the working order required to integrate BSM and HP OO.

Configure the Link Between BSM and HP OO	79
Import HP OO Server Certificates to BSM	80
Permissions	81

Configure the Link Between BSM and HP OO

To configure the integration between BSM and HP OO:

1. In BSM, navigate to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Integrations with other applications**.
4. In the **HP Operations Orchestration** table, locate the HP OO application URL. Modify the setting for the URL used to access the HP OO application—for example, **https://<qualified server name>:8443**.
5. In the same table, enter the user logon name used when invoking run books in an automatic way. The user name must also be defined in HP OO.

Import HP OO Server Certificates to BSM

Import the server certificate from the HP OO server to the BSM gateway server so that the two systems can communicate with each other securely.

To export server certificates from HP OO and import them into BSM in a Windows environment, use the keytool utility that is included in Sun JRE to export and import certificates.

1. Export the **OO Server Certificate**. On the HP OO server, enter:

```
C:\> "%JAVA_HOME%\jre\bin\keytool" -keystore "%ICONCLUDE_
HOME%\Central\conf\rc_keystore" -export -alias sm -file "C:\<Operations
Orchestration server fully qualified host name>.cer"
```

Note:

- If your %JAVA_HOME% environment variable points to the JRE directory instead of the JDK directory, remove jre from the keystore path (C:\> "%JAVA_HOME%\bin\keytool" -keystore) in the command.
- Default keystore password in HP OO is **bran507025**.

If using HP OO in High Availability (HA) mode:

From the BSM Server, export the certificate from the browser (Internet Explorer):

- a. Browse to the HP OO load balancing URL (for example, **https://lbbto.devlab.ad:8444/PAS**).
- b. Click **Continue to this website (not recommended)**.
- c. Click the **Certificate Error** button and select **View certificates**.
- d. Click the **Details** tab and then click **Copy to File....**
- e. Click **Next**.
- f. Select **DER encoded binary X.509** and click **Next**.
- g. Enter the path and file name to where the certificate will be exported (for example, C:\loocert).
- h. Click **Next** and then **Finish**.

2. To import the server certificate you exported from HP OO to the BSM cacerts keystores, copy the ***.cer** file you have just created to **c:** on the BSM gateway and execute:

```
C:\> "%TOPAZ_HOME%\jre\bin\keytool" -keystore  
"%TOPAZ_HOME%\JRE\lib\security\cacerts" -import -alias  
"<Operations Orchestration fully qualified host name>" -file  
"<Operations Orchestration fully qualified host name>.cer"  
C:\> "%TOPAZ_HOME%\jre\bin\keytool" -keystore  
"%TOPAZ_HOME%\JRE64\lib\security\cacerts" -import -alias  
"<Operations Orchestration fully qualified host name>" -file  
"<Operations Orchestration fully qualified host name>.cer"
```

3. Restart BSM on the gateway server.

Note:

- If your **%TOPAZ_HOME%** environment variable points to the JRE directory instead of the JDK directory, remove jre from the keystore path (C:\> "%TOPAZ_HOME%\bin\keytool" -keystore) in the commands.
- Default keystore password in BSM is **changeit**.

Permissions

Grant permissions so that users can create, view, and modify the mapping between BSM CI types and HP OO run books, and invoke HP OO run books from BSM.

For details, see [Chapter 10, "HP Operations Orchestration Integration"](#) in *HP Business Service Management Solutions and Integrations*.

1. To integrate with HP OO, you must set up users with specific permissions. Navigate to **Admin > Platform > Users and Permissions**.
2. Select the user or create a new user.
3. Select **the Operations Orchestration Integration context**.

Note:

- Integration User in HP OO must have **HEADLESS_FLOWS** capability.
- It must be of type **External**.

Chapter 10: Security Settings Configuration

This chapter includes the following topics:

- Overview 82
- Configure the SM Web Tier for LWSSO Support83
- Configure LWSSO in BSM89
- Verify SM – HP OO Flow90
- Verify BSM – HP OO Run Book Invocation Integration91
- Configure LWSSO in UCMDB91
- Configure LWSSO in RC92

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 solution products.

Configure the SM Web Tier for LWSSO Support

To configure the 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 filter-
      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
      above 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-param>
```

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-param>
```

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.lwssso.LwSsoPreAuthent
icationFilter">
    <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.lwssso.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, `smintegrationlwssso`. 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 (for example, the Release Control server).

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"?>

<lwssso-config

xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwssso/2.0">

  <enableLWSSO

    enableLWSSOFramework="true"

    enableCookieCreation="true"

    cookieCreationType="LWSSO"/>

  <webui>
```

```
<validation>

  <in-ui-lwssso>

    <lwsssoValidation id="ID000001">

      <domain>example.com</domain>

      <crypto cipherType="symmetricBlockCipher" engineName="AES"
paddingModeName="CBC" keySize="256"

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

      </lwsssoValidation>

    </in-ui-lwssso>

    <validationPoint

      enabled="false"

      refid="ID000001"

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

    </validation>

    <creation>

      <lwsssoCreationRef useHTTPOnly="true" secureHTTPCookie="true">

        <lwsssoValidationRef refid="ID000001"/>

        <expirationPeriod>50</expirationPeriod>

      </lwsssoCreationRef>

    </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>
```

```
</multiDomain>

</webui>

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

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


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

<SM root directory>\RUN\lwssomconf.xml

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

Update this file as described in [step 4](#).

8. Restart the SM server.

Configure LWSSO in BSM

The OMi-SM integration requires LWSSO to be enabled in both SM and BSM so that users who have logged on to SM are allowed to sign on to BSM through the web tier without providing a user name and password.

To configure LWSSO in BSM:

1. Log on to BSM as a system administrator.
2. Navigate to **Admin > Platform > Users and Permissions > Authentication Management**.
3. Confirm that the following two fields are correctly configured:
 - a. **Token Creation Key (initString)**. Used to connect HP products (minimum length: 12 characters)—for example, smintegrationlwssso. 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 SM) that you want to connect via LWSSO.
 - b. **Trusted Hosts/Domains**. Must contain the domain name of the SM web tier server—for example, **domain.hp.com**.

If these two fields are correctly configured, LWSSO is already enabled in your BSM environment and you can ignore the following steps. If not, proceed with the following steps.

4. Click **Configure**. The **Authentication Management** wizard opens.
5. Click **Next**. The Single Sign-On Configuration pane appears.
6. Do the following:
 - a. In the **Token Creation Key (initString)** field, type a string of characters—for example, **I2VSVvV3EdCO**.

Note: This value must be the same as the `initString` value used in the LWSSO configurations of the other HP applications, such as your SM LWSSO configuration, that you want to connect via LWSSO.

- b. In the **Trusted Hosts/Domains** column, add the domain name of the SM web tier server.
 - c. In the **Type** column, select **DNS** for the SM web tier server.
7. Click **Next** twice, and then click **Finish**.

LWSSO is now enabled in your BSM environment.

Note: For settings not described above, keep the defaults. If you want to change these settings, click **Help** on the Single Sign-On configuration wizard pages.

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, open the SM web client and perform the following:

1. In the **Knowledge Management** module, **Published** documents, select any article.
2. Edit the article.

Note: Remember the article's name.

3. In the edit form, select the **OO Flow Links** tab.
4. Click the drop-down arrow and select any available flow.
5. Click the **Add Link** button.
6. Click the **Add** button again, and then click **Save** to save the record.
7. Click either the **Approve External** or **Approve Internal** buttons to approve the article.
8. Open a new incident.
9. Click the **More** button and select **Search Knowledge**.
10. Search for the title of the **Knowledge** article that you selected in [Step 2](#).

11. Open the article and click the **Execute OO Flow** button.
12. 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.

Verify BSM – HP OO Run Book Invocation Integration

To verify the BSM – HP OO run book invocation integration:

1. In the BSM user interface, navigate to **Admin > Integrations**, and select the **Operations Orchestration** tab.
2. Click the **Add Mapping** button, and map the existing HP OO flow to its CI type.
3. Using the **submitEvents.bat** utility (see ["Verify BSM to SM Configuration" on page 43](#)), create an event with a related type of CI that has mapping (for example, **Node**).
4. Right-click the event and select **Launch > Runbooks > <any available run book>**. The HP OO user interface opens in the context of the relevant run book which the user can execute.

Configure LWSSO in UCMDB

To configure LWSSO in UCMDB:

1. In the UCMDB user interface, navigate to **Administrator > Infrastructure Settings** in the **Configuration** tab, and select **Security**.
2. In the list, scroll down and fill in the following fields:

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



3. Click **Save**.
4. Restart the UCMDB.

Configure LWSSO in RC

To configure LWSSO in RC:

1. In RC user interface, navigate to **Module > Administrator > Configuration > Security**.
2. Click **HP Lightweight SSO (LWSSO)** and fill in the relevant details.

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

3. Click the **Save**  button.
4. Click the **Activate**  button to activate the adapter.
5. Restart the RC service after any change.
6. Create a RC user which has the same account and password as the one in Service Manager.

Chapter 11: UCMDB – RC Integration Configuration

This chapter includes the following topics:

Overview	93
Set Up UCMDB for Integration with RC	93
Set Up RC for Integration with UCMDB	94

Overview

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

Set Up UCMDB for Integration with RC

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

This task includes the following steps:

Prerequisites	93
Deploy the RC Integration Package	93

Prerequisites

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

Deploy the RC Integration Package


1. Copy the rc_package.zip file from

c:\hp\RC910\utilities\patchUpgrade\tempHome\uCmdb\ucmdb-90\extensions on the RC server to c:\hp\UCMDB\UCMDBServer\content\basic_packages on the UCMDB server.
2. Log on to UCMDB user interface from UCMDB server.
3. Navigate to **Administration > Package Manager**.

A list of installed packages appears in UCMDB.

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



The Deploy Packages to Server dialog box opens.

5. Click the **Add**  button and navigate to **c:\hp\UCMDB\UCMDBServer\content\basic_packages**.
6. Click the **rc_package.zip** package and click **Open**, then click **Deploy**.
7. When the installation is complete, a confirmation message appears. Click **OK**.

Set Up RC for Integration with UCMDB

1. In the RC user interface, navigate to **Module > Administrator > Configuration > Integrations > HP Universal CMDB**.

The HP Universal CMDB pane appears on the right.

2. In the HP Universal CMDB version box, click the appropriate version.
3. Navigate to **Integrations > HP Universal CMDB > Available Connections**.
4. Click your HP Universal CMDB server.
5. Enter a valid CMDB server name, port, user name, and password.
6. Click the **Save**  button.
7. In the Save As Draft dialog box, enter the adapter's draft name.
8. Click **Save**.
9. Click the **Activate**  button.

Chapter 12: SM – RC Integration Configuration

This chapter includes the following topics:

Overview	95
Set Up SM Integration with RC	95
Set Up RC for Integration with SM	96
Verify SM – RC Integration	99

Overview

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

- synchronize change data from SM to RC
- update a SM change record from within RC
- launch the RC Change Calendar and Change Assessment from within SM

Set Up SM Integration with RC

This task includes the following steps:

Prerequisites	95
Add RC Integration Instance	96


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

Prerequisites

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

- generated a database schema
- populated the Release Control database

Add RC Integration Instance

1. In Service Manager's System Navigator, navigate to **Tailoring > Integration Manager**.
2. Click the **Integration Instance Manager** tab.
3. Click **Add**  and select **SMtoRC**.
4. In the Integration Template Selection pane, click **Next**.
5. In the Integration Instance Information pane, select **Run at system startup** and click **Next**.
6. In the Integration Instance Parameters pane, click the **General Parameters** tab and enter the following information:

Name	Recommended Value	Description
rc.server.url	http://<user defined>:8080/ccm	Fully qualified domain name server address of RC
rc.adapter.name	<user defined>	Adapter name created in RC (without - adapter extension)
rc.username	<user defined>	RC user name
rcStandalone	true or false	Specified run mode of RC. If RC is connected to UCMDB, select false . If RC is not connected to UCMDB, select true .

7. Click the **Secure Parameters** tab. In the **Value** field, enter your RC password and click **Next**.
8. In the Integration Instance fields, click **Next**.
9. In the Integration Instance Mapping table, click **Finish**.
10. In the Integration Instance Manager pane, click **SMtoRC**.
11. Select the **Enable** check box to enable the integration.

Set Up RC for Integration with SM

Note:

- Verify Service Manager is up and running before continuing with this section.
- Text enclosed in angle brackets (for example, "<your_server_name>") indicates replaceable text.

1. Open a remote session with RC.
2. Navigate to **Start > Run > cmd**.
3. Run the command: **C:\hp\RC910\bin\SdiConfigurer.bat**. The SdiConfigurer.bat batch file asks questions about your system. Answer the questions as follows:

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

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

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

Enter **RC-SM Adapter**.

- Select Service Manager/Center version [9.30 and above].

Select **(6) 9.30 and above**.

- Enter Service Manager user name; for example, [<your user name>].

Enter your user name.

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

- Enter password; for example, [<SM user password>].

Enter your Service Manager user's password.

- Enter Service Manager timezone; for example, [<SM user timezone>].

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

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

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

- Enter Service Manager host name; for example, [<your SM host name in FQDN format>].

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

- Is https required in order to access wsd? [n]

Press **ENTER** for default.

- Enter Service Manager port [13080].




Press **ENTER** for default.

- Insert the url suffix for the wsd file [sc62server/PWS/].


Press **ENTER** for default.

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

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

4. In the RC user interface, navigate to **Module > Administrator > Configuration > Integrations > Service Desk Adapters**.
5. Click the **Add configuration to configuration set**  button and select **Service Desk Adapters**.
6. Navigate to **<HP Release Control installation directory>\bin\result** and open **<adapter_name>.zip**.
7. Click the adapter that you created in the previous step.
8. Click the **Save**  button.
9. Click the **Activate**  button to activate the adapter.
10. Log on to RC as an administrator.
11. Navigate to **Module > Administrator > Configuration > Server**.
12. Change the server name and server address to the server's FQDN.
13. Navigate to **Module > Administrator > Configuration > Security > HP LightweightSSO (LWSSO)**.
14. Correct the domain, initialization string, and protected domains.
15. Create an RC user which has the same account and password as the one in Service Manager.

Verify SM – RC Integration

1. In the Service Manager user interface, navigate to **Change Management > Changes > Open New Change**.
2. Enter all necessary information in the appropriate fields and click the **Save**  button.
3. Browse to your Release Control server. After 30 seconds, your change request appears in the calendar.

Chapter 13: SM – ALM/QC Integration

This chapter includes the following topics:

Overview	100
HP Application Lifecycle Management	101
HP Service Manager	106
HP ALM Synchronizer	114

Overview

One of the Detect to Correct (D2C) Value Stream requirements is an exchange (synch) between problems—usually achieved in HP Service Manager (SM) and HP Application Lifecycle Management/Quality Center (ALM/QC)—which creates a corresponding defect upon demand.

The tool for this linkage is SMQC—a bi-directional interface to exchange defects and requirements between HP Service Manager/Service Center (SM/SC) and HP Application Lifecycle Management/Quality Center (ALM/QC).

SMQC can handle three scenarios:

- SM/SC Change -> ALM/QC Defect,
- SM/SC Change -> ALM/QC Requirement, and
- SM/SC Problem <-> ALM/QC Defect.



When D2C is just focused on SM/SC Problem -> ALM/QC Defect, the full guide can be found at [HP Defects and Requirements Exchange with HP Service Manager/ServiceCenter and HP Quality Center/Application Lifecycle Management Installation and Administration Guide](#).

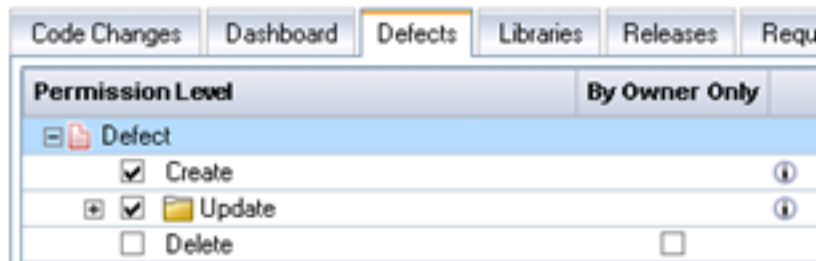
The integration should be configured in three system components:

1. ALM
2. SM
3. SMQC tool (Synchronizer)

HP Application Lifecycle Management

To configure the ALM side of the integration:

1. Log on as a project administrator, and open the **Tools > Customize** menu.
2. Create an Integration Account.
 - a. In the ALM console, select the **Project Users** tab. In the Project Users pane, click **Add User**. In the Add User dialog box, enter the User Name **SMQCIntUser** and click **OK**.
 - b. In the ALM console, select the **Groups and Permissions** tab. In the Groups and Permissions pane, click **New Group** . Create a new group called **SMIntegration** and set as **Viewer**.
 - c. Click the **SMQCIntUser > Membership** tab and  to add the **SMQCIntUser** integration user to the **SMIntegration** group.
 - d. In the **Groups and Permissions** pane, select the **SMIntegration > Permissions > Defects** tab, and select the **Defect > Create** and **Defect > Update** permission levels.




- e. In the **Groups and Permissions** pane, select the **SMIntegration > Permissions > Administration** tab, and select the following to manage favorites:

The screenshot shows the 'Administration' tab selected in the 'Groups and Permissions' pane. The 'Permission Level' section is expanded, and the following permissions are checked:

- ☒ Add Public Favorite View Folders
- ☒ Add Public Favorite Views
- ☐ Allow Major Changes
- ☒ Change User Properties & Password
- ☐ Clear History
- ☐ Configure Automail
- ☐ Customize Module Access
- ☐ Customize Project Entities
- ☐ Customize Project Lists
- ☐ Customize Report Templates
- ☐ Customize Requirement Types
- ☐ Customize Risk-Based Quality Management
- ☐ Customize Sprinter
- ☒ Delete Public Favorite view Folders
- ☒ Delete Public Favorite Views
- ☐ Manage Analysis Menus
- ☐ Manage Business Views
- ☒ Manage Private Favorite Views
- ☒ Manage Project Planning and Tracking
- ☒ Modify Public Favorite view Folders
- ☒ Modify Public Favorite Views
- ☐ Set Up Alert Rules
- ☐ Set Up Cross Project Customization
- ☐ Set Up Groups
- ☐ Set Up Project Users
- ☐ Set Up Workflow
- ☐ Undo Checkouts

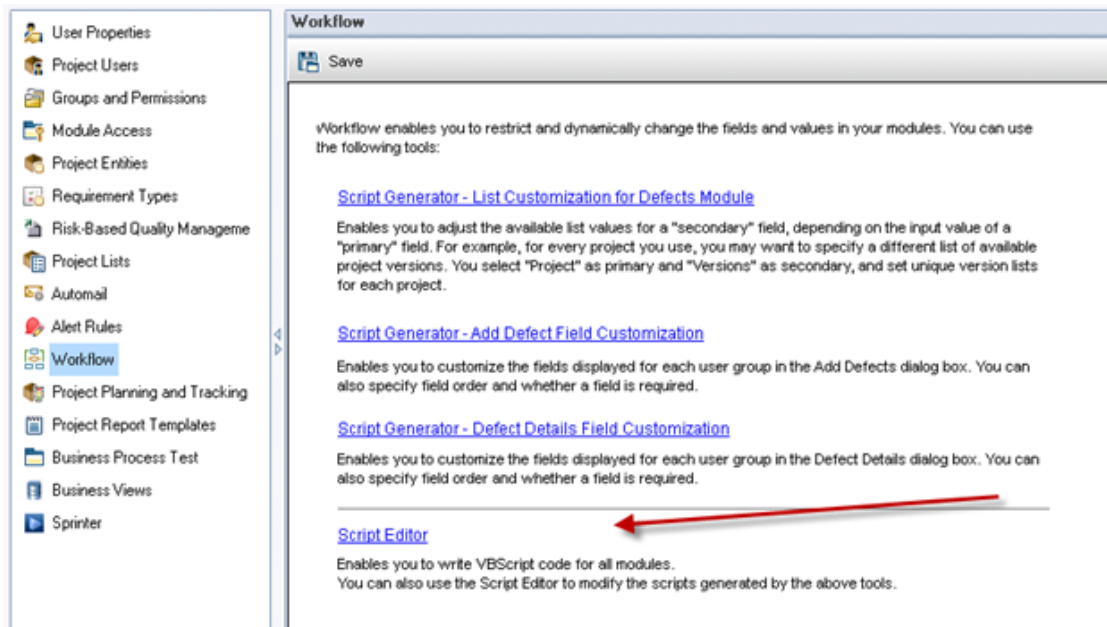
- f. When leaving the page, the **Confirm** dialog box appears. Click **Yes** to save the settings.

3. In the ALM console, select the **Project Entities** tab. In the Project Entities pane, select **Defect > User Fields**. Click  **New Field** to add the following fields:

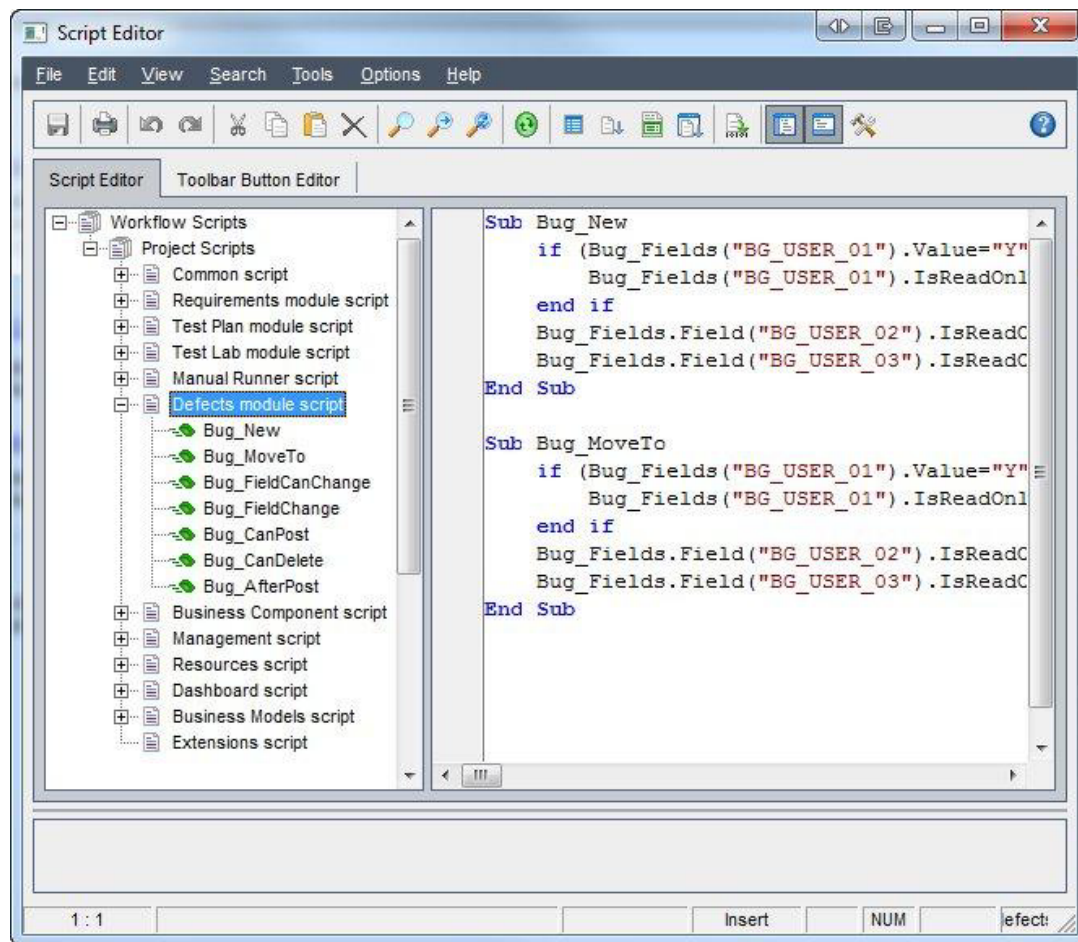
Field Label	Field Type	Length	Remarks
Synchronize with SM Problem	Lookup List/YesNo	255	Select Verify Value check box.
Problem ID	String	255	
Created from	String	255	

When leaving the page, the **Confirm** dialog box appears. Click **Yes** to save the settings.

4. In the ALM console, navigate to **Workflow > Script Editor**.



- Select the **Script Editor** tab.



- Navigate to **Defects module script > Bug_New** and paste the following sub-routines in the blank field.

```
if (Bug_Fields("BG_USER_XX").Value="Y") then
Bug_Fields("BG_USER_XX").IsReadOnly=True
end if

Bug_Fields.Field("BG_USER_XY").IsReadOnly=True
Bug_Fields.Field("BG_USER_XZ").IsReadOnly=True
```


- Navigate to **Defects module script > Bug_Moveto** and paste the following sub-routines in the blank field.

```
if (Bug_Fields("BG_USER_XX").Value="Y") then
Bug_Fields("BG_USER_XX").IsReadOnly=True
end if

Bug_Fields.Field("BG_USER_XY").IsReadOnly=True
Bug_Fields.Field("BG_USER_XZ").IsReadOnly=True
```

Note: Replace XX, XY, and XZ with:

- XX is the field name of the Synchronize with SM Problem field (first line in **Project Entities**).
- XY is the field name of the Problem ID field.
- XZ is the field name of the Created from field.

5. Log on to ALM with the integration account (**SMQCIntUser**).

6. In the **Defects** module, navigate to **View > Filter/Sort > Set Filter/Sort** .

Note: The purpose of this view is to let the ALM Synchronizer correctly filter those defects to be synchronized to SM as problems.

- a. Set **Synchronize with SM Problem** to **Y**.
- b. Add a view to **Favorites**:
 - **Name.** SMIntegrationView
 - **Location.** Private

7. Create a defect and set **Synchronize with SM Problem** to Y.

The screenshot shows the 'New Defect' window with the 'Details' tab selected. The 'Summary' section is empty. The 'Details' section contains the following fields:

Field	Value
Estimated Fix	
Planned Closure	
Problem ID	
Reproducible	Y
Subject	
Target Cycle	
Modified	
Priority	
Project	
Status	New
Synchronize	Y
Target Release	

A checkbox labeled 'Synchronize with SM Problem' is checked at the bottom right of the 'Details' section.

HP Service Manager

The HP Service Manager side of the SM – ALM integration is configured by following ["To configure the SM side of the integration without DEMO unls:" on page 108.](#)

Note: For the SM configuration, use the SM Java Client.

Caution: Back up your Service Manager database and customization before you begin to configure this integration.

Before you start, carefully read the following **Tip**.

Tip: The SMQC integration package includes DEMO configuration unls—**IntegrationAccount.unl** and **ProblemManagement.unl**—available from **SM QC Integration\out-of-box\unl\SM7.10\smqcintegration_vXX.exe**. These unl files contain a predefined configuration that may assist and save you some configuration time. Check the following table to understand the unl content in order to decide how suitable they are for your final configuration.

File Name	Description	Impact
IntegrationAccount.unl	Unload file for integration account	<p>Create.</p> <ol style="list-style-type: none"> 1. Contact SMQCINTEGRATION 2. Change Management profile CMPProfile_QCInt 3. Problem Management profile PMPProfile_QCInt 4. Operator SMQCIntUser (password: smcint) <p>Update. None</p> <p>Delete. None</p>
ProblemManagement.unl	Unload file for Problem Management	<p>Create.</p> <ol style="list-style-type: none"> 1. Sub form pm.qcint.subform 2. Global list SMQC Integration PM Project List (Demo) 3. External access definition QCIntProblemService with a BASIC/Demo configuration 4. Form control PM.pc.ident.and.class <p>Update.</p> <ol style="list-style-type: none"> 1. Form definition: PM.pc.ident.and.class 2. Db dictionary rootcause 3. PM.problem.investigation is NOT being updated. This needs to be done manually as described in step #8. <p>Delete. None</p>

For instructions on how to deploy unl, see ["Importing Unload Files into HP Service Manager"](#).

To configure the SM side of the integration without DEMO unls:

1. Create an SM integration account.
 - a. In the SM console, navigate to **System Administration > Base System Configuration > Contacts** and create a contact.
 - b. In the SM console, navigate to **System Administration > Ongoing Maintenance > Profiles > Problem Management Profiles** and create a profile record.

Tab	Field	Value	Memo
	Profile Name	PMProfile_QCInt	
Problems/Security/Rights	New	Yes	Check box
Problems/Security/Rights	Close	Yes	Check box
Problems/Security/Rights	Update	Always	
Problems/Security/Rights	Reopen	Yes	Check box

- c. In the SM console, navigate to **System Administration > Ongoing Maintenance > Operators>** and create an operator record.

Page	Field	Value
General	Logon Name	SMQCIntUser
General	Full Name	ALM integration default account
General	Contact ID	<i>The contact created in step 1a.</i>
General / Application Profiles	Problem Profile	PMProfile_QCInt
Security	Unlimited Sessions	Yes
Security	Password	<i>Your password</i>
Login Profile	Time Zone	Greenwich / Universal
Login Profile	Date Format	yy/mm/dd
Startup	Execute Capabilities	SOAP API
Startup	Execute Capabilities	ProbAdmin

- In the SM Client, navigate to **System Definition > Tables**. Add the following fields to the **rootcause** table:

Caution: The values shown are required. Do not change them.

Field	Type
qcintegration.type	Character
qcintegration.id	Number
qcintegration.project	Character
qcintegration. created.from	Character

- In the SM console, navigate to **Tailoring > Web Services > WSDL Configuration** and create a custom **External Access Definition** for **QCIntProblemService**.

Caution: The values shown are required. Do not change them.

- **Service Name.** QCIntProblemService
- **Name.** rootcause
- **Object Name.** QCIntProblem
- **Allowed Action/Action Name.** add / Create
- **Allow Action/Action Name.** save / Update

External Access Definition

Service Name:

QCIntProblemService

☐ Released

Name:

rootcause

☐ Deprecated

Object Name:

QCIntProblem

Allowed Actions

Expressions

Fields

Allowed Actions	Action Names	Action Type
add	Create	
save	Update	

4. Enable these fields in the web service:

Field	Caption	Type
id	ProblemID	StringType
sysmodtime	Modified	DateTimeType
qcintegration	QCEntityID	IntType
qcintegration.project	QCProject	StringType
qcintegration.type	QCIntegrationType	StringType
qcintegration.created.from	CreatedFrom	StringType
current.phase	CurrentPhase	StringType
category	WorkFlowType	StringType
subcategory	SubCategory	StringType
product.type	ProductType	StringType
problem.type	ProblemType	StringType
initial.impact	Impact	StringType
severity	Severity	StringType
description	Description	StringType
assignment	AssignmentGroup	StringType
ticket.owner	ProblemOwner	StringType
Open.time	Opened	DateTimeType

5. Define the following expressions for the web service.

```
cleanup($pm.activity);cleanup($rc.update);if same(update in $L.file, update
in $L.file.save) then ($L.need.to.update=true)
$rc.update=update in $L.file;if (dnull($rc.update)={}) then ($rc.update=
{"QC update sent"})
if ($L.need.to.update=true) then ($rc.update={"QC update sent"})
update in $L.file=update in $L.file.save
```

6. In the SM console, navigate to **Tailoring > Tailoring Tools > Global Lists** and create a global list with the following parameters:

Parameter	Value	Remarks
List Name	SMQC Integration PM Project List	
Regen Entry	1 00:00:00	
Build List on Startup?	Yes	Check box
List Variable	\$G.qcintegration.problem.project	Check box
User Defined List?	Yes	
Value List	{"server1/domain1/project1"}	Change to the values for your system Note: No spaces between slashes



Click **Add** to save this global list and, from the **Options** menu, click **Rebuild Global List**.

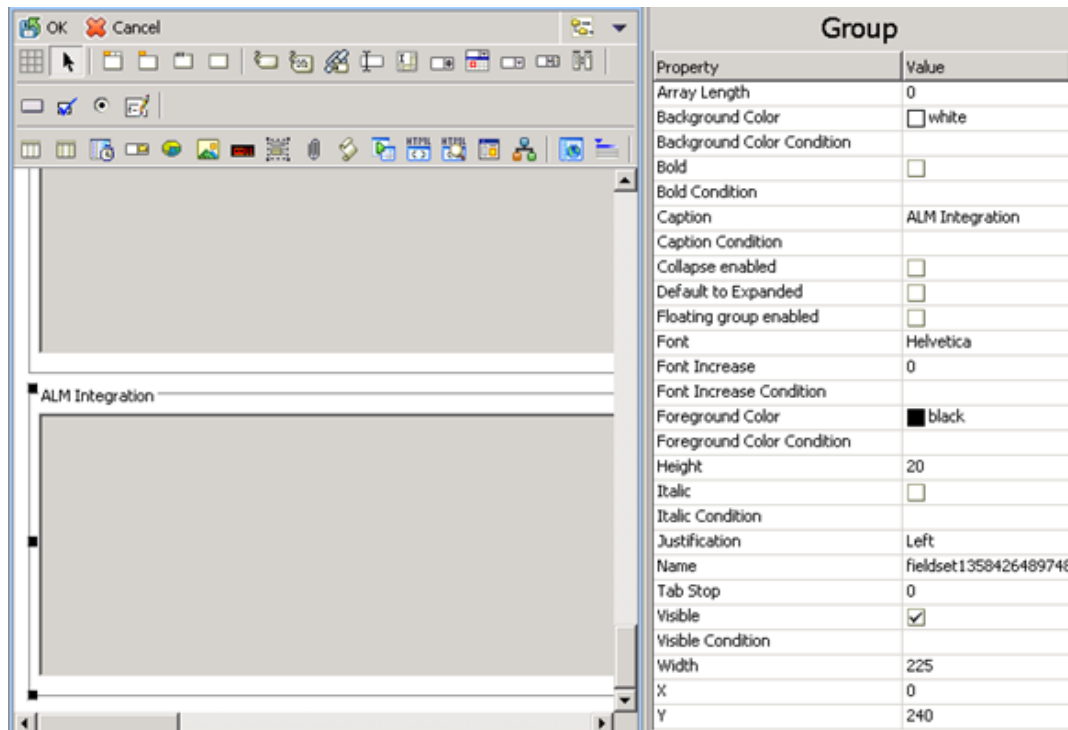
7. Using the SM client (not web tier), navigate to **Tailoring > Forms Designer** and, without using the Form Wizard, create a subform **pm.qcint.subform** with the following components:

Component	Properties
Label	Caption. Synchronize with QC:
Combo Box	Input. qcintegration.type Value List. 0;1; Display List. 0 - Not Synchronize;1 - Synchronize with ALM Defect Select Only. Yes Read-Only Condition. [\$qcint.type.readonly]
Label	Caption. Defect ID:
Text	Input. qcintegration.id Read-Only. Yes

Component	Properties
Label	Caption. Server/Domain/Project:
Combo Box	Input. qcintegration.project Value List. \$G.qcintegration.problem.project Read-Only Condition. [\$qcint.project.readonly] Mandatory Condition. [qcintegration.type]>0
Label	Caption. Created from:
Text	Input. qcintegration.project Read-Only. Yes

8. In the **Forms Designer**, open the default form of one **Problem Investigation and Diagnosis** phase (usually **PM.problem.investigation**).
 - a. Add a **Group** with the caption **ALM Integration**.
 - b. Add a **Subform** to the new tab with the format **pm.qcint.subform**.

- c. Save the changes.



9. From the **Options**  menu, select **Format Control**.

- a. Click **Calculations** and add two rows:

Display	Initial	Calculation
true	true	\$qcint.type.readonly=2;if (qcintegration.type in \$file~=0) then (\$qcint.type.readonly=1)
true	true	\$qcint.project.readonly=2;if (qcintegration.type in \$file~=0 and not null (qcintegration.project in \$file)) then (\$qcint.project.readonly=1)

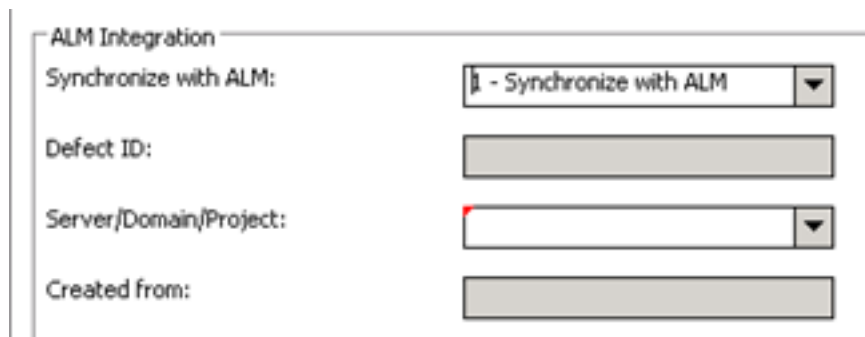
- b. Click **Validations** and add:

Parameter	Value
Validation	not null(qcintegration.project in \$file)
Message	The Server/Domain/Project is required.

Parameter	Value
Add	qcintegration.type in \$file~=0
Update	qcintegration.type in \$file~=0
Set Focus To	qcintegration.project

Save your changes.

10. Create a problem and select **1-Synchronize with QC Defect**.



HP ALM Synchronizer

To configure the **Synchronizer** side of the integration:

1. Download and install **HP ALM Synchronizer Server** from

<http://update.external.hp.com/qualitycenter/qc110/sync/almsynchronizer/HPALMSyncServer.zip>.

2. Download and install **HP ALM Synchronizer Client** from

<http://update.external.hp.com/qualitycenter/qc110/sync/almsynchronizer/HP-ALM-Sync-Client.msi>.

3. Register ALM client on the Synchronizer client machine by opening

http://<YourAlmServer>:8080/qcbin/start_a.jsp?common=true.

4. Download and install **HP Defects and Requirements Exchange** with SM and ALM from

http://update.external.hp.com/qualitycenter/qc110/sync/sm/smqc_integration_v1.02.exe.

5. Copy all files under the **[smqc-release-package]\adapter** directory to the **<QCS_Install_Dir>\adapters\lib** directory.

Adapters include:

- sm-adapter-XX.XX.XXX.jar

Note: XX.XX.XXX is the version number for the current release.

- sm-adapter-axis-1.4.jar
- sm-adapter-commons-discovery-0.2.jar
- sm-adapter-commons-lang-2.3.jar
- sm-adapter-jaxrpc-1.1.jar
- sm-adapter-jdom-1.1.jar
- sm-adapter-saaj-1.2.jar
- sm-adapter-wsdl4j-1.5.1.jar
- sm-adapter-commons-codec-1.3.jar
- sm-adapter-commons-httpclient-3.1.jar

6. Navigate to **Start > All Programs > HP Quality Server Synchronizer > Stop/Start Synchronizer** and restart the Synchronizer service.
7. Edit the following lines in **[release-package]\bin\build.properties** as required for access to Service Manager:

```
#Comment this line by this sign "#" if you do not generate stub jar for  
problem management module  
sm.problem.wsdl=http://service_manager_  
host:13080/sc62server/PWS/QCIntProblemService.wsdl
```

8. Run the **build.bat** script from the operating system's command prompt.

Note: Check the console output for errors.

The stub **[release-package]\build\sm-adapter-ws-client.jar** is generated.

9. Copy the stub to the **<Synchronizer_Client_Install_Dir>\adapters\lib** directory.

10. Navigate to **Start > All Programs > HP ALM Synchronizer** and click **Start Synchronizer**. The directory **<QCS_Install_Dir>\adapters\dat\SM ProblemManagement** appears after the synchronizer service is started. This can take up to one minute.
11. Copy the **[release-package]\sample\configuration_file_default.xml** file to **<QCS_Install_Dir>\adapters\dat\SM ProblemManagement**.
12. **configuration_file_default.xml** provides Problem field values to the SM adapter.

These values include:

- **Field name.** Caption of a field in the SM WSDL configuration form, such as Status, Priority
- **Field types.** String \ Number \ Date \ Single_Value_List \ Multi_Value_List
- **List types.** Array (multi-value list) \ Single-value list

One module should exist: `<itg:module name="problem"`

Note: See **[release-package]\sample\configuration_file_default.xml** in the synchronizer package as an example.

13. Open **HP ALM Synchronizer Client**, and click **Link > Create**.
 - a. Assign the general properties.
 - **Link Name.** defect (can be changed to any other meaningful name)
 - **Endpoint 2 type.** SM ProblemManagement

Click **Next**.

- b. Assign **HP-ALM** endpoint connection properties.

Create Link - Step 2 of 4 - HP-ALM Endpoint

Assign HP-ALM endpoint connection properties:

User name:

Password:

Parameter	Value
ServerURL	http://localhost:8080/qcbin
Domain	Default
Project	D2C

Enter the required information, and click **Next**.

- c. Assign **SM ProblemManagement** endpoint connection properties.

Create Link - Step 3 of 4 - SM ProblemManagement Endpoint

Assign SM ProblemManagement endpoint connection properties:

User name:

Password:

Parameter	Value
QC Project	localhost/Default/D2C
Configuration File Name	configuration_file_default.xml
Service URL	ic62server/PWS/QCIntProblemService.wsdl

Enter the required information, and click **Next**.

Configuration file name can be found in **<QCS_Install_Dir>\adapters \dat\SM ProblemManagement**.

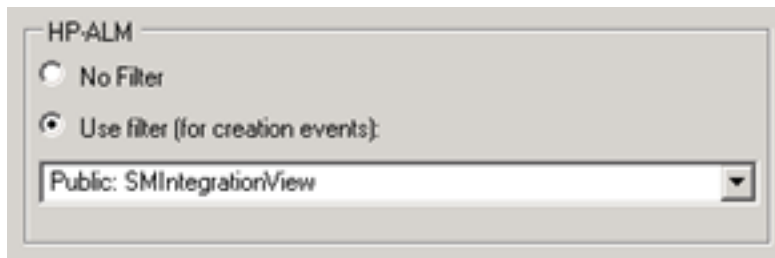
Service URL.**http://<service_manager_**
host>:<port>/sc62server/PWS/QCIntProblemService.wsdl

- d. Select entity types.

Select entity types. Problem by Defect


Note: This is the only available selection.

- e. In the **Filters** tab, select the **SMIntegrationView** filter for the QC endpoint.



- f. Define **Field Mappings**.

ALM	Direction	SM	Constant Value	Remarks
Problem ID	<-	ProblemID		Synchronize back on create: Yes
Defect ID	->	QCEntityID		Synchronize back on create: Yes
Synchronize with SM Problem			Y	
		QCIntegrationType	1	
Created from			Created from SM	
		CreatedFrom	Created from ALM	

ALM	Direction	SM	Constant Value	Remarks
		CurrentPhase	Valid phase name, such as Problem Investigation and Diagnosis	
		QCProject	YourServer/Domain/Project	
		WorkFlowType	Valid category name, such as ITIL	
Summary	<->	Description		
Severity	<->	Severity		Map Values: 
Detected on Date	<-	Opened		
		Impact	Select value	Mandatory field
		ProblemOwner	Select value	Mandatory field
		ProblemType	Select value	Mandatory field
		ProductType	Select value	Mandatory field
		Category	Select value	Mandatory field

- g. Verify all rules are as follows:

Rule	ALM	SM
Creation	Create a corresponding record in the other endpoint.	Create a corresponding record in the other endpoint.
Update	Update its corresponding record in the other endpoint.	Update its corresponding record in the other endpoint.
Deletion	Do nothing.	Do nothing.

The screenshot displays two side-by-side configuration panels. The left panel is titled 'HP-ALM' and the right panel is titled 'SM ProblemManagement'. Each panel contains three sections: 'Creation', 'Update', and 'Deletion (Full Synchronization Only)'. Each section has a title 'When a record is [action] in this endpoint...' followed by three radio button options. In the 'Creation' section, the first option 'Create a corresponding record in the other endpoint' is selected. In the 'Update' section, the first option 'Update its corresponding record in the other endpoint' is selected. In the 'Deletion' section, the first option 'Do nothing' is selected.

- h. Save the configuration.

Note: An integrity check is automatically run.

- i. Click **Enable Link**.
- j. Run **Full Synchronization**.

Part III: Appendix

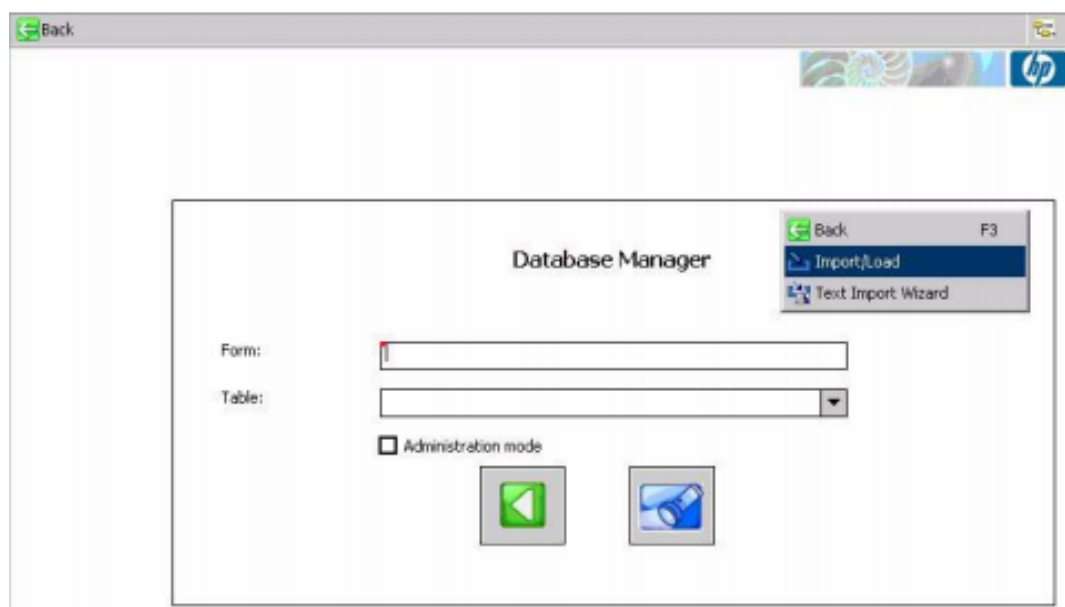
Appendix A: Importing Unload Files into HP Service Manager

This appendix contains:

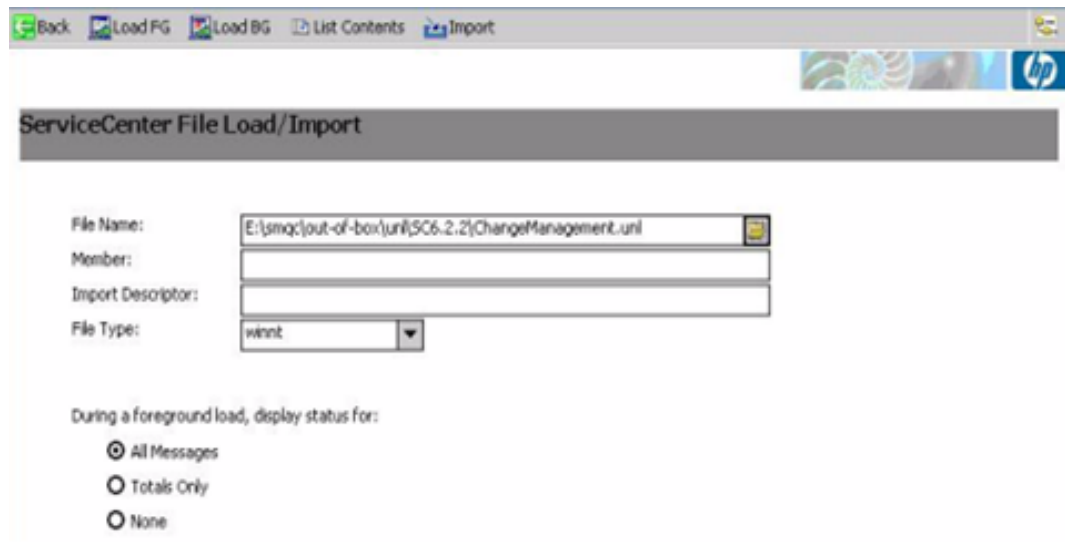
Importing Unload files into Service Manager	122
---	-----

Importing Unload files into Service Manager

1. Log on to **Service Manager/ServiceCenter** with an administrator account.
2. In the SM console, navigate to **Tailoring > Database Manager**.
 - a. Right-click the form and select **Import/Load**.



- b. In File Name field, use the file browser to select the file to load.



The screenshot shows the 'ServiceCenter File Load/Import' web interface. At the top, there is a navigation bar with buttons: 'Back', 'Load FG', 'Load BG', 'List Contents', and 'Import'. Below this is a header bar with the title 'ServiceCenter File Load/Import' and an HP logo. The main form contains the following fields:

- File Name:** A text field containing the path 'E:\smqc\out-of-box\unl\SC6.2.2\ChangeManagement.unl' and a file browser icon on the right.
- Member:** An empty text field.
- Import Descriptor:** An empty text field.
- File Type:** A dropdown menu with 'winnt' selected.

Below these fields, there is a section titled 'During a foreground load, display status for:' with three radio button options:

- ☒ All Messages
- ☐ Totals Only
- ☐ None

- c. In the Import Descriptor field, enter description text or not. Then, select the File Type: **winnt**.
- d. Select an option for the log display and click **LoadFG** to start loading.

Appendix B: Downtime Management

This chapter includes the following topics:

Downtime Management – Overview	124
Prerequisites	127
Downtime Management Solution Diagram	128
Integration Flow	129

Note:

- To configure Downtime Management, in addition to using this guide, see the relevant [CLIP Solution Guide](#).

Downtime Management – Overview

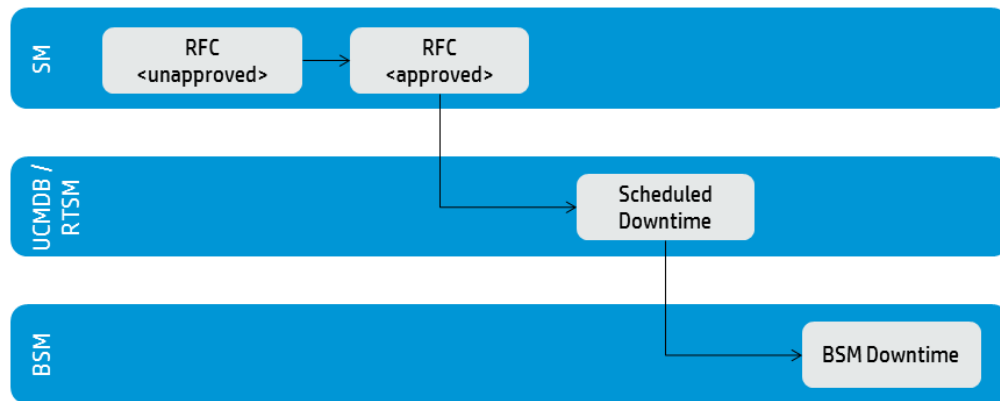
The downtime integration between HP Business Service Management (BSM) and HP Service Manager (SM) includes information exchanges in both of the following directions:

1. **SM > BSM.** When you create a downtime request for change (RFC) in SM, the RFC includes the configuration item (CI) that is under change and a start and end date/time for the downtime. If you do not want to waste time with false alarms in your operations center, and do not want to have these times included in service availability reports, you can set up the integration so that these RFCs are translated to downtimes in BSM.

In this scenario, you install and set up a downtime adapter on your CMS (whether you are working with a UCMDB central CMS or with RTSM). The RFC creates a planned downtime CI in the CMS, and the adapter translates the planned downtime CI to a downtime in BSM.

CLIP and Downtime Management – From SM

From approved RFC to suspended monitoring



1 © Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



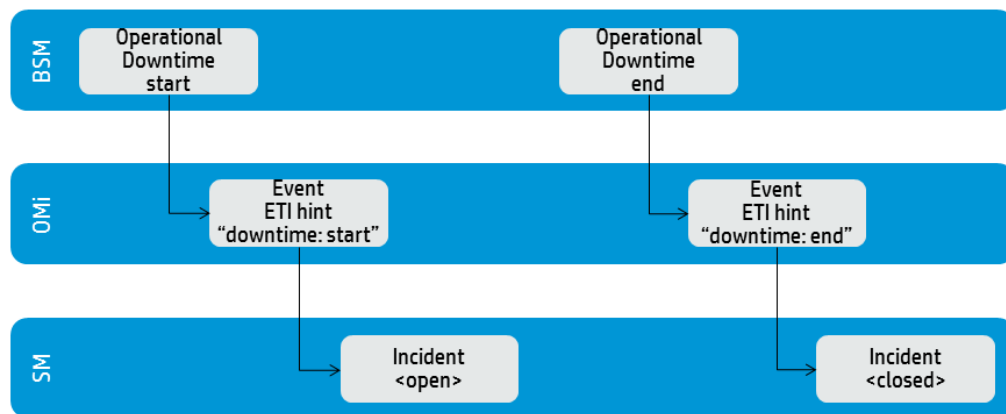
2. **BSM > SM.** When you define downtimes using BSM (for example every Monday and Saturday from 20:30-21:30), in order to proactively support end users, the help desk should be aware of such operational downtimes. After you set up the integration, downtimes in BSM are translated to events, which create corresponding incidents in SM.

In this scenario, when a downtime starts, BSM generates an event. Using the event forwarding mechanism, the event generates an incident in SM. When the downtime ends, an event is sent to close the downtime incident.

A single downtime can be defined on more than one CI. In the case of BSM > SM, a separate event is sent for each CI in the downtime.

CLIP and Downtime Management – from BSM

From Operational Downtime to Service Desk Awareness



1 © Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



Note:

- Following the initial integration, a large amount of data may be communicated from SM to BSM. We recommend that you perform the integration during off-hours to prevent negative impact on system performance.
- The integration consists of two parts: **SM > CMS/RTSM** and **CMS/RTSM > BSM**. You should configure both parts of the integration as one flow, without a significant time lag between setting up the two parts. If you set up the SM > CMS/RTSM part, and then wait a long time before setting up the CMS/RTSM > BSM adapter part, the number of downtimes communicated to BSM initially may be extremely high.

Prerequisites

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

- **HP Universal CMDB.** Server should be installed. Data flow probe should be connected and running (different server than BSM server).

Note: RTSM will function as UCMDDB when UCMDDB is not installed. For all references to UCMDDB, use RTSM instead.

- **HP Service Manager.** Server, Client, Help Server, Web Tier, and Knowledge Management should be installed and running.
- **HP Business Service Management.** Server, including the OMi application, should be installed and running.

BSM machine should have the DDM data flow probe connected and running.

- **HP Operations Orchestration.** Central and Studio should be installed and available for use.

Users and Permissions

The same user name must be used on all the products (they can have different passwords). For example, user **NocOperator1** must exist in both BSM and SM in order to drill down from OMi events into SM incidents. As well, the same user should exist in HP OO in order to execute HP OO run books on CIs.

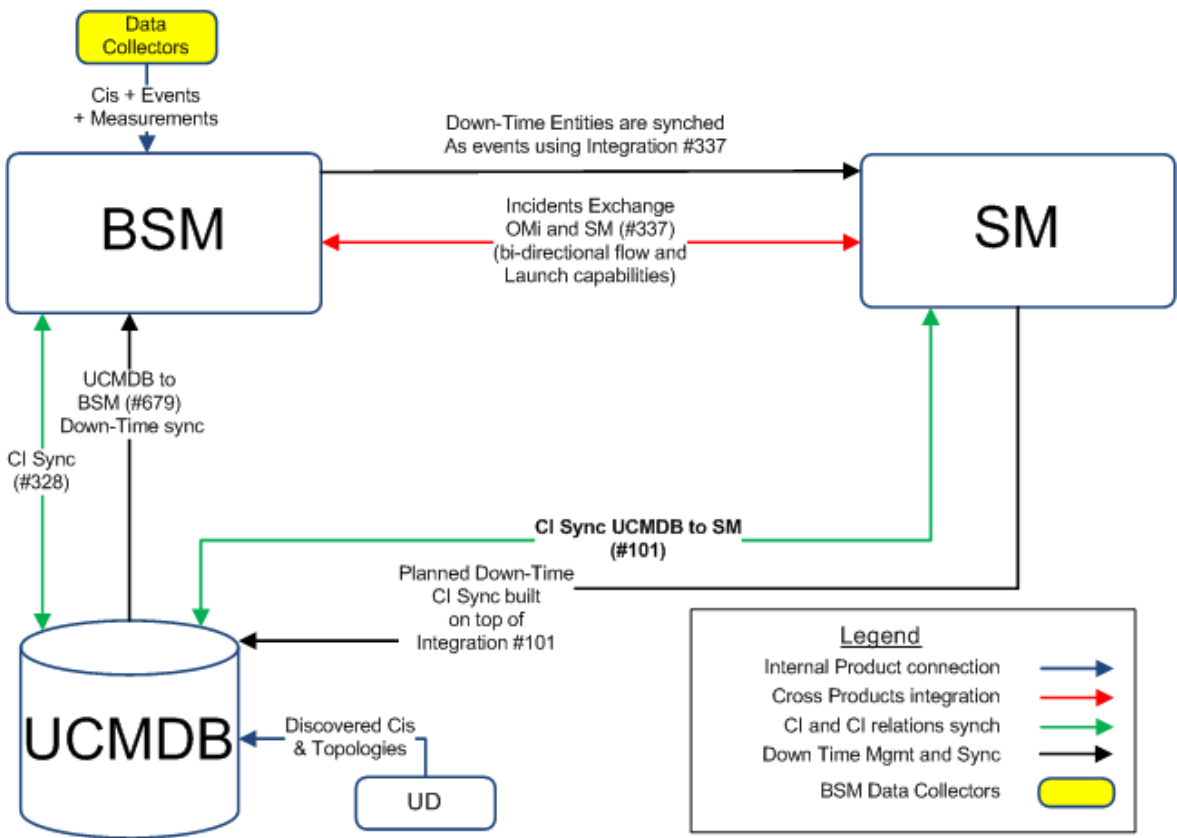
Global ID Generator

To enable the downtime integration, you must have a global ID generator configured in your UCMDDB and BSM environment.

The global ID generator configuration is described in the "UCMDDB – BSM Configuration" chapter of either the [CLIP with Runbook Automation Guide](#) or the [CLIP with Runbook Automation and Knowledge Management Guide](#).

Downtime Management Solution Diagram

The following diagram shows a typical deployment of the Downtime Management Solution.



ID#	Integration Name
#337	Incident Exchange (OMi–SM)
#101	CI sync and actual state federation (UCMDB to SM)
#328	UCMDB–BSM Platform (BAC) synchronization (UCMDB–BSM)
#679	UCMDB to BSM Downtime Integration (BSM–UCMDB)

Integration Flow

This section contains:

A. To create a SMIS SMBSM_DOWNTIME integration	129
B. To integrate SM RFC downtimes with UCMDB	131
C. To integrate SM downtimes with BSM (via UCMDB)	132
D. To send BSM downtime start/stop events ("Off" by default)	133

A. To create a SMIS SMBSM_DOWNTIME integration

1. Log on to the SM system as **System.Admin**.
2. Navigate to **Tailoring > Integration Manager > Add** to add SMIS configuration for SMBSM_DOWNTIME.
3. Select **SMBSM_DOWNTIME** for the Integration Template, and click **Next**.
4. Fill in the running frequency data in the **Interval Time(s)** field. Set this data based on your configuration item (CI) scheduled downtime data volume in the period.
5. Fill in the data for **Max Retry Times**.

Note: 0 is okay since we are not connecting to another system.

6. Fill in the data for the **Log File Directory**. By default, the log will be filed in sm.log.

Click **Next**.

Name, Interval Time, Max Retry Times and Log File Directory are required. If "Run at system startup" is checked, the integration instance will start automatically when SM starts.

Integration Instance Information	
Name: * SMBSM_DOWNTIME	Version: * 1.00
Interval Time (s): 10	Max Retry Times: 0
SM Server:	Endpoint Server:
Log Level: INFO	Category:
Log File Directory: c:\	<input type="checkbox"/> Run at system startup
Description: This is for managing CI downtime information between SM and BSM	

< Previous Next > Finish Cancel

Note: Be sure to select **Run at system startup**.

7. Configure the **SMIS** settings.

- a. Set a value for **WithdrawDowntime**.

When you are making a change using **Change Phase**, if the change has a **valid** outage, **true** means a prompt appears for you to choose to withdraw the outage.

- b. Set values for the **Change** category.

If you only want outage of one category of changes, after your desired phase has been approved, set the phase.

If your category workflow has multiple paths with different final approval phases, use a semicolon ";" to separate them.

In the **Category** column, set **Change** for change categories and **Task** for task categories.

- c. Set a value for **sm.host**. This value is the unique identifier for your SM deployment, which stands for the SM server.

Attention: No ":" in sm.host will break the logic.

- d. Set a value for **sm.reference.prefix**. This value is used to populate the External Process Reference of Scheduled Downtime CI in UCMDB. **Attention: No** must end with ":". SM will append ":" at the end automatically.

Integration Instance Parameters



All configurable parameters are listed here. If some parameters are secure, put them in Secure parameters tab.

General Parameters		Secure Parameters	
WithdrawDowntime	true	General	Set
Emergency Change	ECAB Approval	Change	Set
Normal Change	DCAB Approval	Change	Set
Hardware	Change Approval	Change	Set
Maintenance	Change Approval	Change	Set
Release Management	Verification	Change	Set
Software	Change Approval	Change	Set
Network	Change Approval	Change	Set
sm.host	sm931.testing.hp.com	General	Set
sm.reference.prefix	urn:x-hp:2009.sm	General	Set

- e. Click **Next**, **Next**, **Finish**.
- f. Select the **SMIS**.
- g. Click **Enable**.
- h. Click **Yes**.

B. To integrate SM RFC downtimes with UCMDB

Populate (sync) UCMDB with the downtime configuration items (CIs).

1. Log on to **UCMDB**.
2. In **Administration > Data Flow Management > Integration Studio**, verify the integration point in front of the SM exists and is active.
3. Click **Test connection** and verify success.
4. In the **Population** tab, add two additional integration jobs—one named **DT Population** based on **CLIP Downtime Population** TQL, and another named **DT Relationship** based on **CI To Downtime CI With Connection** TQL.
5. Log on to the SM server. Select the **Configuration Management** tab and navigate to **Resources > Configuration Item Relationships**.
6. Add a relation between the **Upstream** CI (for example, any business service instance) and the **Downstream** CI (the affected CI), and then click **Add**.
7. In the **Change Management** tab, open a new request for change (RFC). Verify the **Service**, **Affected CI**, and **Scheduled DownTime Start/End** are filled in.

Note: The **Service** and **Affected CI** values should be equal to the **Upstream/Downstream** CI values you put in the previous step.

8. Navigate to **More > Change Phase**. Move the RFC phase to the **Change Approval** phase.
9. Log on to **Service Manager** as user **Change.Approver**. Open the **Approval** In box and approve the change.
10. Wait for **SMBSM_DOWNTIME/DT Population/DT Relationship** to run.

Note: By default, it runs every minute.

11. Log on to **UCMDB**. In Modeling Studio, search for the **ScheduledDowntime** CI. A downtime CI is created with a relationship to the affected CI.

C. To integrate SM downtimes with BSM (via UCMDB)

1. To enable downtimes defined in SM to be sent to BSM, you must add an integration adapter to the UCMDB where downtimes are defined as follows:
 - a. From **C:\HPBSM\Adapters** in the BSM file system, copy **BSMDowntimeAdapter.zip** to the UCMDB's machine file system.
 - b. Within the UCMDB user interface, navigate to **Administration > Package Manager**.
 - c. Click **Deploy packages to server (from local disk)**.
 - d. Browse to the BSMDowntimeAdapter and click **Deploy**.
2. Create an integration point in front of BSM as follows:
 - a. Within the UCMDB user interface, navigate to **Data Flow Management > Integration Studio**.
 - b. Click **New integration point**, enter a name and description of your choice, and select **SM scheduled Downtime Integration**.
 - c. Enter the following information for the adapter: BSM Gateway hostname and port, the integration point credentials, communication protocol, and the context root (if you have a non-default context root).
 - d. Click **OK**, then click the **Save** button above the list of the integration points.
 - e. Click **Test Connection** and verify success.
3. Use the **Statistics** tab in the lower pane to track the number of downtimes that are created or updated. By default, the integration job runs every minute. If a job has failed, open the **Query Status** tab and double-click the failed job to see more details on the error.

If there is an authentication error, verify the BSM credentials entered for the integration point.

If you receive an unclear error message with code, this generally indicates a communication problem. Check the communication with BSM. If no communication problem is found, restart the MercuryAS process.

A failed job will be repeated until the problem is fixed.

D. To send BSM downtime start/stop events ("Off" by default)

To enable BSM to send downtime definitions to SM, you must edit a hidden infrastructure setting as described below. This procedure generates events in OMi. You can then use the event forwarding mechanism to generate incidents in SM when a downtime in BSM begins and ends.

1. Access the following location with your browser:

`http://<BSM hostname>:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=Foundations%3AService%3DInfrastructure+Settings+Manager`

2. In the **setGlobalSettingValue** method, define the parameter values as follows:

`contextName = downtime; settingName = downtime.event.send.enable; newValue = true`).

Click **Invoke**.

3. Restart BSM.

For details on how to use the event forwarding mechanism to generate incidents in SM, see the **Event Forwarding** section in BSM online help or in the *HP BSM Administration Guide*.