HPE Value Stream

Document Version: 2.2

Detect to Correct Concept and Configuration Guide

Document Release Date: August 2016

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hp.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Software Support site or click **Create an Account** 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 HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hp.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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 to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: https://softwaresupport.hp.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

Contents

Part I: Detect to Correct Concept Guide

Chapter 1: Detect to Correct Value Stream Concepts

This chapter includes:

Overview

The Detect to Correct (D2C) Value Stream provides a framework for the work of IT operations integrating Service Monitoring, Event, Incident, Problem, Change Control, Configuration Management, Service Remediation, and Service Level functions. It also provides a comprehensive overview of the business of IT operations and the services these teams deliver. Anchored by the Service Model, the D2C Value Stream delivers new levels of insight that help improve understanding of the inter-dependencies among the various operational domains; including Event, Incident, Problem, Change Control, and Configuration Management. It also provides the business context for operational requests and new requirements. The D2C Value Stream is designed to accommodate a variety of sourcing methodologies across services, technologies, and functions. This value stream understands the inter-relationships and inter-dependencies required to fix operational issues. It supports IT business objectives of greater agility, improved uptime, and lower cost per service.

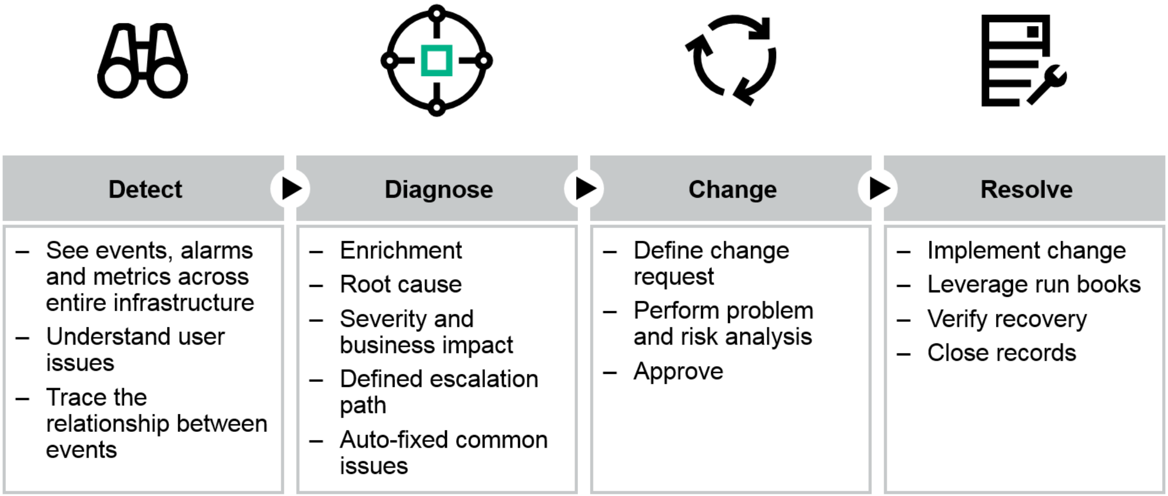
The D2C Value Stream provides a framework for bringing IT service operations functions together to enhance IT results and efficiencies. Data in each operation’s domain is generally not shared with other domains because they do not understand which key data objects to share and do not have a common language for sharing. When projects are created to solve this, it is often too difficult and cumbersome to finish or there is an internal technology or organization shift that invalidates the result.

The D2C Value Stream defines the functional components and the data that needs to flow between components that enhance a business and service-oriented approach to maintenance and facilitates data flow to the other value streams.

The key value propositions for adopting the D2C Value Stream are:

- Timely identification and prioritization of an issue
- Improved data sharing to accelerate ability to understand the business impact
- Automation both within domains and across domains
- Ensuring an operating model, capabilities, and processes that can handle the complexity of service delivery across multiple internal and external domains
- Effective linkage of Events to Incidents to Problems to Defects in the R2D Value Stream

Typical activities include:



Detect	Diagnose	Change	Resolve
– See events, alarms and metrics across entire infrastructure – Understand user issues – Trace the relationship between events	– Enrichment – Root cause – Severity and business impact – Defined escalation path – Auto-fixed common issues	– Define change request – Perform problem and risk analysis – Approve	– Implement change – Leverage run books – Verify recovery – Close records

To view the previous version of this guide, see the *Detect to Correct Concept and Configuration Guide Version 1.2* (https://softwaresupport.hpe.com/km/KM00439730).

Who Should Read This Guide

This guide is intended for:

- Presales personnel
- Professional Services architects and engineers
- Deployment engineers
- Quality automation engineers
- IT personnel

- Enterprise Architects on either the Hewlett Packard Enterprise or the customer side
- Anyone who wants to learn about the Detect to Correct-related best practices

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

HPE Software Support accesses the HPE Software Support website. 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 > HPE Software Support**. The URL for this website is www.hp.com/go/hpsoftwaresupport.

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

To find more information about access levels, go to:
http://h20230.www2.hp.com/new_access_levels.jsp

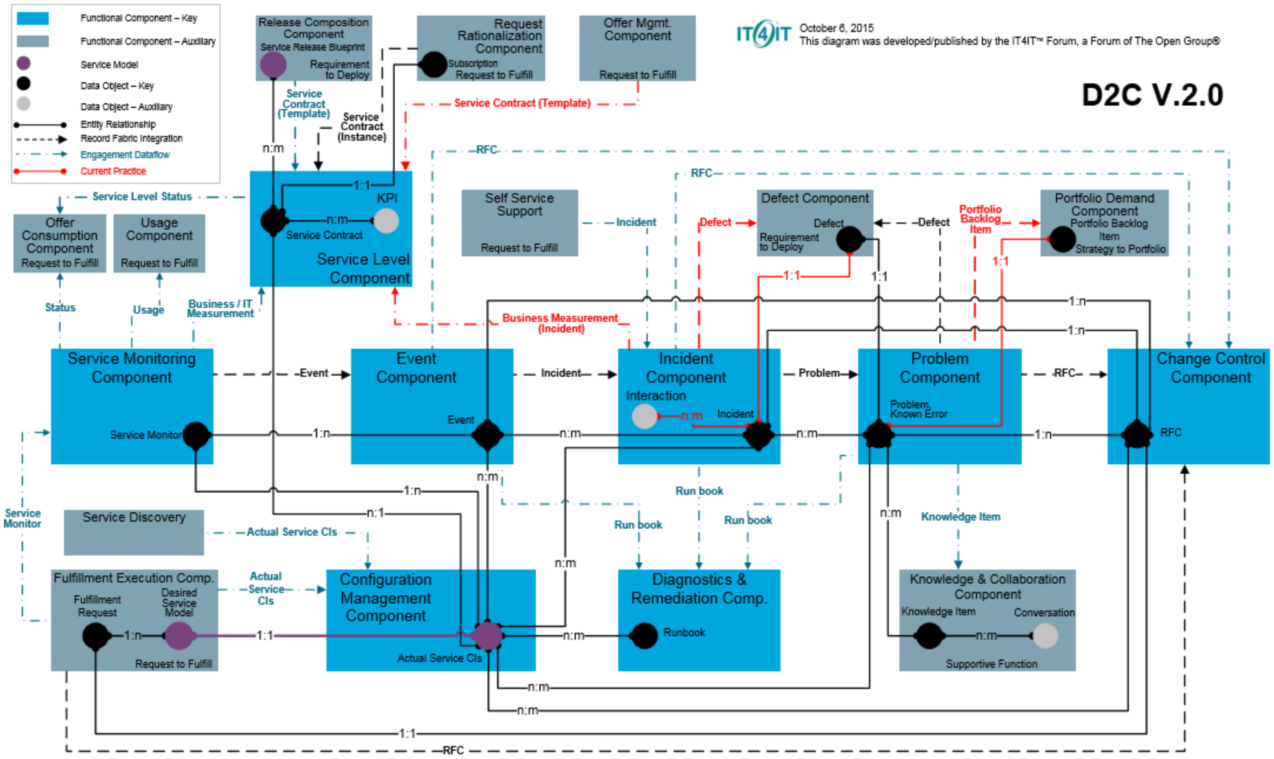
> To register for an HP Passport user ID, go to:
> http://h20229.www2.hp.com/passport-registration.html.

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

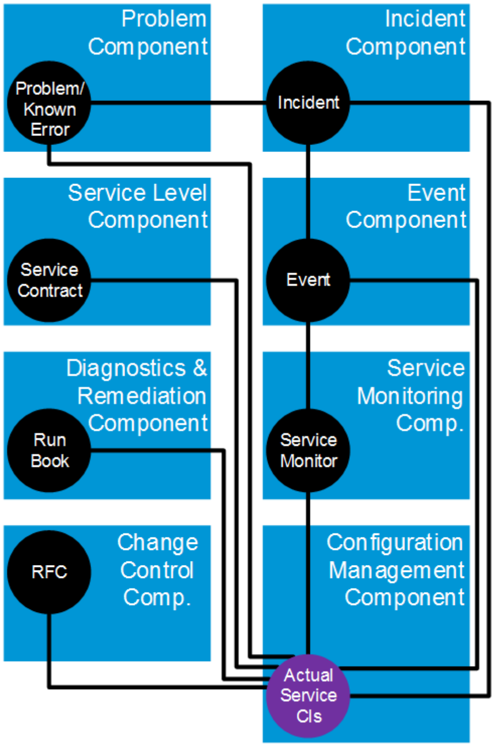
HPE Software Solutions Now accesses the HPESW Solution and Integration Portal Web site. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this Web site is https://softwaresupport.hpe.com/km/KM01702731.

Detect to Correct Value Stream Diagram

The following diagram illustrates the Functional Components and Data Objects that comprise the Detect to Correct Value Stream, as described in the IT4IT™ Reference Architecture.



Detect to Correct Functional Components



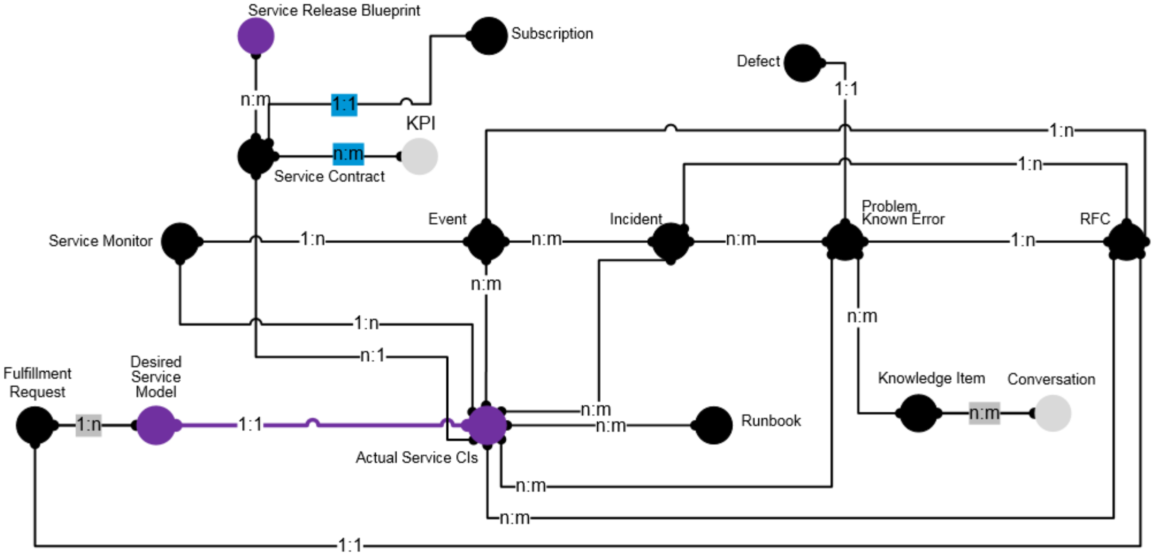
The functional components for this value stream are:

- **Service Monitoring Component.** In charge of creating, running, and managing monitors that measure all aspects/layers of a service, such as infrastructure (system and network), application, and security. It is also in charge of storing all measurement results and calculating compound measurements.
- **Service Level Component.** Enables the design and creation of Service Contracts (SLAs). It is responsible for the management of all Service Contract data objects throughout their life cycle, including the governance of the Service Contract Instances from the moment they are instantiated. This functional component is also responsible for collecting the relevant information in order to calculate the KPIs that are specified in the Service Contract and exposing data that reflects that actual performance against the defined Service Level Objectives.
- **Event Component.** Manages Events through the Event life cycle for Events that occur on any IT service. The Event life cycle includes but is not limited to detecting, categorizing, filtering, analyzing, correlating, logging, prioritizing, and closing the Event.

- **Incident Component.** Facilitates normal service operations restoration as quickly as possible and minimizes the impact on business operations, thus optimizing service quality and availability. Service restoration can be facilitated through the following means:
  - In partnership with the Service Monitoring Functional Component, filter end-user interactions and determine which ones should be associated with Incidents,
  - Detect Incidents, investigate the impact across all domains (server, network, security, and so on), and determine the correct action to take,
  - Initiate change and/or remediation activity for some categories of Incidents.
- **Problem Component.** Responsible for managing the life cycle of all problems. The objectives of the Problem Functional Component are to solve severe/repeating Incidents, prevent Incidents from happening, and minimize the impact of Incidents that cannot be prevented. The Problem cause is not usually known at the time of the Problem data object instance creation, and the Problem Functional Component is responsible for the investigation. The Problem Functional Component also serves as the main exit point from D2C for the feedback information about IT services issues. The feedback is reported to Requirement to Deploy (R2D) in the form of Defects and to the Strategy to Portfolio (S2P) in the form of Portfolio Backlog Items (Demand request).
- **Configuration Management Component.** Focused on tracking the inventories of actual IT configuration items (CIs) and their associated relationships. It identifies, controls, records, reports, audits, and verifies service CIs; including versions, constituent components, their attributes, and relationships.
- **Diagnostics and Remediation Component.** Provides diagnostics information and/or remediation steps to shorten the Mean Time to Repair (MTTR). Run books help streamline diagnosis and remediation for service functions by applying knowledge solutions to service anomalies.
- **Change Control Component.** System that is responsible for managing the life cycle of all of the Requests for Change (RFC) in the IT environment. The Change Control Functional Component makes sure that Changes are done in a standardized and auditable way so that the business risk is minimized.

Detect to Correct Data Objects

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



The Data Objects for this value stream are:

- **Actual Service CI.** A service model data object that serves as the data store for the realization of the service in the production environment. CIs may be populated by service discovery, created by manual processes, or sourced from other processes such as IT Asset Management. A CI is defined as any component that may need to be managed in order to deliver an IT service. Typical CIs include but are not limited to: application services, infrastructure services, databases, message queues, batch jobs, logical transactions, servers (virtual and physical), network devices, storage devices, racks, power distribution units, laptops, software packages, and components.
- **Service Monitor.** Performs the operational measurement aspects of a CI or an IT service in order to understand the current operational status of that CI or IT service.
- **Event.** Represents an alert/notification signifying a change of state of a monitored CI.
- **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.** An auxiliary shared data object. 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.** 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.
- **Request for Change (RFC).** A request to implement an operational modification needed to restore a service or a CI to a usable state.
- **Interaction.** An auxiliary data object that is a record of an end-user contact with the service desk. 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 supportive function data object that was previously defined in the Request to Fulfill (R2F) Value Stream. 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.
- **Conversation.** A supportive function data object that describes a collaborative dialog between two people in the context of IT knowledge.
- **Fulfillment Request.** An auxiliary data object that describes all fulfillment aspects of an IT service, which includes items such as provisioning, deploying, modifying, actions (that is, start, stop, and so on), decommissioning, and so on.
- **Desired Service Model.** An auxiliary service model data object that serves as an instantiation of the unbound Service Catalog Entry, which is the binding of the relevant parameters that determine how a service is deployed/fulfilled. This results in a single realized deployment for the service. The parameters are set by the user’s selections made in the Offer Consumption Functional Component (from the Request to Fulfill Value Stream), as well as the determinations made in the design of the service that are interpreted by the Fulfillment Execution Functional Component (from the Request to Fulfill Value Stream).
- **Portfolio Backlog Item.** An auxiliary data object that represents the repository of all incoming demands, including but not limited to new requests, enhancement requests, and defect fix requests.
- **Service Contract.** Describes the service characteristics and supports service measurement

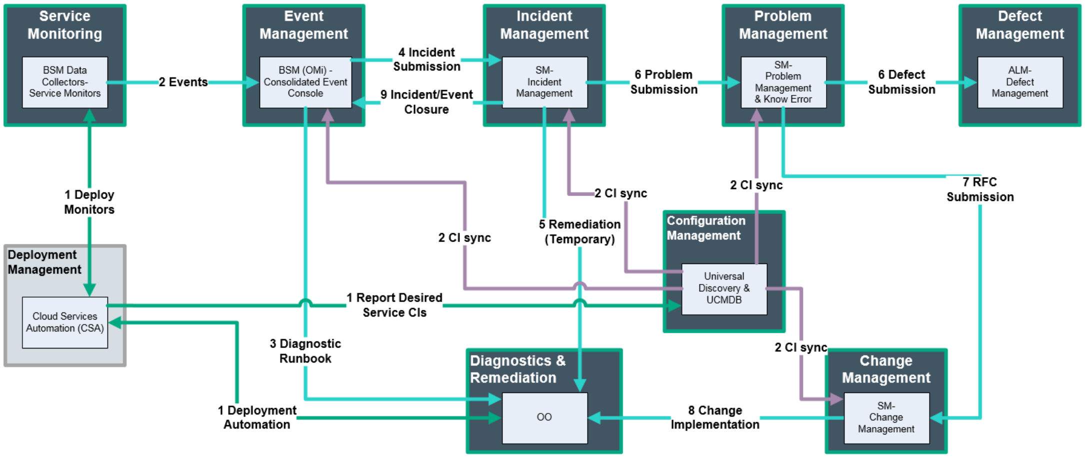
tracking, governance, and audit. Service Contracts can be related to logical services as well as physical services. Service Contracts related to logical services are known as Service Contract templates, while Service Contracts related to physical services are known as Service Contract instances. Each Service Contract data object is comprised of two main parts: the General Contract definitions (also known as the header) and the Service Level Objects (SLOs – the line items) that also enable nesting other Service Contracts that define Service Levels for different aspects of the service. These lines may need to be detailed due to the service being composed of multiple services, because there are multiple providers involved, or to cover different areas of Service Levels.

- **KPI.** An auxiliary data object that holds the definition of an objective that is measured, its requested thresholds, and the exact mathematical method in which measurement data items are used in order to calculate the objective.
- **Service Release Blueprint.** An auxiliary service model data object that holds the information and details related to a specific release to a specific environment.
- **Subscription.** An auxiliary data object that is managed by the Request Rationalization Functional Component (from the Request to Fulfill Value Stream). This data object represents the rights to access a service that has been provided to a consumer.

Detect to Correct 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 Data Objects are created and maintained between the various HPE Products that implement the Functional Components described in "Detect to Correct Functional Components" on page 13.

Additional use cases and the D2C lab diagram follow the main use case flow.



Use case main flow:

1. BSM monitors and OMi monitors discover CIs and send them to the UCMDB. Discovery also populates the UCMDB and the UCMDB syncs the CIs to SM and sends the global IDs (GIDs) back to BSM and OMi.
2. The BPM and SiS monitors report their data into BSM. OM reports its Events to OMi. BSM forwards its Events to OMi and the Events are correlated as cause and symptoms.
3. OO is used (from BSM) to run diagnostics and check the status of the service.
4. Incident is opened from the causal Event.
5. Resolution options:
   a. OO is fired from the Incident through the SM Knowledge Management (KM) to automate a workaround fix like a service restart.
   b. A Problem is opened from the Incident in SM, and then a Defect is opened from the Problem in

ALM. Once the Defect is fixed, the following (third) resolution option is used.

c. A Change is opened from the Problem in SM, then the RFC goes through the Change life cycle (using Release Control).

6. Since it is an emergency Change, it is automatically approved and OO is fired to implement the Change.
7. The Change implementation solves the issue and the Incident and the Event are closed.

Additional use cases:

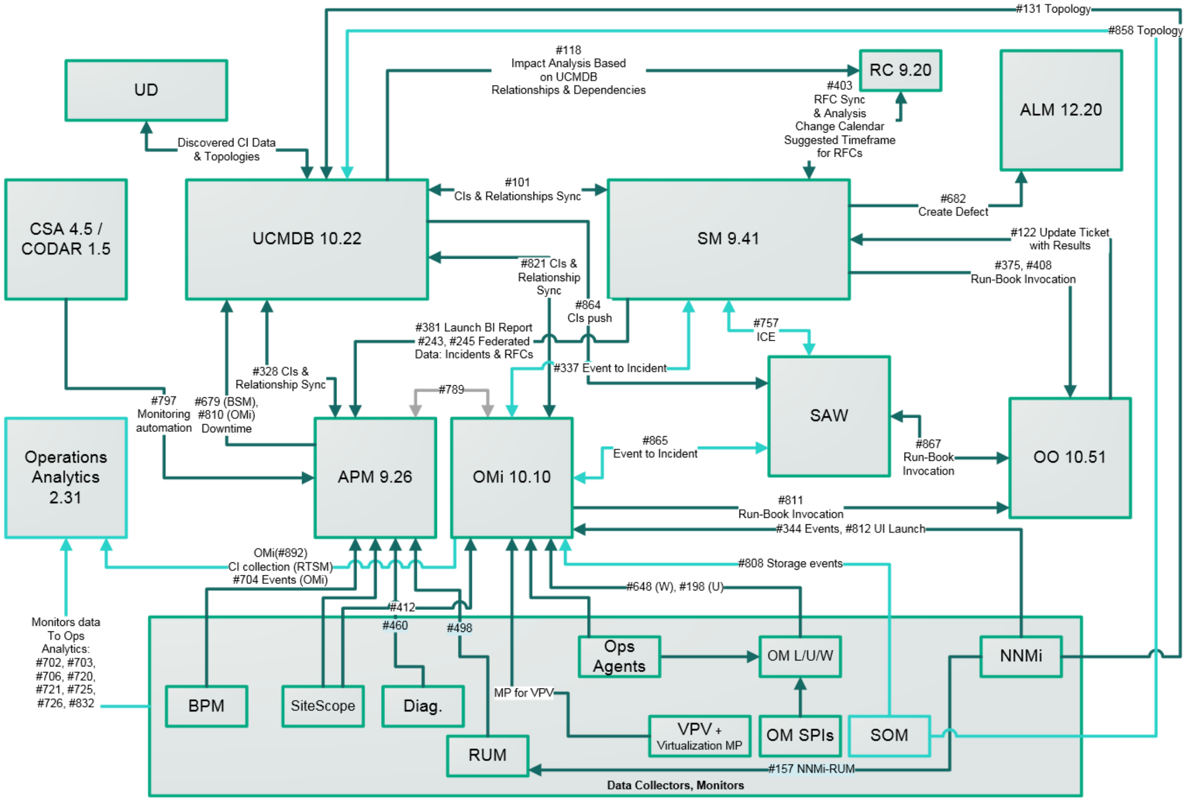
1. Connection between D2C and R2F (Monitoring Automation) from the Fulfillment Execution functional component to the Service Monitoring functional component. BSM and OMi receive monitoring definitions from CSA/Codar, and the monitors are defined.
2. Downtime Management (DT) between SM (through UCMDB) to APM/OMi. DT is created in SM for the change implementation:
   a. RFC is approved in SM.
   b. DT CI created in SM and is synced to the UCMDB using an existing CLIP integration enhancement.
   c. DT CI is pushed to BSM and a BSM DT is created to suppress any events during the change implementation phase.
   d. OO is fired to implement the change.
3. Unrelated to the previous change, an operational DT event is sent from BSM to SM to provide visibility to the Help Desk of that Operational DT.
   a. BSM DT that was created sends a **Start** Event that turns into an SM Incident.
   b. When the DT ends, another event is created and sent to SM to close the Incident.
4. Advanced monitoring—adding RUM, NNMi, OM agent, SPIs, and SOM.
5. Service Anywhere as a replacement to SM in the main use case flow.
6. Unstructured monitoring—adding the Ops Analytics products into the system.
7. Creating a D2C multi-supplied environment:
   a. Integrate Event to Incident in two paths (OMi to SM and SAW per domains) to simulate LOB/Central IT Incident submission.
   b. Integrate SM and SAW for the Incident Case Exchange use case to close the loop of

Incidents. Start with the point-to-point integration.

c. Incident Case Exchange between central IT (SM) and LOB IT (SAW).

Detect to Correct Value Stream Lab Diagram

The following diagram illustrates the integrations that were used to assemble the D2C end-to-end use cases.



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:

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. The HPSW Product versions used in this guide are examples. Check your HPSW Product's Support Matrix for viable alternatives.

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 Version 2.x* (https://softwaresupport.hpe.com/km/KM00701234).

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.

To view the previous version of this guide, see the *Detect to Correct Concept and Configuration Guide Version 1.2* (https://softwaresupport.hpe.com/km/KM00439730).

Prerequisites

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

- **HPE Universal CMDB.** Server is installed. Data flow probe is connected and running (different server than BSM server).
- **HPE Application Lifecycle Management.** Server, client, and the synchronizer package are installed.
- **HPE Business Service Management.** Server is installed and running. BSM machine has the DDM data flow probe connected and running.
- **HPE Operations Manager i.** Server installed. Data flow probe installed on a separate server and connected to OMi.
- **HPE Service Manager.** Server, Client, Help Server, Web Tier, and Knowledge Management are installed and running.
- **HPE Operations Orchestration.** Central and Studio are installed and available for use.
- **HPE Release Control.** Server 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 OMi and SM in order to drill down from OMi Events into SM Incidents. As well, the same user should exist in HPE OO in order to execute HPE OO run books on CIs.

Hardware and Software Requirements

This section includes the following topics:

Supported Versions

> **Note:** The following versions are the supported versions for the D2C use case only.
>
> For the hardware and software requirements, see the product documentation.
>
> IT Service Management functions can be implemented using either a Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based Service Anywhere.

Product	Version	Instructions
Business Service Management	- 9.25 or later **Recommended.** 9.25	For installation instructions, see the *HP Business Service Management BSM Installation Guide*.
Operations Manager i	- 10.01 or later **Recommended.** 10.01	For installation instructions, see the *HP Operations Manager i Installation and Upgrade Guide*.
Application Lifecycle Management	- 12.20 or later **Recommended.** 12.20	For installation instructions, see the *HP Application Lifecycle Management Installation and Upgrade Guide – Windows*.
Service Manager	- 9.40 or later **Recommended.** 9.40	For installation instructions, see the *HP Service Manager Interactive Installation Guide*.
Universal CMDB	- 10.20 or later **Recommended.** 10.20	For installation instructions, see the *HP Universal CMDB Configuration Manager User Guide*.
Operations Orchestration	- 10.21 or later **Recommended.** 10.21	For installation instructions, see the *HP Operations Orchestration Installation Guide*.

Product	Version	Instructions
Release Control	• 9.20 or later **Recommended.** 9.20	For installation instructions, see the *HP Release Control Deployment Guide*.

Enterprise Hardware and Software Requirements

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

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

- **HPE Universal CMDB.** For more information, see the *HP Universal CMDB Support Matrix Version 10.20*.
- **HPE Application Lifecycle Management.** For more information, see the *Integration Support Matrices for HP ALM and Tools 12.20 and Tools 12.02*.
- **HPE Business Service Management.** For more information, see *HP Business Service Management System Requirements and Support Matrixes Version 9.25*.
- **HPE Operations Manager i.** For more information, see *HP Operations Manager i Release Notes Version 10.01*.
- **HPE Service Manager.** For more information, see the *HP Service Manager Support Matrix Version 9.40*.
- **HPE Operations Orchestration.** For more information, see the *HP Operations Orchestration System Requirements Version 10.2x*.
- **HPE Release Control.** For more information, see the *HP Release Control Support Matrix Version 9.20*.

HPE Business Service Management – Overview

HPE Business Service Management (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, and custom reporting and alerting. BSM is based on a common foundation of shared work flow, 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.

HPE Operations Manager i – Overview

HPE Operations Manager i (OMi) is a universal event-correlation software that uses IT topology to automatically correlate related events for quicker and easier root-cause identification—essential in today's complex virtualized and cloud environments—and for heightened efficiency of ITIL Event and Incident management.

OMi is one of HP's Business Service Management (BSM) solutions. It provides a way for customers to pull together events from different monitoring tools. The monitoring tools can be HPE software such as HPE Operations Manager, HPE Operations Agent, HPE ArcSight Logger, and HPE SiteScope, or third-party tools such as IBM Tivoli Enterprise Console (TEC), Microsoft System Center Operations Manager (SCOM), or Nagios. OMi with its BSM connectors can pull that monitoring data together, reduce duplicate event reporting, and prioritize the events by business criticality.

Deploying OMi in an enterprise network environment is a process that requires system architecture design, resource planning, and a well-planned deployment strategy. HPE Software Professional Services offers consulting services to assist customers with OMi strategy, planning, and deployment. For information, contact an HPE representative.

HPE Application Lifecycle Management – Overview

HPE 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 work flow in a central repository.

HPE Service Manager – Overview

HPE Service Manager (SM) is a comprehensive and fully-integrated IT service management software suite that enables you to improve service levels, balance resources, control costs, and mitigate risk exposure to an organization. Service Manager enables you to manage services using a **lifecycle** approach, with consistent improvement built into the governance model. In the context of the Detect to Correct Value Stream, the following modules of HPE Service Manager are leveraged:

- HPE Service Manager Incident Management automates the reporting and tracking of a single Incident or of a group of Incidents, and helps you to achieve service performance that meets Service Level Agreement (SLA), Operation Level Agreement (OLA), and Underpinning Contract (UC) targets.
- HPE Service Manager Problem Management helps you to identify the underlying reasons for one or more Incidents, implement workarounds, identify known errors, and provides permanent solutions that minimize the effects of Incidents caused by errors in the IT infrastructure.
- HPE Service Manager Change Management tracks changes to service assets and configuration items in your infrastructure.
- HPE Service Manager Knowledge Management supports Knowledge-Centered Support (KCS) standards and guidelines by providing a natural language search engine and a rich-text authoring

tool that enables users to search, update, and author knowledge articles. An integration with HPE Operations Orchestration allows the execution of automated run books in a knowledge article context.

HPE Universal CMDB – Overview

HPE Universal CMDB (UCMDB) 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.

HPE Operations Orchestration – Overview

HPE Operations Orchestration (HPE 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 website pages

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

HPE 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

HPE 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

HPE Release Control – Overview

HPE 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

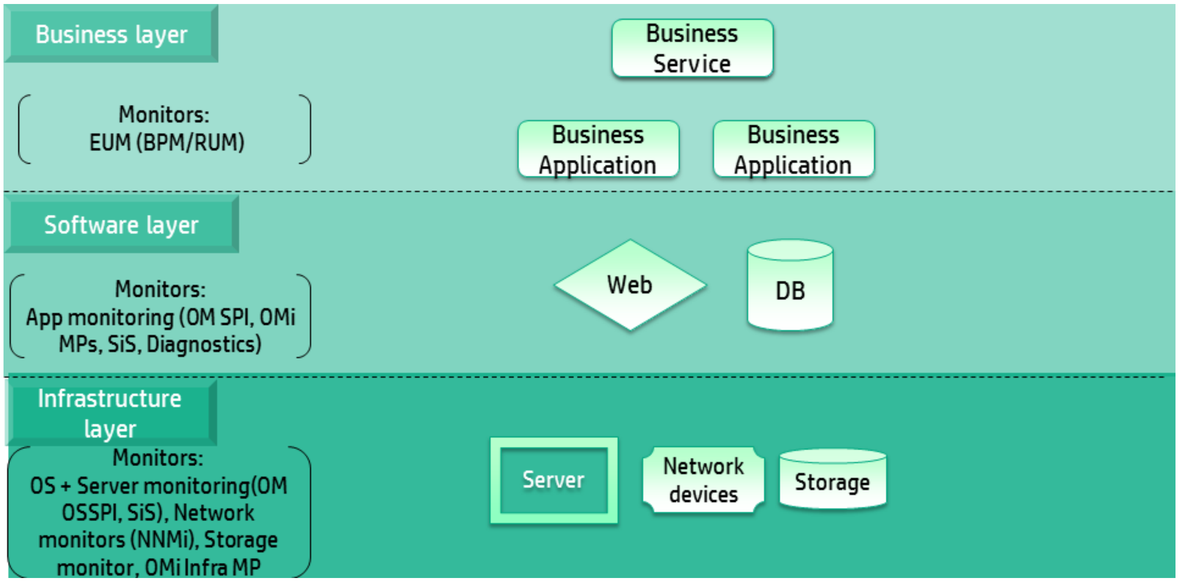
This chapter includes:

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.


Business layer
Monitors: EUM (BPM/RUM)
Business Service
Business Application
Business Application
Software layer
Monitors: App monitoring (OM SPI, OMi MPs, SiS, Diagnostics)
Web
DB
Infrastructure layer
Monitors: OS + Server monitoring(OM OSSPI, SiS), Network monitors (NNMi), Storage monitor, OMi Infra MP
Server
Network devices
Storage

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 Operations Bridge.

- **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 Version 2.x* (https://softwaresupport.hpe.com/km/KM00701234).

Chapter 4: Detect to Correct CI Synchronization

This chapter includes:

Overview

Detect to Correct Value Stream use cases cross individual software boundaries. Therefore, there is a need for an overarching model of configuration items and their relations.

Multiple products implement the CMDB technology.

For instance:

- HPE Operations Manager i (OMi),
- HPE Business Service Management (BSM),
- as well as HPE Universal CMDB (UCMDB) itself.

Because of this, it is a requirement for selected configuration items and their relations to be synchronized across the various products.

Doing a global all-to-all synchronization is not feasible from a performance perspective, and the extensions of the data model in individual products complicate this further.

The HPE recommended approach for configuration item (CI) synchronization is documented in the *HPE RTSM Best Practices Guide* (https://softwaresupport.hpe.com/km/KM01996511). The Detect-to-Correct Value Stream functionality relies on the synchronization of CI data as described in that guide.

Areas of specific interest include:

- Setting UCMBD as a global ID generator
- Synchronization of infrastructure and business CIs between UCMDB and OMi
- Synchronization of business CIs between UCMDB and BSM
- Synchronization of CIs between UCMDB and Service Manager

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

Chapter 5: OMi – APM Integration Configuration

This chapter includes:

Overview

> **Note:** In the following sections, the product is referred to as BSM. The integration of BSM Version 9.25 and later with OMi is referred to as the APM integration.

Integrating HPE Application Performance Management (APM) into HPE Operations Manager i (OMi) allows you to:

- Design a dashboard in which you see OMi and APM data displayed side by side. It is possible to drill down into the APM data from this dashboard.
- Integrate user interface components from separately deployed APM systems directly into the OMi user interface workspaces. In this way, relevant information is shown directly within the OMi user interface, although this data comes from the APM system.

For more information, see the *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).

Prerequisites

- **Data Flow Probe** must be installed.

  Data Flow Probes must be installed and connected to OMi RTSM and UCMDB.

  For details, see "Install the UCMDB Data Flow Probe" in Chapter 3 in *HPE Operations Manager i Version 10.10 OMi Integrations Guide*.

Configure the APM Integration with OMi

This task includes the following steps:

Task 1: Align the LWSSO Configuration

Align the Lightweight Single Sign-On (LWSSO) configuration in both deployments. This enables viewing the APM components in the OMi user interface.

To align LWSSO in the APM deployment:

1. In BSM, navigate to **Administration > Platform > Users and Permissions > Authentication Management**.
2. In the Single Sign-On Configuration pane, click **Configure**.
3. Click **Next**.
4. Set the initString in **JMX to get Token Creation Key (initString)**—for example, **sample_ common_initString**.
5. Click **Finish**.

To align LWSSO in the OMi deployment:

1. In OMi, navigate to **Authentication Management: Administration > Users > Authentication Management**.
2. In the **Single Sign-On Configuration** list, click the **Configure** button. The **Single Sign-On Configuration** wizard opens.
3. Click **Next**.
4. In the Single Sign-On dialog box, select **Lightweight**.
5. Set the same initString you entered in **JMX to get Token Creation Key (initString)** in APM to

the **Token Creation Key (initString)**.

6. Click **Next**.
7. Click **Finish**. The configuration is saved.

Task 2: Create the Integration User and Configure through the APM User Interface

First create your integration user in APM's jmx console. Next configure the integration user through the APM user interface.

To create the integration user:

1. In your APM deployment, go to the jmx console: **http://<*APM server*>:21212/jmx-console**
2. Select **UCMDB Service:Security Services**.
3. Go to **createIntegrationUser()** and create your integration user.
   - **customerID.** 1
   - **userName.** <*integration user name*>
   - **password.** <password>
   - **dataStoreOrigin.** <any value>
4. Click **Invoke**.
5. Invoke the **getUsersList MBean** with **customerID=1** to check if the user is shown in the list of integration users.

If you are using an **admin** user, no further action is required.

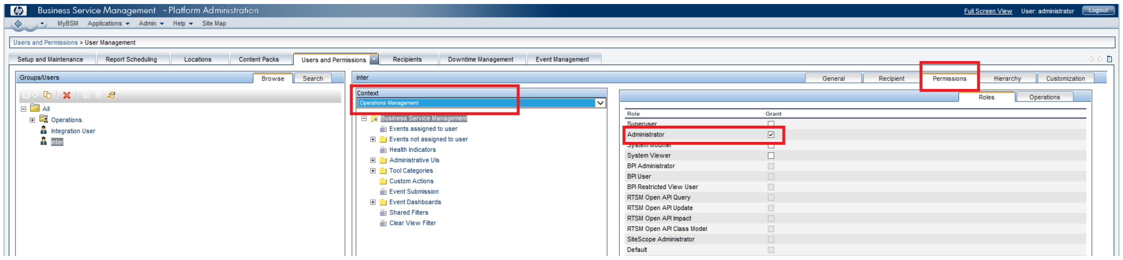
If you are not using an **admin** user, configure the following:

To grant administrative permissions to the integration user:

> **Note:** If the integration user is **admin**, this procedure is not necessary.

1. In your APM deployment, navigate to **Admin > Platform > User and Permissions > User Management**.
2. Select **Create New Users** using the same user name as the integration user previously created.

3. After creating the user, select it and click the **Permissions** tab.
4. From the **Context** drop-down list, select **Operations Management**.



Context: Operations Management

Role	Grant
Superuser	☐
Administrator	☑
System Modifier	☐
System Viewer	☐
BPI Administrator	☐
BPI User	☐
BPI Restricted View User	☐
RTSM Open API Query	☐
RTSM Open API Update	☐
RTSM Open API Impact	☐
RTSM Open API Class Model	☐
SiteScope Administrator	☐
Default	☐

5. In the **Roles** tab, for the **Administrator**, select the **Grant** check box.
6. Click **Apply Permissions**. The integration user is created.

Task 3: Set Up APM Connected Server in OMi and Start the Topology Synchronization

To set up the APM connected server in OMi and start the topology synchronization:

1. **Set up an APM Connected Server in OMi.**

   a. On the OMi deployment, navigate to **Administration > Setup and Maintenance > Connected Servers**.

   b. Click the **New** button. In the Connected Servers drop-down box, select **APM**. The **General** page of the **Create New Server Connection – APM** wizard opens.

   c. Enter the name of your APM deployment. The display name is automatically entered. Click **Next**. The Server Properties page opens.

   d. Enter the fully qualified domain name (FQDN) of the BSM Gateway server.

   e. Enter the **User Name** and **Password** of the integration user.

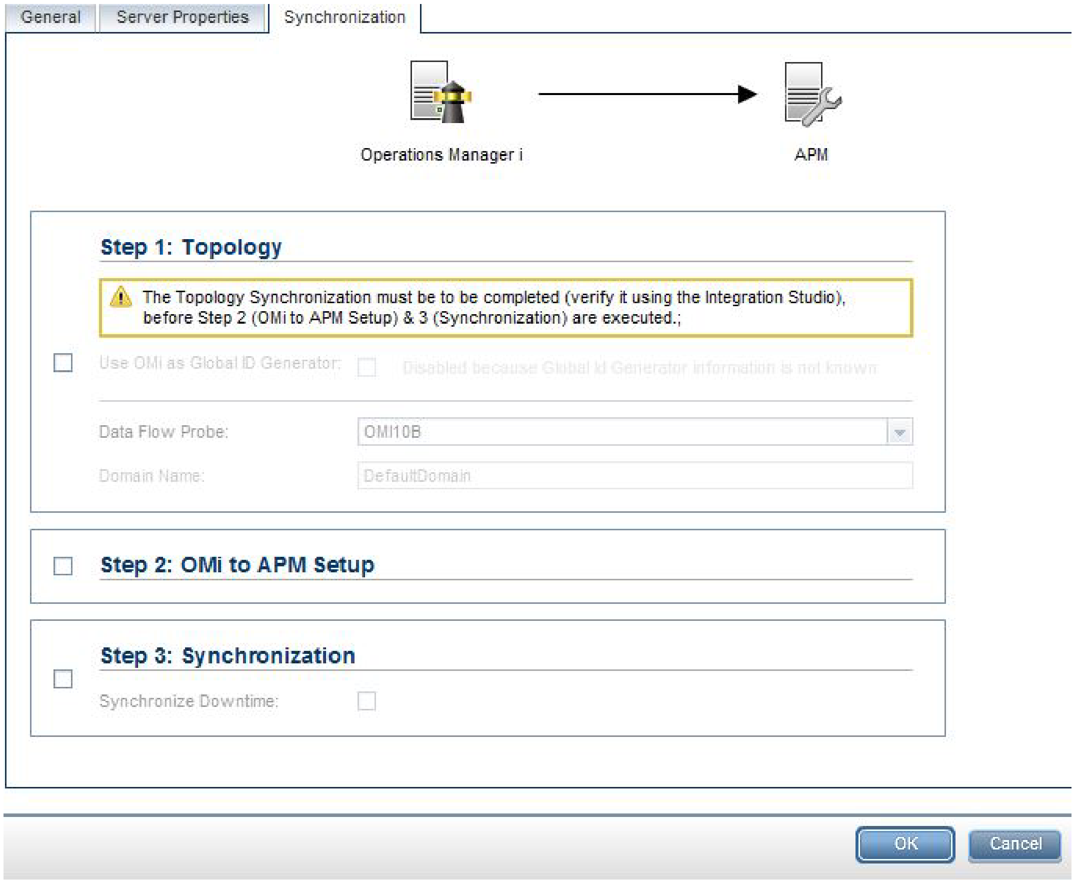
   Optional: If the URL path has changed, you must also add the new URL.

   > **Caution:** If you click **Test Connection** now, you will receive an error because there has been no synchronization yet.

   f. Click **Next.**The Synchronization pane of the **Create New Server Connection – APM** wizard is displayed.

g. In the **Create New Server Connection – APM** wizard, verify that **Step 1: Topology** is not selected.

> **Note:** According to HPE RTSM Best Practices, external UCMDB should be set as a global ID generator. This causes the **Use OMi as Global ID Generator** option to be grayed out. In that case, topology synchronization is done from BSM to UCMDB and from UCMDB to BSM as a separate action.
>
> For more details, see "OMi – APM Integration with External UCMDB" in Chapter 3 in the *HPE Operations Manager i Version 10.10 OMi Integrations Guide*.



Step 1: Topology

The Topology Synchronization must be to be completed (verify it using the Integration Studio), before Step 2 (OMi to APM Setup) & 3 (Synchronization) are executed.;

□ Use OMi as Global ID Generator: □ Disabled because Global Id Generator information is not known

Data Flow Probe: OMI10B

Domain Name: DefaultDomain

□ Step 2: OMi to APM Setup

□ Step 3: Synchronization

Synchronize Downtime: □

h. To complete the **Create New Server Connection** wizard, select a **Data Flow Probe** and click **Finish**.

Verify the Topology Synchronization

a. **To check the status of the integration jobs on the OMi server:**

   i. Navigate to **Administration > Setup and Maintenance > Connected Servers**.

   ii. The tool tip in the Connected Servers pane underneath your connected server tells you the status of the last executed job.

   iii. Wait until one integration job runs successfully before continuing.

   iv. To update the status, in the Connected Servers pane, click the **Refresh** button.

b. **To check the status of the integration jobs in the RTSM Integration Studio:**

   i. Navigate to **Administration > RTSM Administration > Data Flow Management > Integration Studio**. On the left-hand side of the Integration Studio, there is a list of all integration points.

   ii. Select the **APM2UCMDB** integration point. There will be two integration jobs:

   - sync_continuous
   - sync_initial

   iii. Wait until at least one of these completes before continuing. You can manually start either integration job by clicking the **Full Synchronization** icon or the **Delta Synchronization** icon.

2. **Continue the OMi to APM setup.**

   a. After the previous steps are complete, on the OMi server, navigate to:

   Administration > Setup and Maintenance > Connected Servers

   b. Double-click your APM connected server to open the **Edit Server Connection** wizard.

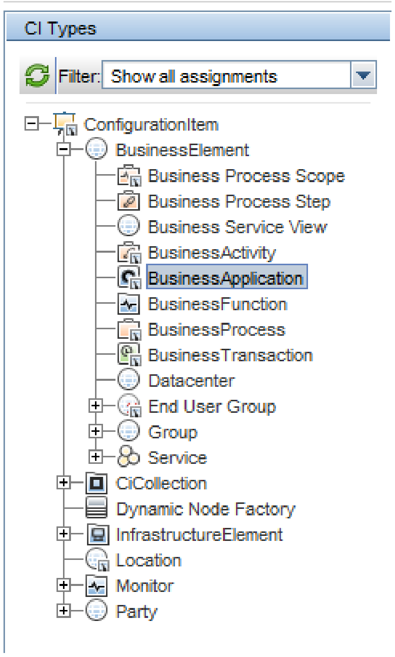
   c. Go to the **Synchronization** tab.

   d. Select the **Step 2: OMi to APM Setup** check box.

   e. Click **Finish**. The integration is complete.

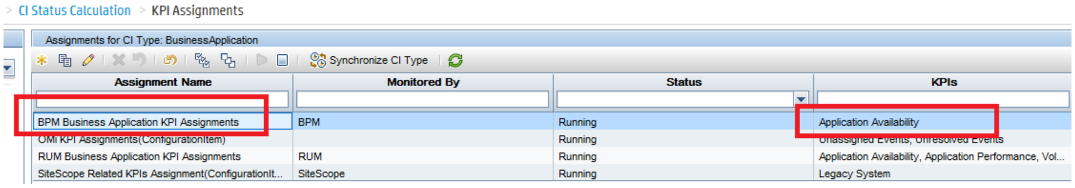
   f. Navigate to **Administration > Service Health > CI Status Calculation > KPI Assignments**.

g. In the KPI Assignments window, in the CI Types pane, navigate to **ConfigurationItem > BusinessElement** and select the **BusinessApplication** CI type.



Filter: Show all assignments

h. In the KPI Assignments window, in the KPI's column, select the **Assignment Name: RUM Business Application KPI Assignments** and click **Edit** ✎.



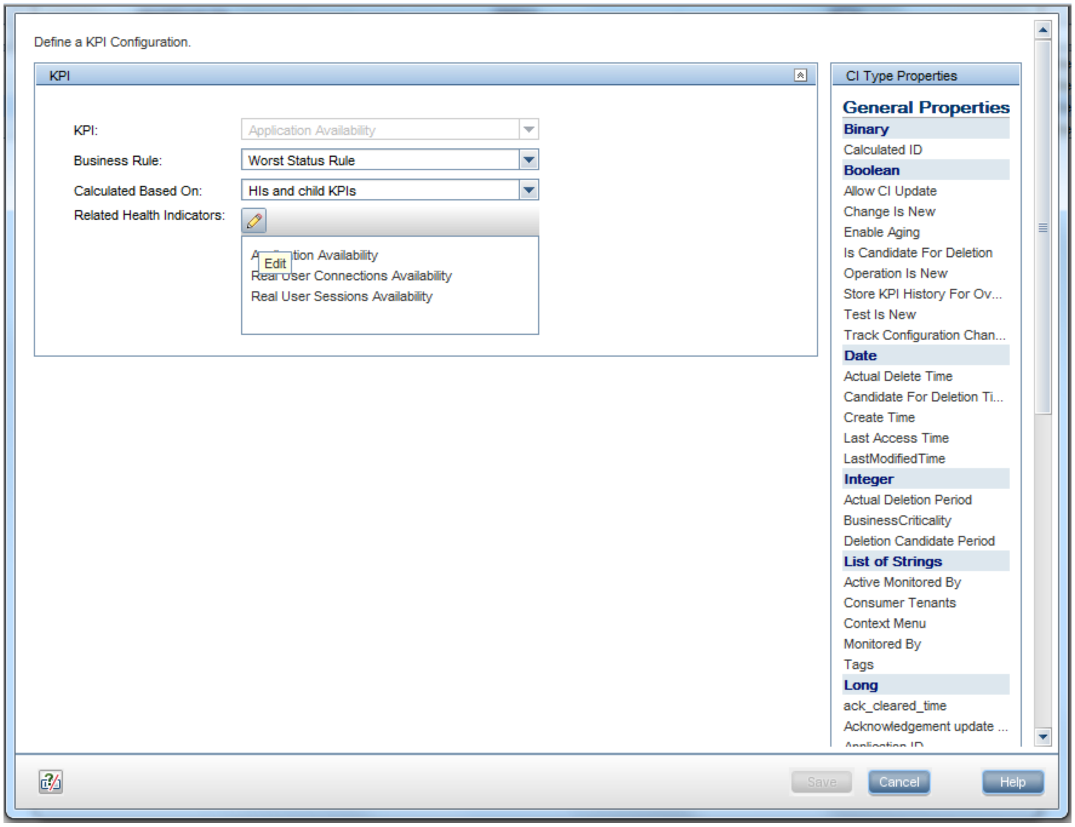
Assignments for CI Type: BusinessApplication

Assignment Name	Monitored By	Status	KPIs
BPM Business Application KPI Assignments	BPM	Running	Application Availability
OMi KPI Assignments(ConfigurationItem)		Running	Unassigned Events, Unresolved Events
RUM Business Application KPI Assignments	RUM	Running	Application Availability, Application Performance, Vol...
SiteScope Related KPIs Assignment(ConfigurationIt...	SiteScope	Running	Legacy System

The Edit KPI for Assignment for CI Type dialog box appears.

i. In this dialog box in the **KPI Configurations** section, select the **Application Availability KPI** and click **Edit**.

j. For the **Related Health Indicators**, click **Edit** ✎.



Define a KPI Configuration.

KPI

KPI: Application Availability

Business Rule: Worst Status Rule

Calculated Based On: HIs and child KPIs

Related Health Indicators:

Application Availability
Real User Connections Availability
Real User Sessions Availability

CI Type Properties

General Properties
Binary
Calculated ID
Boolean
Allow CI Update
Change Is New
Enable Aging
Is Candidate For Deletion
Operation Is New
Store KPI History For Ov...
Test Is New
Track Configuration Chan...
Date
Actual Delete Time
Candidate For Deletion Ti...
Create Time
Last Access Time
LastModifiedTime
Integer
Actual Deletion Period
BusinessCriticality
Deletion Candidate Period
List of Strings
Active Monitored By
Consumer Tenants
Context Menu
Monitored By
Tags
Long
ack_cleared_time
Acknowledgement update ...
Application ID

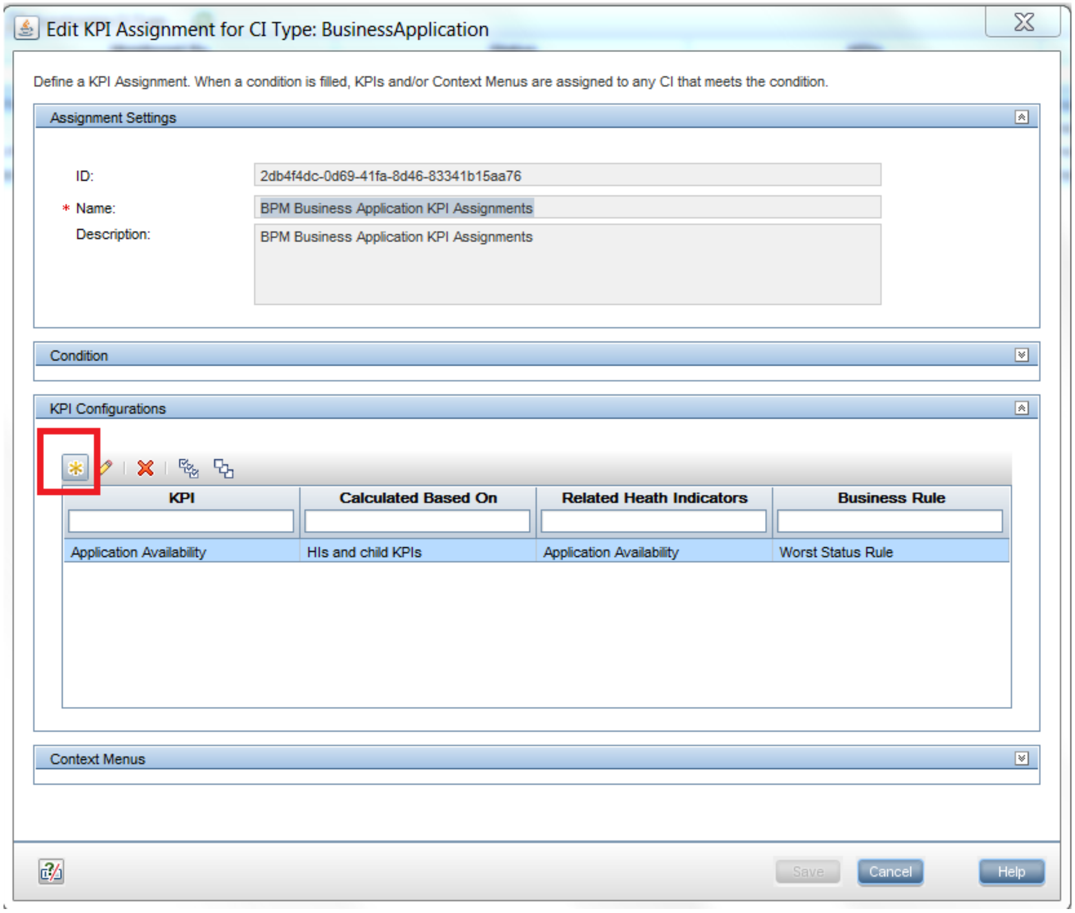
k. In the Related Health Indicator dialog box, under **Applicable Health Indicators**, move **Application Availability** to the **Selected Health Indicators** column and click **Apply**.

l. Click **Save.**

m. Click **Save.**

n. In the KPI Assignments window, in the **KPIs** column, select the **Assignment Name: BPM Business Application KPI Assignments** and click **Edit** ✎. The Edit KPI for Assignment dialog box appears.

o. In the Edit KPI for Assignment: BusinessApplication dialog box, under KPI Configurations, click the **New** button.



Edit KPI Assignment for CI Type: BusinessApplication

Define a KPI Assignment. When a condition is filled, KPIs and/or Context Menus are assigned to any CI that meets the condition.

Assignment Settings

ID: 2db4f4dc-0d69-41fa-8d46-83341b15aa76

* Name: BPM Business Application KPI Assignments

Description: BPM Business Application KPI Assignments

Condition

KPI Configurations

KPI	Calculated Based On	Related Heath Indicators	Business Rule
Application Availability	HIs and child KPIs	Application Availability	Worst Status Rule

Context Menus

p. In the Add KPI to Assignment dialog box, in the **KPI** selection box, select **Application Availability**.

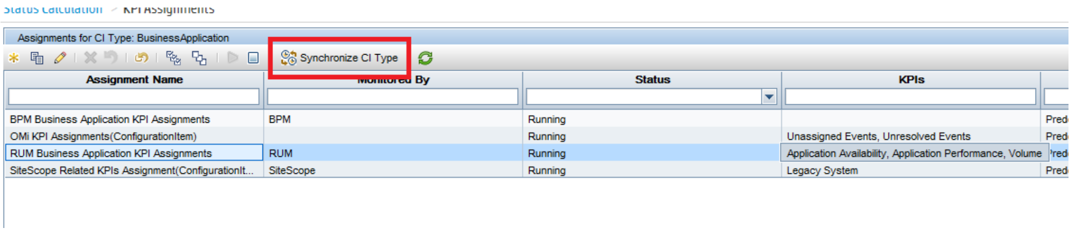
q. For the **Related Health Indicators**, click **Edit** .

r. Under **Applicable Health Indicators**, move **Application Availability** to the **Selected Health Indicators** column and click **Apply**.

s. Click **Save**.

t. Click **Save**.

u. On the toolbar, select **Synchronize CI Type**.



Assignments for CI Type: BusinessApplication

Assignment Name	Monitored By	Status	KPIs	
BPM Business Application KPI Assignments	BPM	Running		Pred
OMi KPI Assignments(ConfigurationItem)		Running	Unassigned Events, Unresolved Events	Pred
RUM Business Application KPI Assignments	RUM	Running	Application Availability, Application Performance, Volume	'red
SiteScope Related KPIs Assignment(ConfigurationIt...	SiteScope	Running	Legacy System	Pred

v. Using Application Performance Health Indicators (HI) and KPIs, repeat steps **2.g** through **2.u**.

3. **Finalize the integration configuration.**

   a. In OMi, navigate to **Administration > Setup and Maintenance > Connected Servers**.

   b. Double-click the APM connected server. The **Edit Server Connection** wizard opens.

   c. Select the **Step 3: Synchronization** check box. This triggers the initial synchronization of all KPI states for all APM CIs.

> **Note:** This initial synchronization is necessary in order to view the current state on the APM system.
>
> The APM and OMi integration does not synchronize BPM-related CIs and Events from BSM to OMi. In order to enable these capabilities, see Appendix B, "Adding BPM CIs and Events to OMi" on page 163.

Chapter 6: OMi – SM Incidents Exchange Integration

This chapter includes:

Overview

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

HPE Operations Manager i (OMi) events and their updates can be automatically or manually forwarded to HPE Service Manager (SM) as Events. 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 OMi 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 OMi to SM

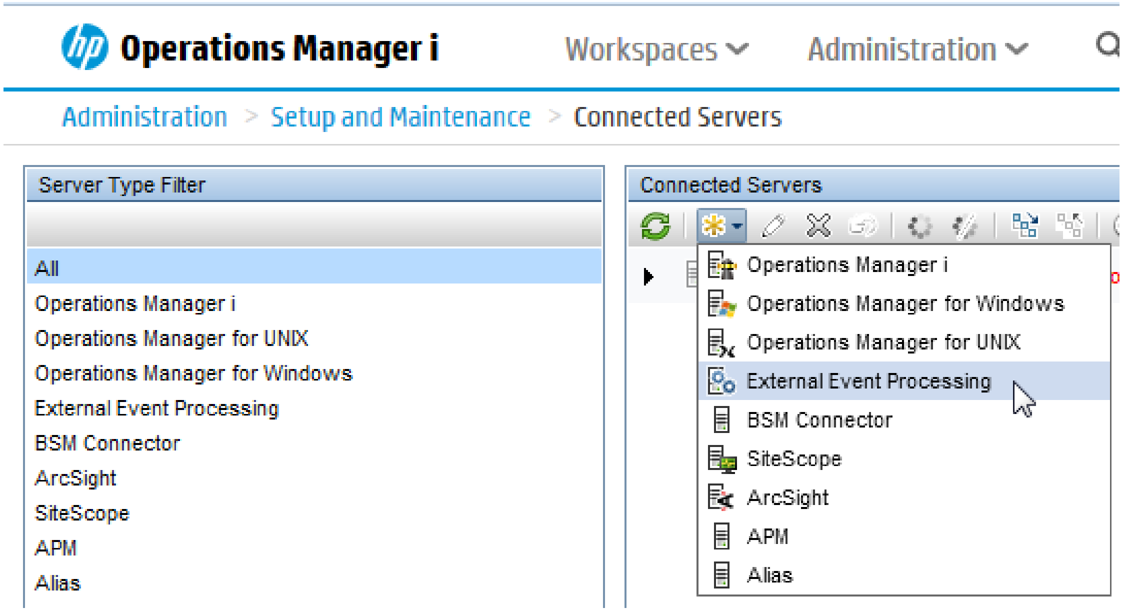
> **Note:**
>
> - Before starting this procedure, create a user in SM with full administrative permissions to use for the integration. Remember these user details as you will need them in the following procedure.
> - For instructions on how to create the user, see the Service Manager documentation.
> - Be sure to modify **ServiceManagerAdapter.groovy** to support the installed SM Version (specifically, the web-tier version).
> - For more information about this configuration of this integration, see Part V: "Operations Manager i – Service Manager Integration" in *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).
> - This section provides instructions for IT Service Management functions using SM. For integrations using Software-as-a-Service (SaaS)-based HPE Service Anywhere (SAW), see "OMi – SAW Integration Configuration" on page 128.

To configure the SM server as a target connected server:

> **Caution:** When integrating OMi with SM Version 9.40, make sure that one of the following patches is applied:
>
> - HPSM_00700 - Service Manager 9.40.2001 p2 - Server for Linux
> - HPSM_00701 - Service Manager 9.40.2001 p2 - Server for Solaris
> - HPSM_00702 - Service Manager 9.40.2001 p2 - Server for Windows
> - HPSM_00706 - Service Manager 9.40.2001 p2 - OMi Integration

1. In OMi Version 10.01, navigate to the Connected Servers manager: **Administration > Setup and Maintenance > Connected Servers**.

2. In the Connected Servers pane, click the **New** button and select **External Event Processing**.


Operations Manager i
Workspaces
Administration
Administration > Setup and Maintenance > Connected Servers
Server Type Filter
All
Operations Manager i
Operations Manager for UNIX
Operations Manager for Windows
External Event Processing
BSM Connector
ArcSight
SiteScope
APM
Alias
Connected Servers
Operations Manager i
Operations Manager for Windows
Operations Manager for UNIX
External Event Processing
BSM Connector
SiteScope
ArcSight
APM
Alias

The **Create New Server Connection – External Event Processing** 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. Enter the **Fully Qualified DNS Name** of the SM target server.

   In **CI Type** drop-down list, select **Service Manager System** and click **Next**.

7. For the Integration type, select **Call 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.

8. 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 fit the deployed SM web tier name—for example, **webtier-9.40**.

   c. Click **OK** to save this copy of the script and close the Manage Scripts dialog box.

9. Click **Next**. The Outgoing Connection pane appears.

10. Provide the following Even Forwarding credentials to the Even 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 if the configuration is done on a development/testing environment. **Note:** For production, it is recommended to use secure HTTP. For more details, see *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).
Supports Synchronize and Transfer Control	**<selected>**	Confirm this check box is selected. 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. 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. If the **Supports Synchronize and Transfer Control** flag is not set for any target connected server, the **Transfer Control** to option does not appear at all in the Event Browser context menu. 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.

> **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 Chapter 22, "OMi – SM Integration with UCMDB" in the *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).
>
> - Enter the appropriate value in the **Port** field.

11. Click the **Test connection** link located on the top of the window.
12. Click **Next**. The Event drill down pane appears.
13. 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 drill down to SM, you must install a web tier client for your SM server according to your SM server install/configuration instructions.
    > - In the Event drill down 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 drill down 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 drill down 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.

14. 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 14 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.
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

Field	Sample Value	Description
		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.
omi.mgr.id	**f3832ff4-a6b9-4228-9fed-b79105afa3e4**	Universally Unique Identifier (UUID) automatically generated in OMi for the target Service Manager server. **Note:** This parameter was introduced to support multiple OMi servers. Service Manager uses the UUID to identify from which OMi server an Incident was opened. Be aware that if you delete the connected server configuration for the Service Manager server in OMi and then recreate the same configuration, OMi generates a new UUID. You need to reconfigure the integration instance by changing the old UUID to the new one.

7. 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.

8. Click **Next** twice, and then click **Finish**. The Integration Instance Manager window appears.
9. 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 OMi to SM Configuration

The OMi to SM integration enables the creation of SM Incidents based on OMi Events.

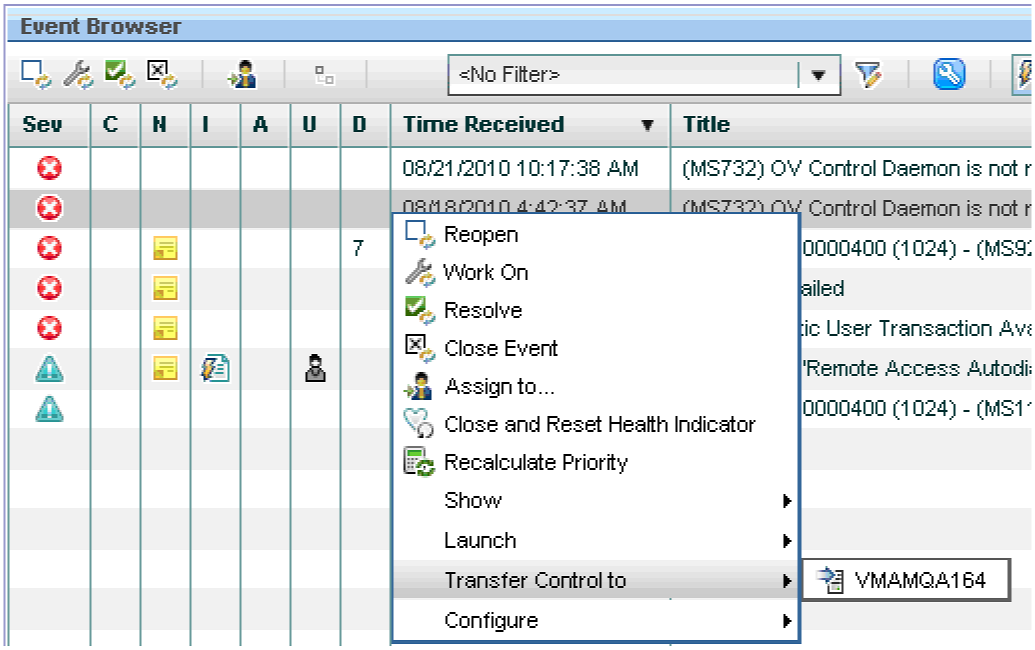
To verify the OMi-SM configuration:

1. Create a new Event in OMi.

   For example, use the Event **submitEvents.bat** that resides in **<*OMi 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.

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



4. 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.
>
> Alternatively, if LWSSO is already configured in OMi and SM, click the Incident ID, which is a link, and it will launch **Service Manager** showing the Incident details.

5. In the SM user interface, navigate to the **Incident Management** module and click the **Search Incidents** option.

6. 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 7: OMi – SM Business Impact Report Integration

This chapter includes:

Overview

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

HPE Operations Manager i (OMi) 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 the event on Business Service CIs, Application CIs, and Business Process CIs includes KPI data and over-time data. For example, if the status for a host CI is critical, you can use the report to display the status of the Business Service CIs to which the host CI is attached.

When deployed as part of the D2C Value Stream, including the integration of OMi with HPE Service Manager (SM), Service Desk Agents perform an initial investigation and review of Incidents. This is done in the Incident Management module in SM. The Incident Management user launches the impact report from an Incident in the context of the Incident's affected CI and validates the updated status of the business impact to categorize and prioritize the Incident.

Access Business Impact Report via SM User Interface

> **Note:** This section provides instructions for IT Service Management functions using SM. For integrations using Software-as-a-Service (SaaS)-based HPE Service Anywhere (SAW), see "OMi – SAW Integration Configuration" on page 128.

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

To add a Business Impact Report integration instance:

1. Log on to the HPE 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).

Name	Recommended Value	Description
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	**<*OMi 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 OMi 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 OMi and SM integration enables launching the 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 an OMi Event. (For details, see "Verify OMi to SM Configuration" on page 56.)
2. In the Incident Details window, click the **More** button and select **Launch Business Impact Report**. The OMi 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 OMi logon details to log on to OMi. A Business Impact Report appears in the context of the relevant CI (affected CI in the Incident record).

Chapter 8: Execute HPE OO Flows from OMi

This chapter includes:

Overview

HPE Operations Orchestration (HPE OO) provides a simple way for customers to run scripts for automatic actions. The integration with HPE Operations Manager i (OMi) utilizes the HPE 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 execution can be activated manually by the Operations Bridge user, or automatically according to predefined rules and conditions.

> **Note:** This document uses HPE OO Version 10.21 and OMi Version 10.01. The procedure may be different for other versions, but the value to the end user is essentially the same since the same integration use cases are implemented. For more information, see each product's Support Matrix and relevant integration documentation.

Execute HPE OO Flows from OMi User Interface

This task describes the configuration steps needed to integrate OMi and HPE OO.

Configure the Link Between OMi and HPE OO

To configure the integration between OMi and HPE OO:

1. In OMi, navigate to **Administration > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Integrations with other applications**.
4. In the **HPE Operations Orchestration** table, locate the HPE OO application URL. Modify the setting for the URL used to access the HPE 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 HPE OO.

Import HPE OO Server Certificates to OMi

> **Note:** The following instructions are for HPE OO Version 10.01. For HPE OO Version 9.x, see Chapter 27 in Part VII, "Operations Manager i – Operations Orchestration Integration" in *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).

Task 1: Export server certificates from HPE OO and import them into OMi in a Windows environment.

> **Note:** By default, HPE OO supports all self-signed certificates. However, in a production environment, it is recommended to change this default to a custom CA or a well known CA for security reasons.

Use the Keytool utility that is included in JRE to export server certificates from HPE OO and import them into OMi in a Windows environment.

1. On the **OO Server**, enter

   ```
   [OO install folder]\java\bin\keytool.exe -keystore "[OO install folder]
   ```

```
\central\var\security\key.store" -export -alias tomcat -file
"<path>\<Operations

Orchestration fully qualified host name>.cer"
```

2. When prompted for a password, enter `changeit`.

Task 2: Import the Server Certificate from the HPE OO server to the OMi Gateway Server

By importing the Server Certificate from the HPE OO server to the OMi Gateway Server, the two systems can communicate with each other securely.

1. To import the server certificate you exported from HPE OO to the OMi cacerts keystores:

   On the OMi Gateway Server and Data Processing Server, enter the following commands:

   ```
   "%TOPAZ_HOME%\JRE\bin\keytool" -keystore "%TOPAZ_

   HOME%\JRE\lib\security\cacerts" -import -alias "<Operations Orchestration

   fully qualified host name>" -file "<path>\<Operations Orchestration fully

   qualified host name>.cer"
   ```

2. When prompted for a password, enter `changeit`.
3. To prevent a certificate error, make sure that this certificate is imported as a trusted root certification authority on any browser that will be accessing OMi.

   The procedure for importing the certificate may vary slightly depending on the type of browser that you are using. For example, if you are using Internet Explorer, follow these steps:

   a. Click **Tools > Internet Options > Content > Certificates**.

   b. In the Trusted Root Certification Authorities tab, click the **Import...** button.

   c. Click **Next** to start the Certificate Import Wizard.

   d. Specify the file you want to import, and then click **Next**.

   e. Select the **Place all certificates in the following store** radio button, and then click **Browse**.

   f. Select **Trusted Root Certification Authorities**, and then click **Next**.

   g. Click **Finish**.
4. Restart **OMi**.

Permissions

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

For details, see Chapter 26, "OMi – OO Integration Overview" in *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).

To integrate with HPE OO, set up users with specific permissions:

1. Navigate to **Administration > Users > Users, Groups, and Roles**.
2. Select the user or create a new user and grant them a role with **Operations Orchestration Integration** permissions.

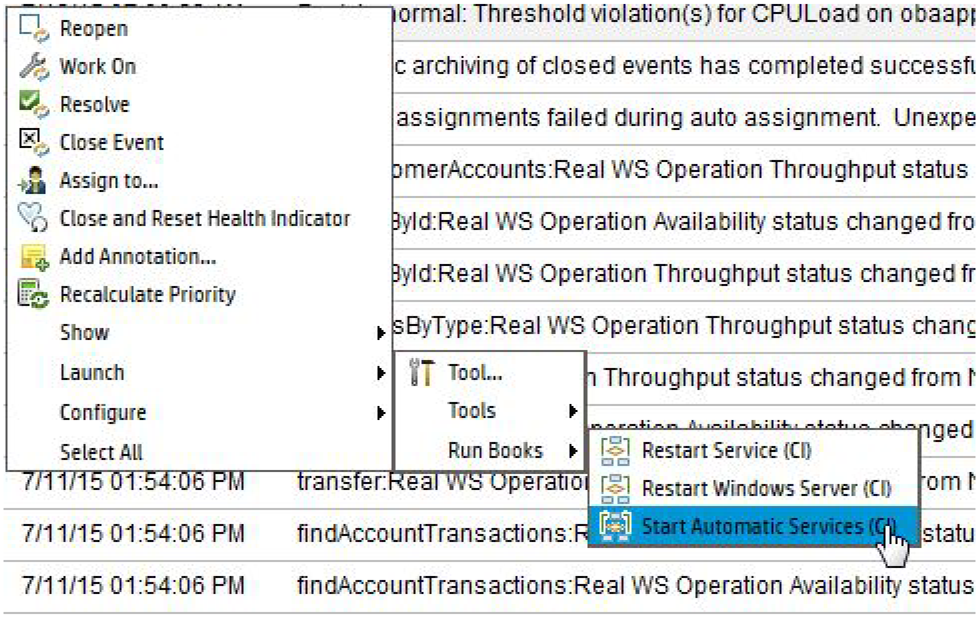
When setting up the users, keep the following in mind:

- Set up an integration user with the same name in OMi and OO—for example, **OMiOO_integr_user**.
- In OMi, the user must have the **Operations Console > Run Book Execution** permission and the **RTSM Permission > Resource Type > Queries** permission to execute run books.
- To enable an OMi user to map a run book to the selected CI type, in OMi, the user must have the **Operations Console > Run Book Mappings** permission to administer run books.

Validation

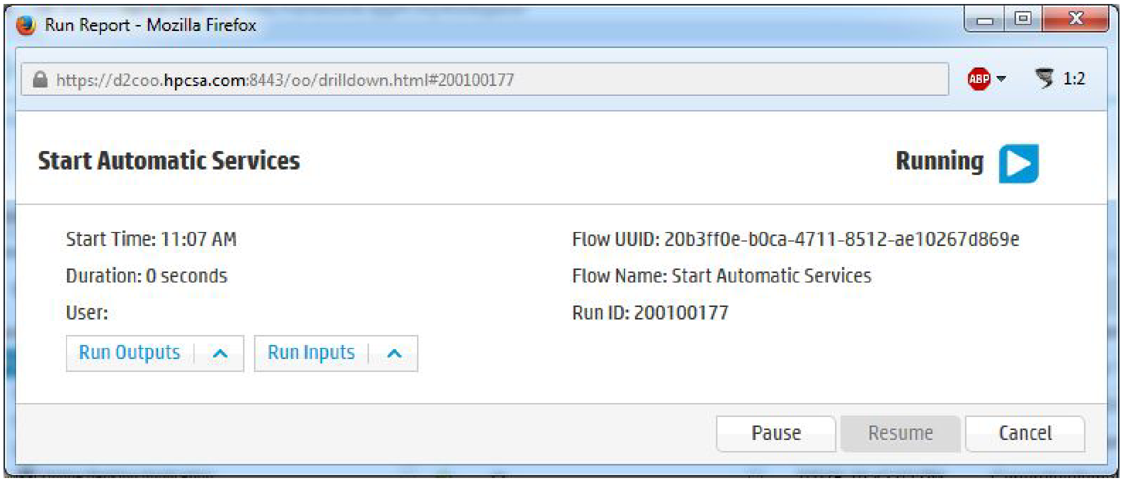
To validate the integration's successful setup:

1. Navigate to the **Event** console and select an Event with a related CI that has HPE OO's run book mapped—for example, an Event related to a Windows' host.
2. Right-click the Event and select **Launch > Run Books**.


Reopen
Work On
Resolve
Close Event
Assign to...
Close and Reset Health Indicator
Add Annotation...
Recalculate Priority
Show
Launch
Configure
Select All
Tool...
Tools
Run Books
Restart Service (CI)
Restart Windows Server (CI)
Start Automatic Services (CI)
ormal: Threshold violation(s) for CPULoad on obaap
c archiving of closed events has completed successfu
assignments failed during auto assignment. Unexpe
omerAccounts:Real WS Operation Throughput status
3yId:Real WS Operation Availability status changed fro
3yId:Real WS Operation Throughput status changed fr
sByType:Real WS Operation Throughput status chang
n Throughput status changed from N
nged
7/11/15 01:54:06 PM transfer:Real WS Operatio
rom N
7/11/15 01:54:06 PM findAccountTransactions:R
statu
7/11/15 01:54:06 PM findAccountTransactions:Real WS Operation Availability status

3. Select the appropriate run book to execute—For example, **Start Automatic Services**.

If the flow has the appropriate input parameter values, the execution starts and progress is displayed in a pop-up window such as:



Run Report - Mozilla Firefox
https://d2coo.hpcsa.com:8443/oo/drilldown.html#200100177
1:2

Start Automatic Services

Running

Start Time: 11:07 AM

Duration: 0 seconds

User:

Flow UUID: 20b3ff0e-b0ca-4711-8512-ae10267d869e

Flow Name: Start Automatic Services

Run ID: 200100177

Run Outputs
Run Inputs
Pause
Resume
Cancel

Chapter 9: Execute HPE OO Flows from SM

This chapter includes:

Overview

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

HPE Operations Orchestration (HPE 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 HPE OO flows communicate and document procedures, decreasing dependencies on individuals or groups. For more information, see the HPE OO documentation.

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

> **Note:** This document uses HPE OO Version 10.21 and SM Version 9.40. The procedure may be different for other versions, but the value to the end user is essentially the same since the same integration use cases are implemented. For more information, see each product's Support Matrix and relevant integration documentation.

Enable HPE OO Flows from SM – KM Module

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

Prerequisites

In order to execute OO flows in the context of Incident records:

1. install and enable the KM Engine, which 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 9.40\SearchEngine\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 9.40\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 > Knowlegebases, click **Search**.

   b. **In the Knowledge Library.** Confirm the status is online. If not, click **Full Reindex**.

Configure SSL on HPE OO

> **Note:**
>
> - By default, HPE OO supports all self-signed certificates. However, in a production environment, it is recommended to change this default to a custom CA or a well known CA for security reasons.
> - This procedure applies to configuring SM with HPE OO Version 10.21. To configure with other HPE OO versions, see your SM Help Server.

Task 1: Configure Central SSL Server Certificate with FQDN

You can generate a self-signed certificate using the Keytool utility.

1. Stop **Central** and back up the original key.store file located in ***<installation dir>*/central/var/security/key.store**.
2. Open a command line in ***<installation dir>*/central/var/security**.
3. Delete the existing server certificate from the **Central** key.store file using the following command:

   ```
   keytool -delete -alias tomcat -keystore key.store -storepass changeit
   ```

4. Generate a self-signed certificate using the following command:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keypass changeit -keystore key.store
   -storepass changeit -storetype JKS -dname "CN=<CENTRAL_FQDN>, OU=<ORGANIZATION_
   UNIT>, O=<ORGANIZATION>, L=<LOCALITY>, C=<COUNTRY>"
   ```

5. Start **Central**.

Task 2: Configure SSL on OO Central

1. Stop the **HP Operations Orchestration Central** service.
2. Search for the **keytool.exe** file installed on your machine and append its location to the **Path** variable in your system environment.
3. Open a command line in **<*installation dir*>/central/var/security**.
4. Run the following command:

   ```
   keytool.exe -export -alias tomcat -file "xxx\oo10-certificate.cer" -keystore
   "%OO_Home%\central\var\security\key.store" –storepass changeit
   ```

   > **Note:** Later, when configuring SSL in Service Manager, you will import **oo10-certificate.cer** into the Service Manager trust store file.

5. Start the HP OO service.

Configure SSL on SM

> **Note:** This section provides instructions for IT Service Management functions using SM. For integrations using Software-as-a-Service (SaaS)-based HPE Service Anywhere (SAW), see "Execute HPE OO Flows from SAW" on page 142.

To configure SSL on SM:

1. Stop the **Service Manager Server** service.
2. Copy **oo10-certificate.cer** into a directory on the Service Manager server host.

   > **Note:** This is the certificate you created when configuring SSL in HPE OO.

3. Search for the **keytool.exe** file and append its location to the **Path** variable in the system environment. Open a CMD window under **%SM_home%\Server\RUN**.
4. Use the following command to import the OO certificate into the Service Manager trust store file:

   ```
   keytool.exe -import -alias xxx -file “xxx\oo10-certificate.cer” -keystore
   smtrust –storepass smoointabc123
   ```

5. Answer **Y** when prompted. The confirmation message **Certificate was added to keystore** appears. Verify **smtrust** was created under **<*SM_home*>\Server\RUN**.

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

   ```
   # Certificates

   truststoreFile:smtrust

   truststorePass:smoointabc123
   ```

7. Start the **Service Manager Server** service.

Add an SMOO Integration Instance

To add an SMOO integration instance:

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

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

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

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

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

Enable an Integration Instance

To enable an integration instance:

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

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

Configure LWSSO in HPE OO

If Lightweight Single Sign-On (LWSSO) is enabled in both SM and HPE OO, users who have logged on to SM are allowed to sign on to HPE 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 109.

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

To configure LWSSO in HPE 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 HPE products (minimum length: 12 characters)—for

example, smintegrationlwsso. Make sure that this value is the same as that used in the LWSSO configurations of the other HPE 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-lwsso>
       <lwssoValidation id="ID000001">
       <domain>asia.hpqc.net</domain>
       <crypto cipherType="symmetricBlockCipher"
       engineName="AES" paddingModeName="CBC"       keySize="256"
encodingMode="Base64Url"
       initString="sample_common_initString"></crypto>
       </lwssoValidation>
       </in-ui-lwsso>
       </validation>
       <creation>
       <lwssoCreationRef id="ID000002">
       <lwssoValidationRef refid="ID000001"/>
       <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
       </creation>
</webui>
```

4. Restart the HPE OO services.

Chapter 10: SM – ALM/QC Integration

This chapter includes:

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
- 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 *Defects and Requirements Exchange with HP Service Manager and HP Application Lifecycle Management Installation and Administration Guide* (https://softwaresupport.hpe.com/km/KM01532231).

The integration should be configured in three system components:

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

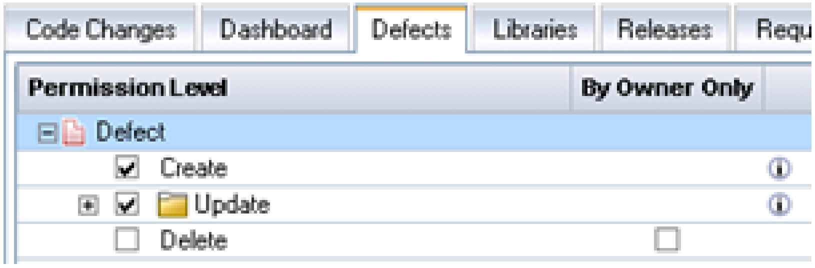
To complete the setup, the user must obtain the ALM Synchronizer tool appropriate for the ALM version being used. Refer to following pages to locate the latest published integration package.

- *HP ALM Synchronizer* (https://hpln.hp.com/group/synchronizer-content-alm)
- *Defects and Requirements Exchange with HP Service Manager/ServiceCenter and HP ALM* (https://hpln.hp.com/page/defects-and-requirements-exchange-hp-service-managerservicecenter-and-hp-alm)

HPE Application Lifecycle Management

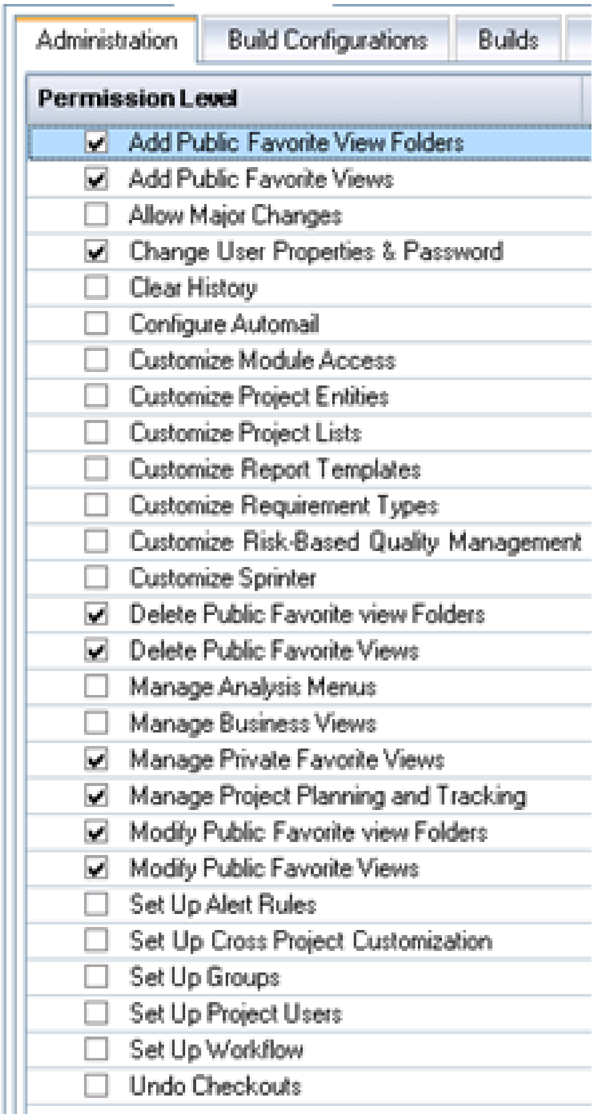
To configure the ALM side of the integration:

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 both the **Defect > Create** and **Defect > Update** permission levels.



Permission Level	By Owner Only
⊟ Defect	
☑ Create	
⊞ ☑ Update	
☐ Delete	☐

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



Permission Level

- ☑ 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.

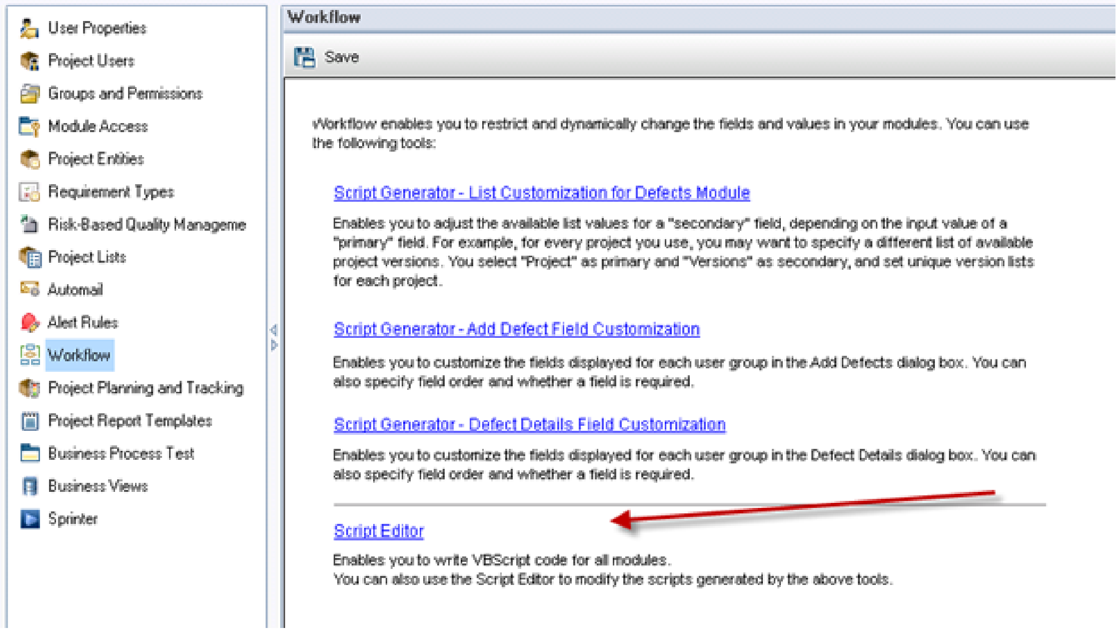
3. In the ALM console, select the **Project Entities** tab. In the Project Entities pane, select **Defect > User Fields**. Click **New Field** to add the following fields:

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

Field Label	Field Type	Length	Remarks
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**.



Workflow enables you to restrict and dynamically change the fields and values in your modules. You can use the following tools:

Script Generator - List Customization for Defects Module

Enables you to adjust the available list values for a "secondary" field, depending on the input value of a "primary" field. For example, for every project you use, you may want to specify a different list of available project versions. You select "Project" as primary and "Versions" as secondary, and set unique version lists for each project.

Script Generator - Add Defect Field Customization

Enables you to customize the fields displayed for each user group in the Add Defects dialog box. You can also specify field order and whether a field is required.

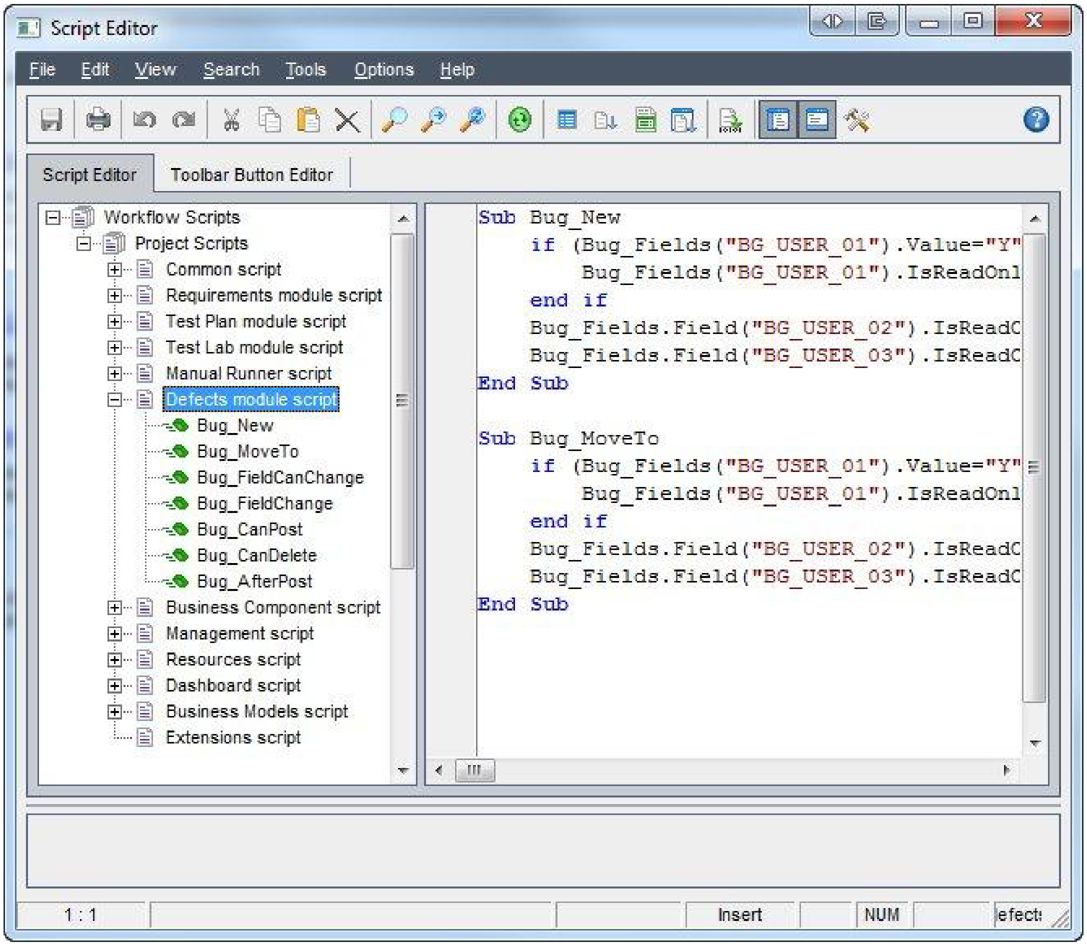
Script Generator - Defect Details Field Customization

Enables you to customize the fields displayed for each user group in the Defect Details dialog box. You can also specify field order and whether a field is required.

Script Editor

Enables you to write VBScript code for all modules.
You can also use the Script Editor to modify the scripts generated by the above tools.

- Select the **Script Editor** tab.



```
Sub Bug_New
    if (Bug_Fields("BG_USER_01").Value="Y"
        Bug_Fields("BG_USER_01").IsReadOnl
    end if
    Bug_Fields.Field("BG_USER_02").IsReadC
    Bug_Fields.Field("BG_USER_03").IsReadC
End Sub

Sub Bug_MoveTo
    if (Bug_Fields("BG_USER_01").Value="Y"
        Bug_Fields("BG_USER_01").IsReadOnl
    end if
    Bug_Fields.Field("BG_USER_02").IsReadC
    Bug_Fields.Field("BG_USER_03").IsReadC
End Sub
```

- 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** .

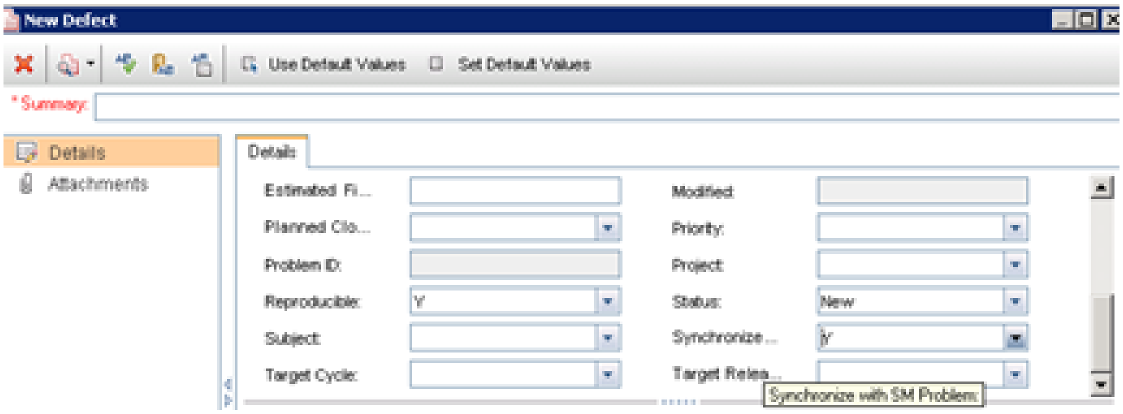
   > **Note:** The purpose of this view is to let the ALM Synchronizer correctly filter those defects to be synchronized to SM as problems.

   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**.



Reproducible: Y

Status: New

Synchronize...: Y

HPE Service Manager

> **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.

To configure the SM side of the integration:

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.

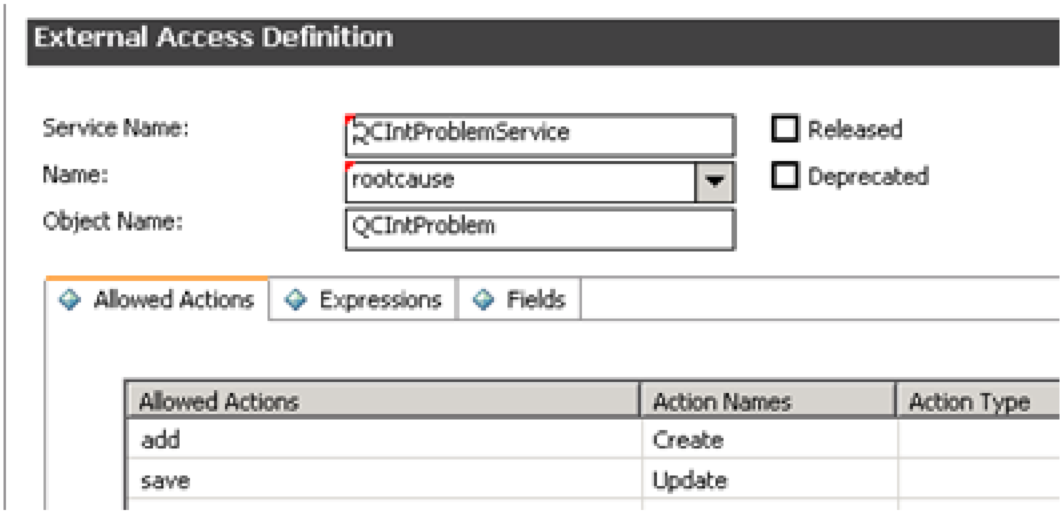
Page	Field	Value
General	Logon Name	SMQCIntUser
General	Full Name	ALM integration default account
General	Contact ID	*The contact created in step 1a.*
General / Application Profiles	Problem Profile	PMProfile_QCInt
Security	Unlimited Sessions	Yes
Security	Password	*Your password*
Login Profile	Time Zone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

2. 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

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



External Access Definition

Service Name: QCIntProblemService
Name: rootcause
Object Name: QCIntProblem
□ Released
□ Deprecated

Allowed Actions	Action Names	Action Type
add	Create	
save	Update	

> **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

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 $L.file;if (denull($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:

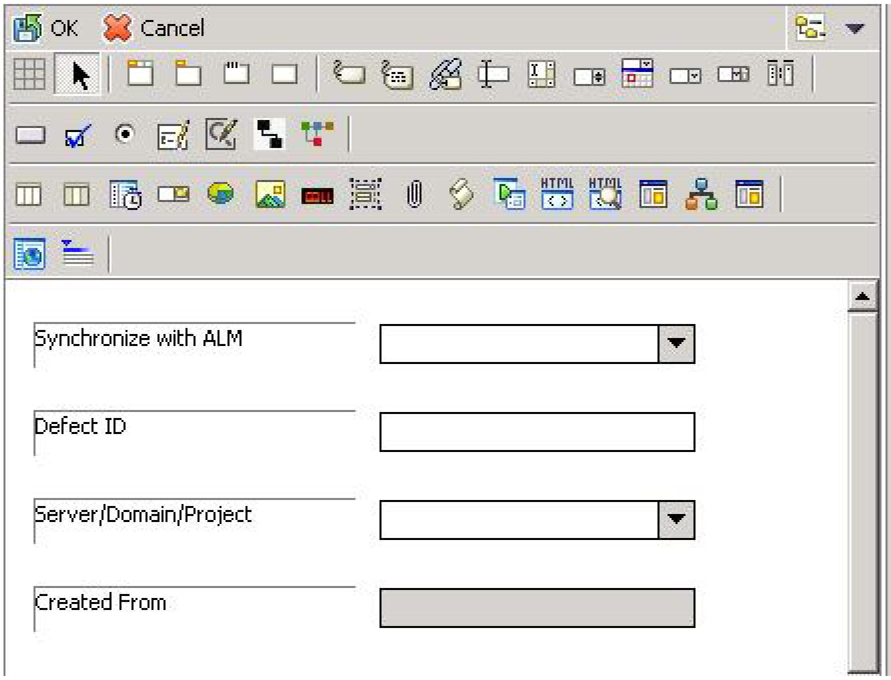
Parameter	Value	Remarks
List Name	SMQC Integration PM Project List	
Regen Entry	1 00:00:00	
Build List on Startup?	Yes	Check box
List Variable	$G.qcintegration.problem.project	Check box
User Defined List?	Yes	
Value List	{"server1/domain1/project1"}	Change to the values for your system **Note:** No spaces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

Component	Properties
	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



Synchronize with ALM

Defect ID

Server/Domain/Project

Created From

8. Add the subform created in the previous step to selected Problem Management forms:

   a. In Forms Designer, locate one of the Problem Management forms and click **Design**.

      > **Note:** This could be named differently depending on which version of Service Manager is being used—for example, **pbm.problem.logging**.

   b. Add a **Notebook** tab with the caption **ALM Integration** and add the **pm.qcint.subform** to it. Save the changes.

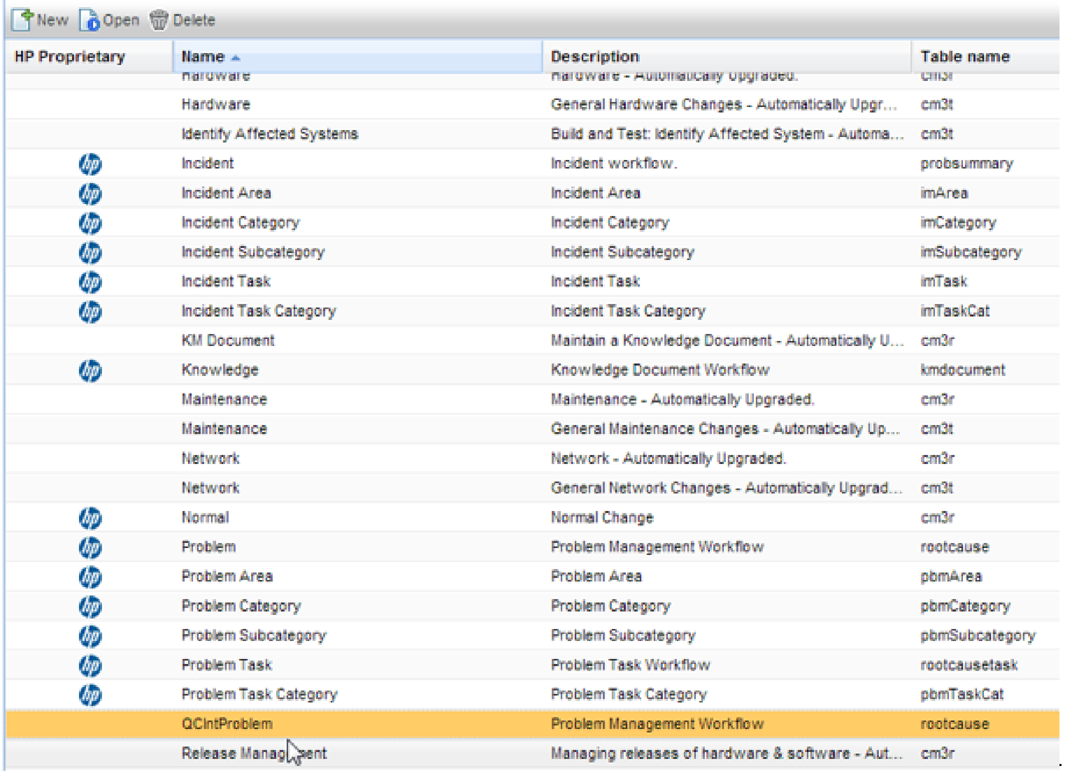
   c. Where needed, repeat the steps above for additional Problem Management forms to display ALM-related information.

9. Create rules that will define the behavior of the fields we added in different phases of the Problem record life cycle.

> **Note:** Since we are using Service Manager with the Process Designer Content Pack, the following steps are different from the out-of-the-box Service Manager setup.

a. Navigate to **Tailoring > Process Designer > Copy Existing Workflow**.

b. Locate, select, and copy the **Problem** entry. Create a name for the new workflow—for example, **QCIntProblem**.



HP Proprietary	Name	Description	Table name
	Hardware	Hardware - Automatically Upgraded.	cm3r
	Hardware	General Hardware Changes - Automatically Upgr...	cm3t
	Identify Affected Systems	Build and Test: Identify Affected System - Automa...	cm3t
hp	Incident	Incident workflow.	probsummary
hp	Incident Area	Incident Area	imArea
hp	Incident Category	Incident Category	imCategory
hp	Incident Subcategory	Incident Subcategory	imSubcategory
hp	Incident Task	Incident Task	imTask
hp	Incident Task Category	Incident Task Category	imTaskCat
	KM Document	Maintain a Knowledge Document - Automatically U...	cm3r
hp	Knowledge	Knowledge Document Workflow	kmdocument
	Maintenance	Maintenance - Automatically Upgraded.	cm3r
	Maintenance	General Maintenance Changes - Automatically Up...	cm3t
	Network	Network - Automatically Upgraded.	cm3r
	Network	General Network Changes - Automatically Upgrad...	cm3t
hp	Normal	Normal Change	cm3r
hp	Problem	Problem Management Workflow	rootcause
hp	Problem Area	Problem Area	pbmArea
hp	Problem Category	Problem Category	pbmCategory
hp	Problem Subcategory	Problem Subcategory	pbmSubcategory
hp	Problem Task	Problem Task Workflow	rootcausetask
hp	Problem Task Category	Problem Task Category	pbmTaskCat
	QCIntProblem	Problem Management Workflow	rootcause
	Release Management	Managing releases of hardware & software - Aut...	cm3r

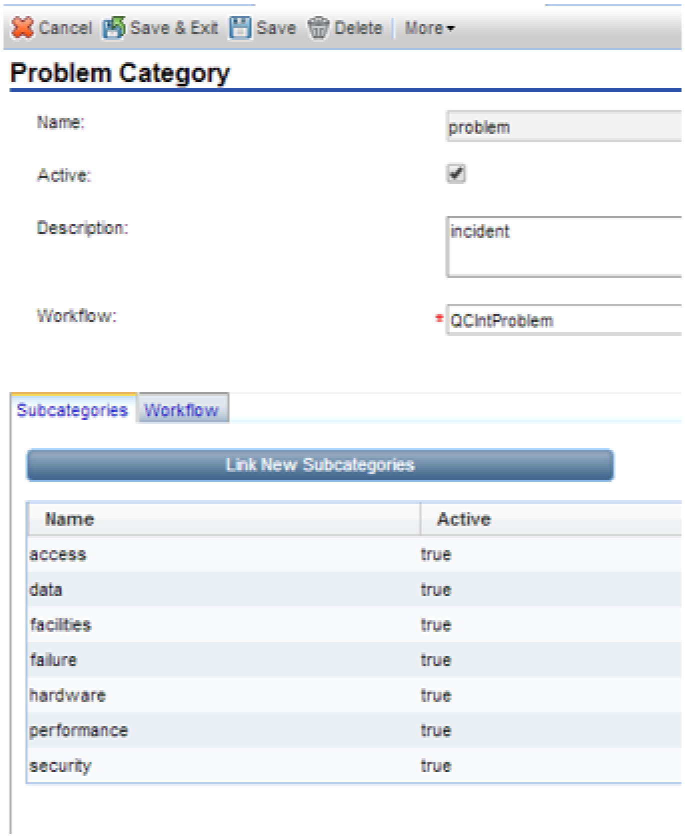
c. From the System Navigator, navigate to **Problem Management > Configuration > Problem Categories** and click **Search**.

d. In the **Problem Category** page, remove the currently assigned workflow from the **Workflow** field.

e. Select the problem category for which you want to add a workflow—for example, **Problem**.

f. Enter **QCIntProblem** in the **Workflow** field.

> **Note:** Use the new workflow name defined in step b above.



Problem Category

Name:	problem
Active:	☑
Description:	incident
Workflow:	* QCIntProblem

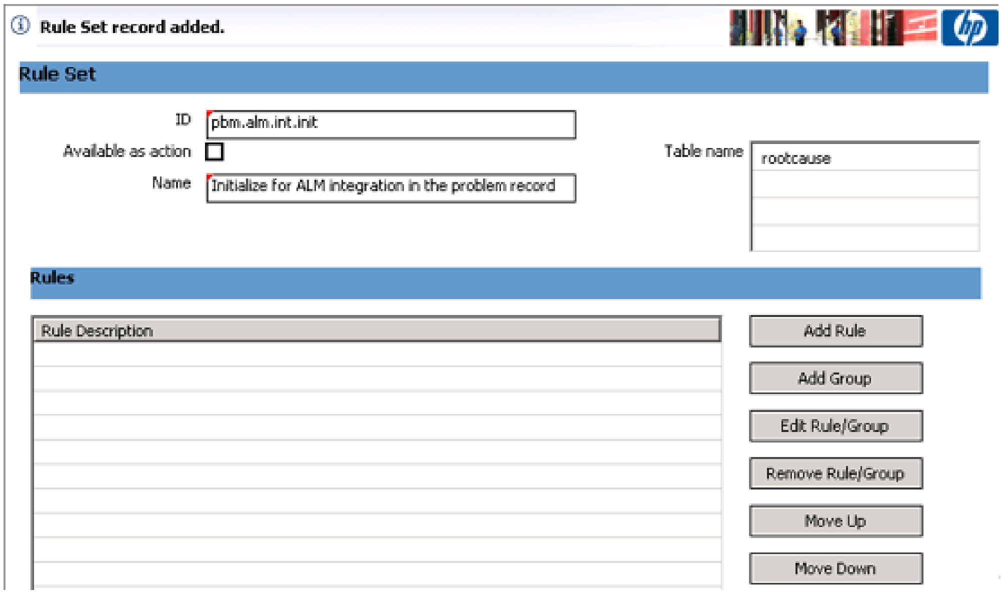
Name	Active
access	true
data	true
facilities	true
failure	true
hardware	true
performance	true
security	true

g. Click **Save** to associate the Problem Category with the workflow.

h. Click **Add Rule**.

i. Create a new rule set for initialization.

   i. From the System Navigator, navigate to **Tailoring > Process Designer > Rule Sets** and enter the values as shown in the following figure:



Rule Set record added.

Rule Set

ID pbm.alm.int.init

Available as action □

Name Initialize for ALM integration in the problem record

Table name rootcause

Rules

Rule Description

   ii. Click **New** and **Save**.

   iii. Click the **Add Rule** button.

   iv. In the **Select Rule Type** page, click **Run JavaScript**.

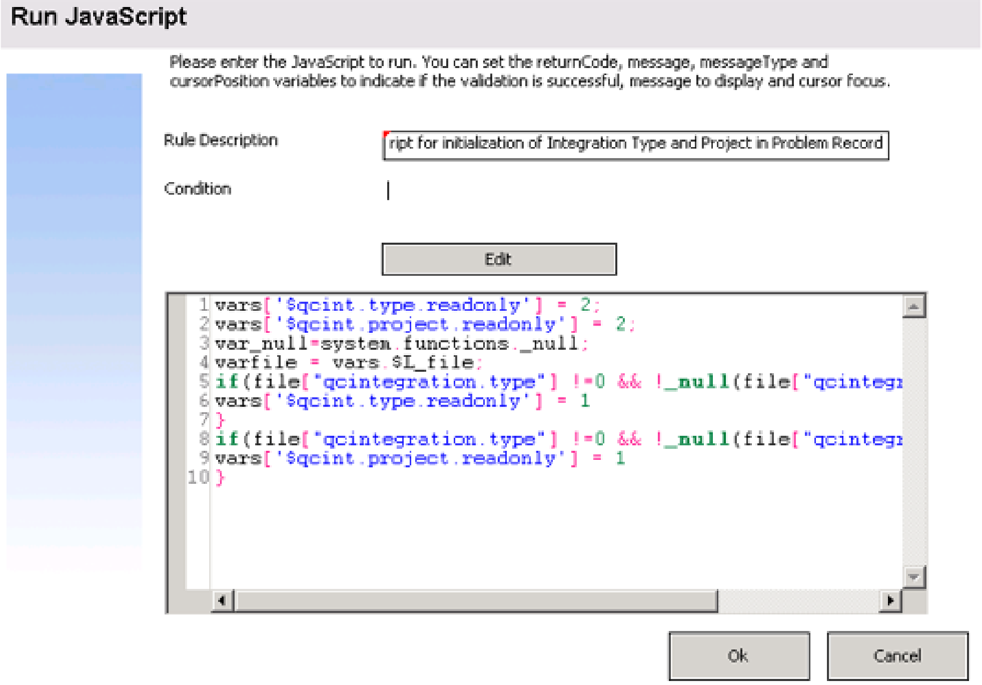
   v. On the **Run JavaScript** page, enter the following values and click **OK**.

Field Name	Description
Rule Description	Run JavaScript for initializing Integration type and project in the Problem Record

Statement	`vars['$qcint.type.readonly'] = 2;`
	`vars['$qcint.project.readonly'] = 2;`
	`var_null=system.functions._null;`
	`varfile = vars.$L_file;`
	`if(file["qcintegration.type"] !=0 && !_null(file ["qcintegration.type"])) {`
	`vars['$qcint.type.readonly'] = 1`

Field Name	Description

	`}`
	`if(file["qcintegration.type"] !=0 && !_null(file ["qcintegration.project"])) {`
	`vars['$qcint.project.readonly'] = 1`
	`}`



Run JavaScript

Please enter the JavaScript to run. You can set the returnCode, message, messageType and cursorPosition variables to indicate if the validation is successful, message to display and cursor focus.

Rule Description: ript for initialization of Integration Type and Project in Problem Record

Condition:

```
vars['$qcint.type.readonly'] = 2;
vars['$qcint.project.readonly'] = 2;
var_null=system.functions._null;
varfile = vars.$L_file;
if(file["qcintegration.type"] !=0 && !_null(file["qcintegr
vars['$qcint.type.readonly'] = 1
}
if(file["qcintegration.type"] !=0 && !_null(file["qcintegr
vars['$qcint.project.readonly'] = 1
}
```

vi. Click **Save** and **Exit**.

10. Create a new rule set for validation.

    a. From the System Navigator, navigate to **Tailoring > Process Designer > Rule Sets** and enter the following values:

Field	Value
ID	pbm.alm.int.validation
Name	Validation for ALM integration in the Problem Record
Table Name	rootcause

b. Click **New** and **Save**.

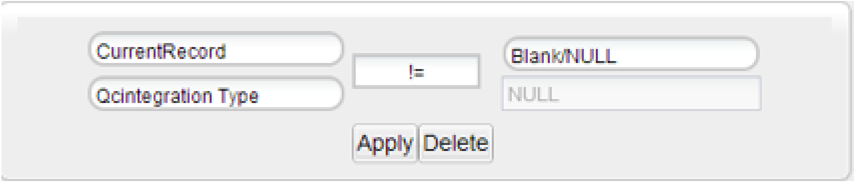
c. Click **Add Rule**.

d. In the **Select Rule Type** page, click **Set Mandatory Fields**.

e. Click **Edit**.

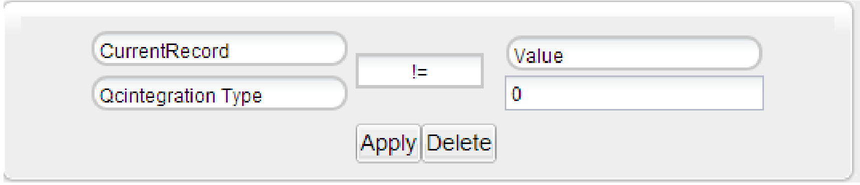
The **Condition** editor opens.

f. Add an expression as shown in the following figure and click **Apply**.



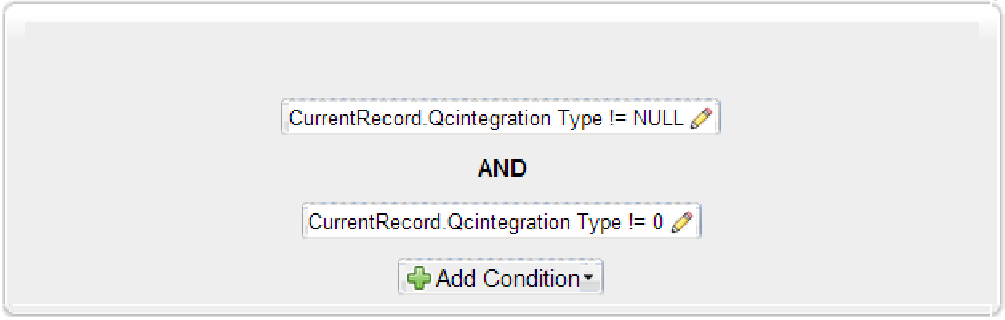
CurrentRecord
Qcintegration Type
!=
Blank/NULL
NULL

g. Add another expression as shown in the following figure and click **Apply**.



CurrentRecord
Qcintegration Type
!=
Value
0

h. After clicking **Apply**, the following dialog box appears:



CurrentRecord.Qcintegration Type != NULL

AND

CurrentRecord.Qcintegration Type != 0

Click **OK** at the bottom of the dialog box.

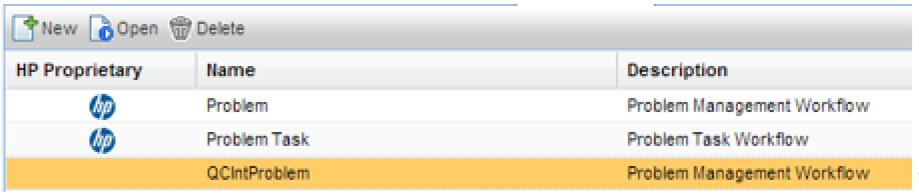
i. Click **OK**. The **Set Mandatory Fields** page closes.

j. Click **Save** and **Exit**.

11. Associate the new workflow with the new initialization and validation rule sets.

a. From the **System Navigator, navigate to Problem Management > Configuration > Workflows**.

b. Select **QCIntProblem** in the workflows list and click **Open**.

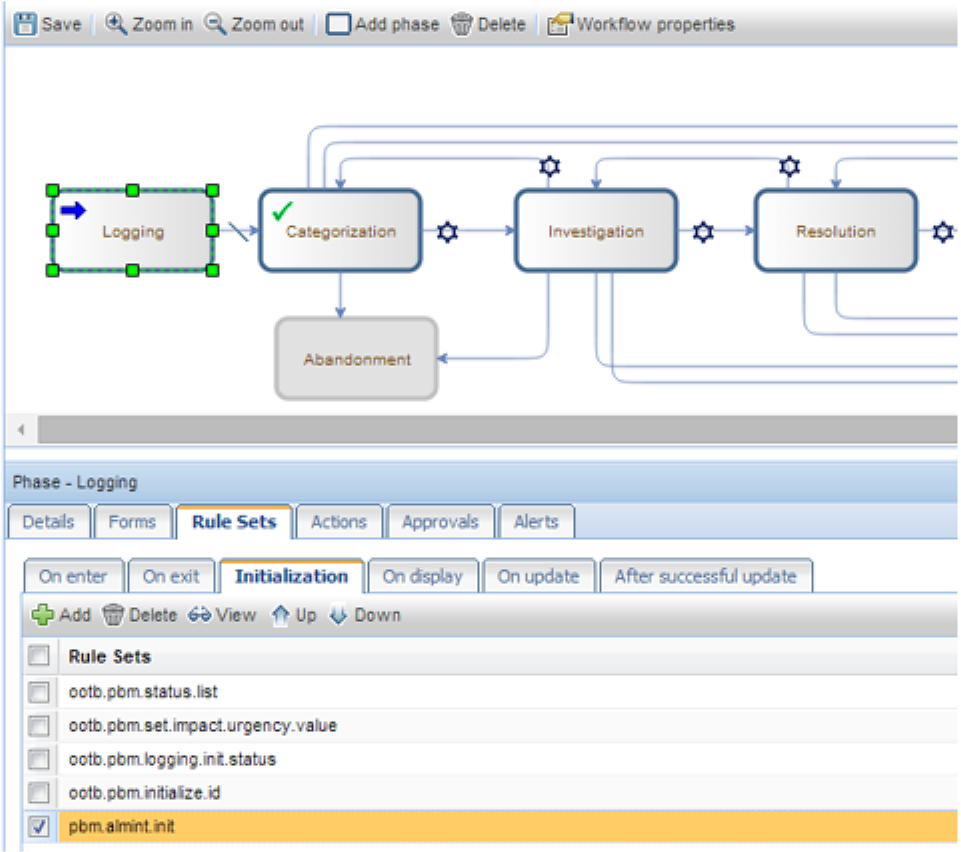


HP Proprietary	Name	Description
hp	Problem	Problem Management Workflow
hp	Problem Task	Problem Task Workflow
	QCIntProblem	Problem Management Workflow

c. Select the first phase in the workflow graph.

d. Click the **Rule Sets** tab and then the **Initialization** tab.

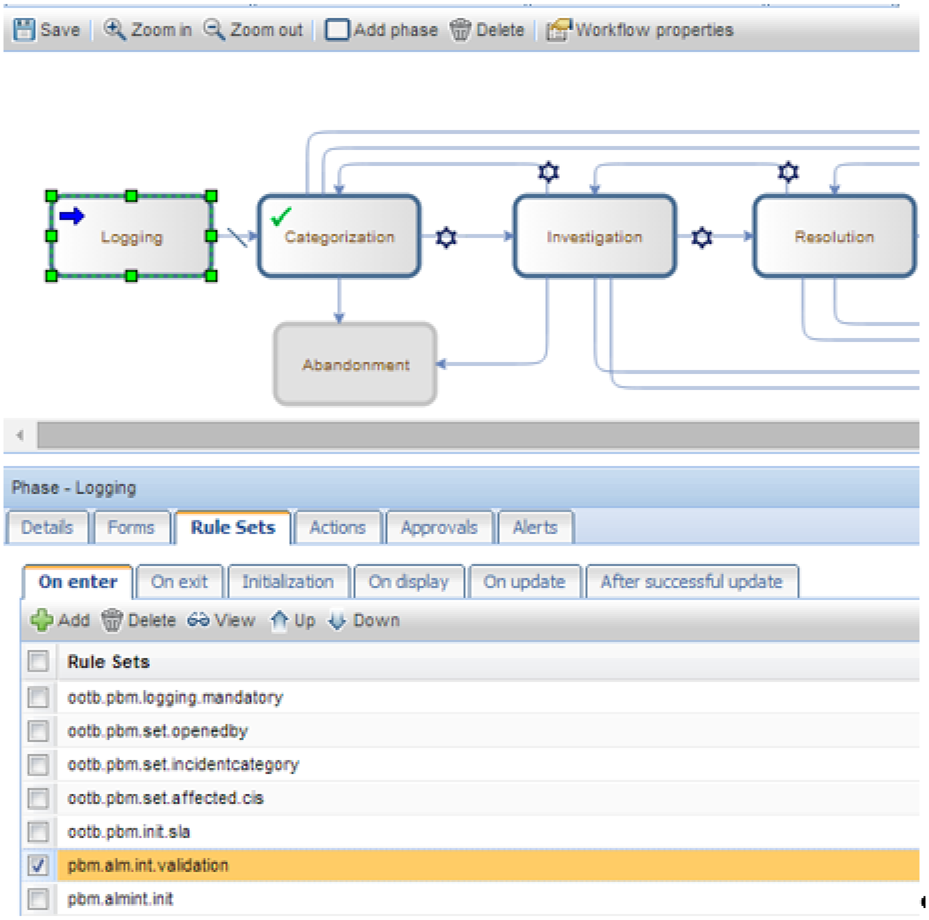
e. Click **Add** and select the initialization rule set you just created.



☐	Rule Sets
☐	ootb.pbm.status.list
☐	ootb.pbm.set.impact.urgency.value
☐	ootb.pbm.logging.init.status
☐	ootb.pbm.initialize.id
☑	pbm.almint.init

12. Repeat steps **11.d.** and **11.e.** for the **On display** tabs.

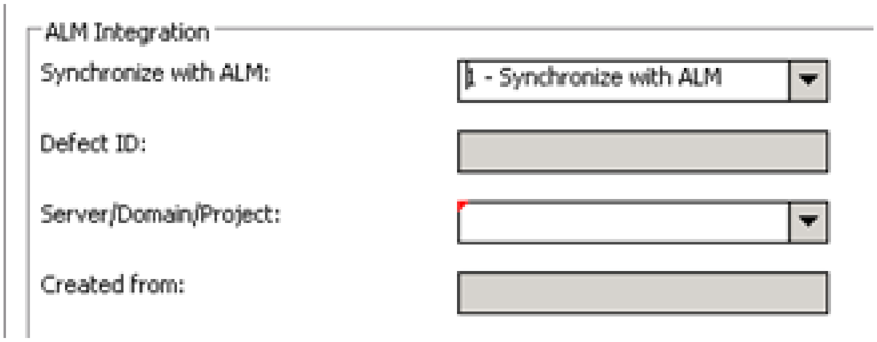
13. Select the **On enter** tab and select the Validation rule set you just created.



☐	Rule Sets
☐	ootb.pbm.logging.mandatory
☐	ootb.pbm.set.openedby
☐	ootb.pbm.set.incidentcategory
☐	ootb.pbm.set.affected.cis
☐	ootb.pbm.init.sla
☑	pbm.alm.int.validation
☐	pbm.almint.init

14. Click **Save**.

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



ALM Integration

Synchronize with ALM:	1 - Synchronize with ALM
Defect ID:	
Server/Domain/Project:	
Created from:	

HPE ALM Synchronizer

To configure the Synchronizer side of the integration:

1. Download and install the latest ALM Synchronizer Server and Client appropriate for the ALM version in use.
2. Download the latest **HP Defects and Requirements Exchange with HPE Service Manager and HPE ALM** package and extract the files from the zip archive.
3. Register ALM client on the Synchronizer client machine by opening http://<*YourAlmServer*>:8080/qcbin/start_a.jsp**?common=true**.
4. Copy all files under the **[smqc_integration_v1.0x]\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
5. Navigate to **Start > All Programs > HP Quality Server Synchronizer > Stop/Start Synchronizer** and restart the Synchronizer service.

6. Edit the following lines in **[smqc_integration_v1.0x]\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
   ```

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

   > **Note:** Check the console output for errors.

   The stub **[smqc_integration_v1.0x]\build\sm-adapter-ws-client.jar** is generated.

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

9. Navigate to **Start > All Programs > HPE 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.

10. Copy the **[smqc_integration_v1.0x]\sample\configuration_file_default.xml** file to **<*QCS_Install_Dir*>\adapters \dat\SM ProblemManagement**.

11. **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:** For example, see **[release-package]\sample\configuration_file_default.xml** in the synchronizer package.

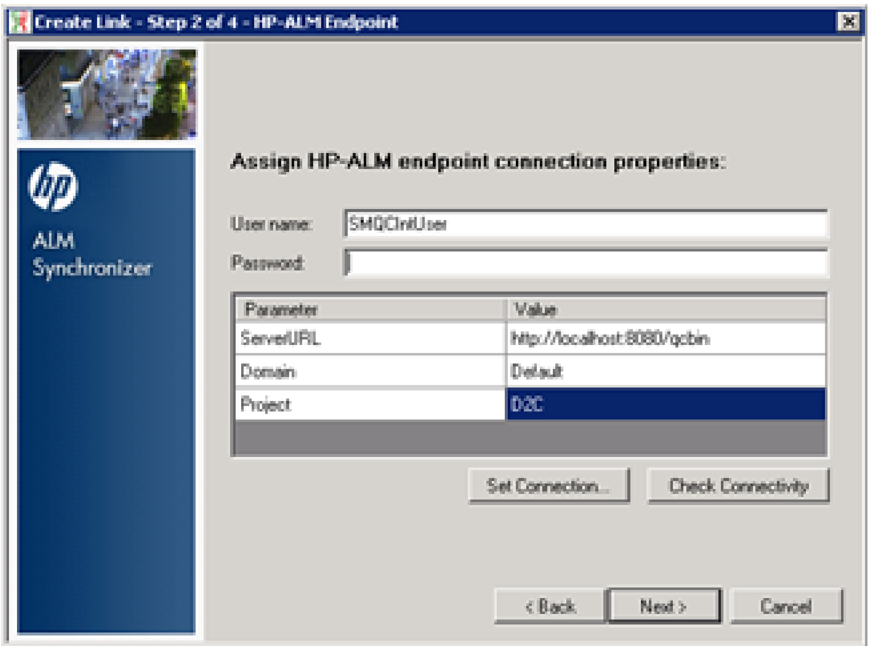
12. Open **HPE ALM Synchronizer Client** and click **Link > Create**.

    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:

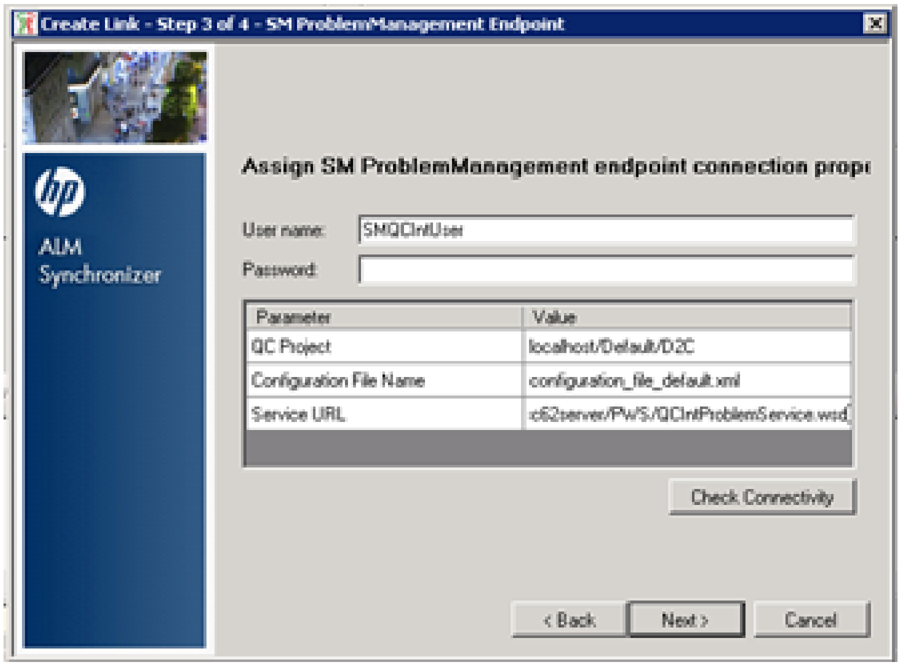
User name: SMQCIntUser

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 prop

User name: SMQCIntUser

Password:

Parameter	Value
QC Project	localhost/Default/D2C
Configuration File Name	configuration_file_default.xml
Service URL	c62server/PWS/QCIntProblemService.wsd

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

Configuration File Name can be found in **<*QCS_Install_Dir*>\adapters \dat\SM ProblemManagement**.

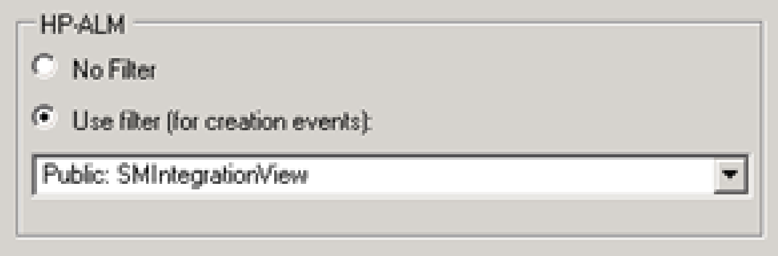
Service URL.http://<*service_manager_ host*>:<port>/sc62server/PWS/QCIntProblemService.wsdl

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.



HP ALM

○ No Filter

● Use filter (for creation events):

Public: SMIntegrationView

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	
		CurrentPhase	Valid phase name, such as **Problem Investigation and Diagnosis**	
		QCProject	YourServer/Domain/	

ALM	Direction	SM	Constant Value	Remarks
			Project	
		WorkFlowType	Valid category name, such as **ITIL**	
Summary	<->	Description		
Severity	<->	Severity		For an example of mapping values, see "Example of Severity Mapping Values:" below.
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

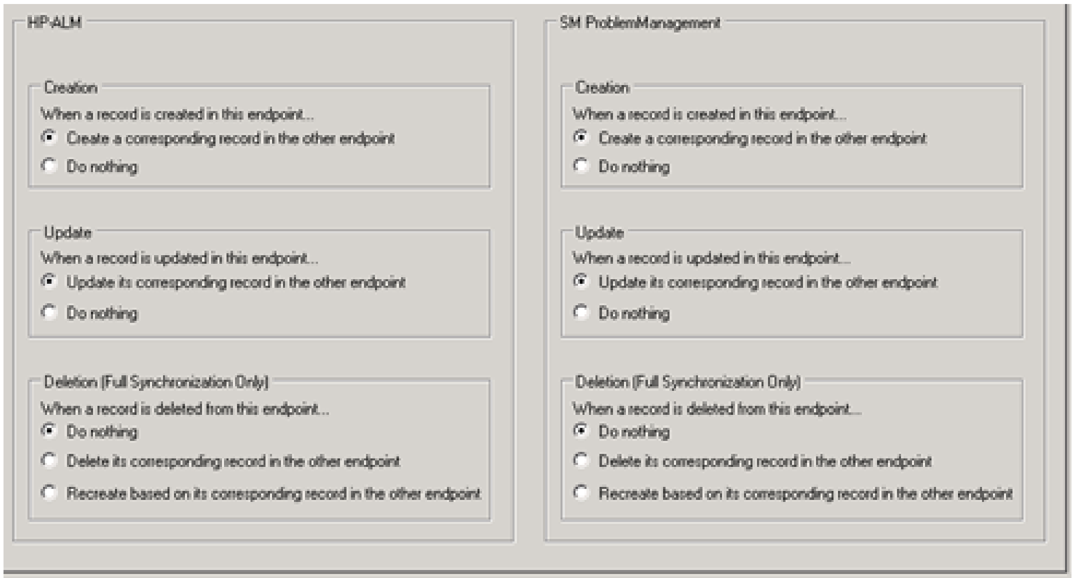
Example of Severity Mapping Values:

HP-ALM Value	Direction	SM ProblemManagement Value
1-Low	<-->	4-User
2-Medium	<-->	3-Multiple Users
3-High	<-->	2-Site/Dept
4-Very High	<-->	1-Enterprise

> **Note:** In a customized environment, additional fields and values may need to be mapped to satisfy entity creation/modification requirements.

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.



HP-ALM

Creation
When a record is created in this endpoint...
● Create a corresponding record in the other endpoint
○ Do nothing

Update
When a record is updated in this endpoint...
● Update its corresponding record in the other endpoint
○ Do nothing

Deletion (Full Synchronization Only)
When a record is deleted from this endpoint...
● Do nothing
○ Delete its corresponding record in the other endpoint
○ Recreate based on its corresponding record in the other endpoint

SM ProblemManagement

Creation
When a record is created in this endpoint...
● Create a corresponding record in the other endpoint
○ Do nothing

Update
When a record is updated in this endpoint...
● Update its corresponding record in the other endpoint
○ Do nothing

Deletion (Full Synchronization Only)
When a record is deleted from this endpoint...
● Do nothing
○ Delete its corresponding record in the other endpoint
○ Recreate based on its corresponding record in the other endpoint

h. Save the configuration.

> **Note:** An integrity check is automatically run.

i. Click **Enable Link**.

j. Run **Full Synchronization**.

Chapter 11: UCMDB – RC Integration Configuration

This chapter includes:

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 contains the following steps:

Prerequisites

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

Deploy the RC Integration Package

To deploy the RC integration package:

1. Copy the rc_package.zip file from **C:\HP\RC920\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

To 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:

Overview

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

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

To add an 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.

To set up RC for integration with SM:

1. Open a remote session with RC.
2. Navigate to **Start > Run > cmd**.
3. Run the command: **C:\hp\RC920\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 wsdl? [n]

     Press **ENTER** for default.

   - Enter Service Manager port [13080].

     Press **ENTER** for default.

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

     Press **ENTER** for default.

   The following confirmation message 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 **Import configuration set** button.
6. Navigate to **<*RC 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

To verify the 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: Security Settings Configuration

This chapter includes:

Overview

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

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

Using LWSSO in a solution simplifies the user’s work flow by avoiding the need to enter authentication details each time the flow passes between the 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.lwsso.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.lwsso.LwSsoIntegration"/>**

4. In the lwssofmconf.xml file located in the WEB-INF\classes folder of the SM Web client deployment, set the following parameters.

    - Set the value of enableLWSSOFramework to true (default is false).

    - ***<domain>.*** Domain name of the server where you deploy your web tier. For example, if your web tier's fully qualified domain name is mywebtier.example.com, then the domain portion is example.com.

    - ***<initString>.*** Password used to connect HP products (minimum length: 12 characters)—for example, smintegrationlwsso. Make sure that this value is the same as that used in the LWSSO configurations of the other HP applications (such as HP OO and BSM) that you want to connect via LWSSO.

    - ***<multiDomain>.*** The <*multiDomain*> element should include the domain names (DNSDomain), server names (NetBiosName), IP addresses (IP), fully-qualified domain names (FQDN) of the SM web tier server and other product servers (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"?>
    <lwsso-config
    xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/2.0">
     <enableLWSSO
      enableLWSSOFramework="true"
      enableCookieCreation="true"
      cookieCreationType="LWSSO"/>

      <webui>

       <validation>
        <in-ui-lwsso>
    ```

```
     <lwssoValidation id="ID000001">
      <domain>example.com</domain>
       <crypto cipherType="symmetricBlockCipher" engineName="AES"
paddingModeName="CBC" keySize="256"
        encodingMode="Base64Url" initString="sample_common_initString"/>
     </lwssoValidation>
    </in-ui-lwsso>

     <validationPoint
       enabled="false"
       refid="ID000001"

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

   </validation>

   <creation>
     <lwssoCreationRef useHTTPOnly="true" secureHTTPCookie="true">
       <lwssoValidationRef refid="ID000001"/>
       <expirationPeriod>50</expirationPeriod>
     </lwssoCreationRef>
   </creation>

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

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

    <multiDomain>
     <trustedHosts>
      <DNSDomain>example.com</DNSDomain>
      <DNSDomain>example1.com</DNSDomain>
      <NetBiosName>myserver</NetBiosName>
      <NetBiosName>myserver1</NetBiosName>

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

  </webui>

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

   <groupIntegration
     groupPrefix=""
```

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

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

   <*SM root directory* > \RUN\lwssofmconf.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 OMi

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

To configure LWSSO in OMi:

1. Log on to OMi as a system administrator.
2. Navigate to **Administration > 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, smintegrationlwsso. Make sure that this value is the same as that used in the LWSSO configurations of the other HP applications (such as HP OO and SM) that you want to connect via LWSSO—for example **sample_common_initString**.
   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 OMi 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, **sample_common_initString**.

    > **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 OMi 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.

Configure LWSSO in BSM (or APM)

The BSM-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 **Administration > Users > 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, **smintegrationlwsso**. Make sure that this value is the same as

that used in the LWSSO configurations of the other HP applications (such as HP OO and 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, **sample_common_initString**.

      > **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 OMi – HP OO Run Book Invocation Integration

To verify the OMi-HP OO run book invocation integration:

1. In the OMi user interface, navigate to **Admin > Operations Console > Run Book Mappings**.
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 OMi to SM Configuration" on page 56), 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 **HPE Lightweight SSO (LWSSO)** and fill in the relevant details.

Parameter	Description
Domain	Network domain name (for example, HP.com)

Parameter	Description
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 14: UCMDB – SAW Integration Configuration

This chapter includes:

Overview

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

The integration between HP Universal CMDB (UCMDB) and HP Service Anywhere (SAW) enables synchronization to automatically update SAW with information gathered from UCMDB using the On-Premise Bridge.

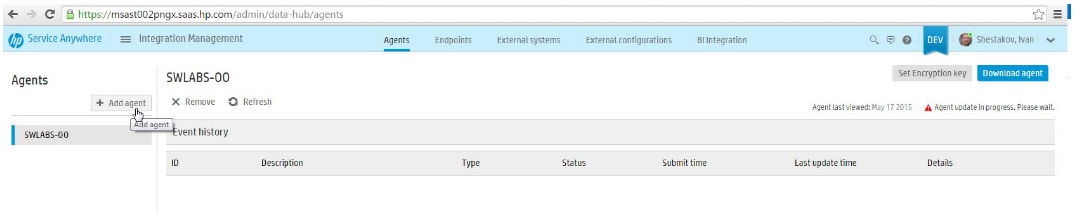
Synchronize CIs Between UCMDB and SAW

This task describes how to set up the CI synchronization between UCMDB and SAW.

> **Note:** This section provides instructions for IT Service Management functions using Software-as-a-Service (SaaS)-based SAW. For integrations using HPE Service Manager (SM), see the UCMDB – SM integration described in the *HPE RTSM Best Practices Guide* (https://softwaresupport.hpe.com/km/KM01996511).

To synchronize CIs between UCMDB and SAW:

1. Download and install the **On-Premise Bridge Agent**.
2. Create an agent.
   a. In SAW, navigate to **My Dashboards**. Under **Administration > Utilities**, select **Integration**.
   b. Click the **Add agent** button.



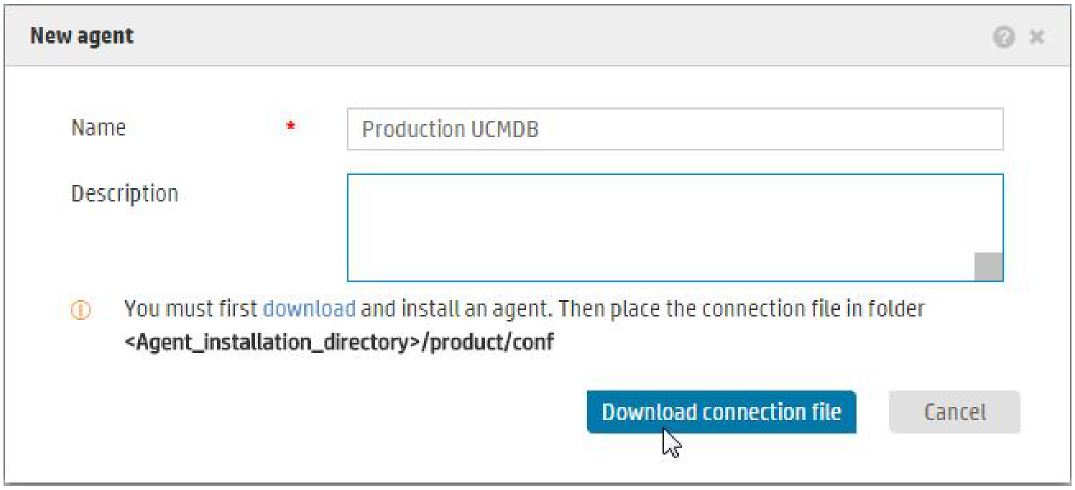
https://msast002pngx.saas.hp.com/admin/data-hub/agents

Agent last viewed: May 17 2015

Agent update in progress. Please wait.

ID	Description	Type	Status	Submit time	Last update time	Details

   c. Fill in the name for the integration agent (for example, **Production UCMDB**) and click the **Download connection file** button.



Name * Production UCMDB

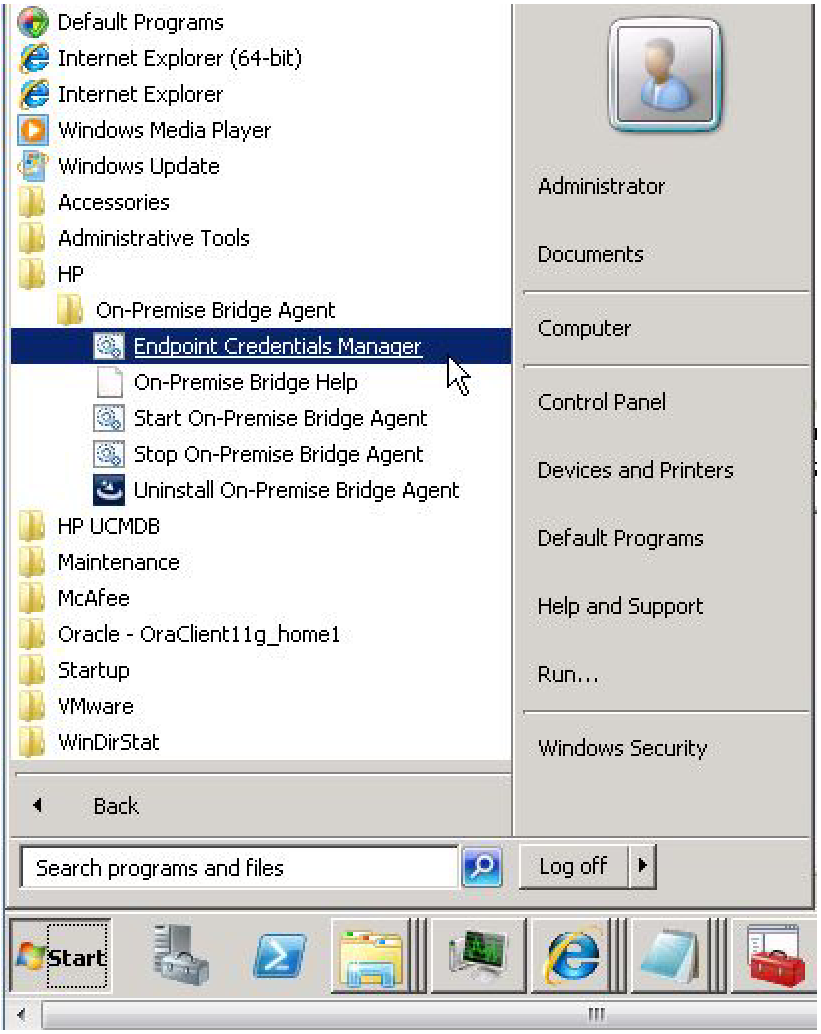
Description

You must first download and install an agent. Then place the connection file in folder <Agent_installation_directory>/product/conf

   d. Follow the on-screen instructions to copy the produced connection file to the Bridge Agent server.
3. Specify the endpoint credentials.

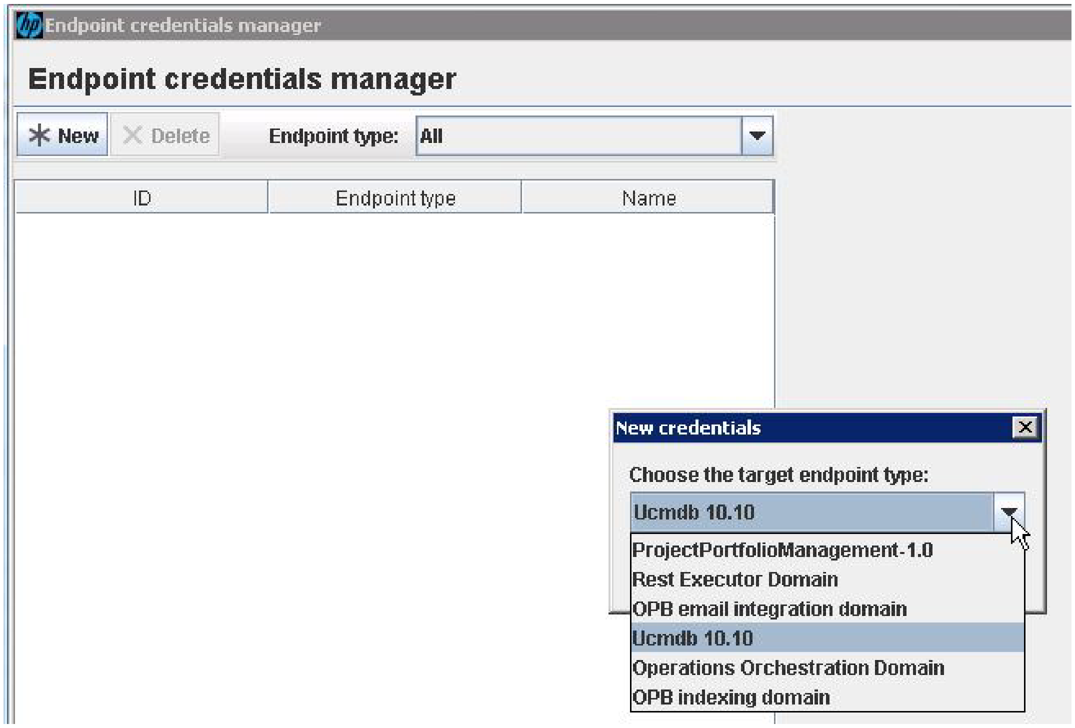
For more information, see *How to specify credentials using the Endpoint Credentials Manager* (https://mslon001pngx.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbCredentialsTool.htm) and *How to specify credentials using a command line tool* (https://mslon001pngx.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbCredentialsCmdLine.htm) in SAW.

a. In the **On-Premise Bridge Agent** machine, navigate to **Start > Programs > HP > On-Premise Bridge Agent > Endpoint Credentials Manager**.



b. In the **Endpoint Credentials Manager** dialog box, click the **New** button.

In the **New credentials** drop-down list, select **UCMDB 10.10** as the target endpoint type.

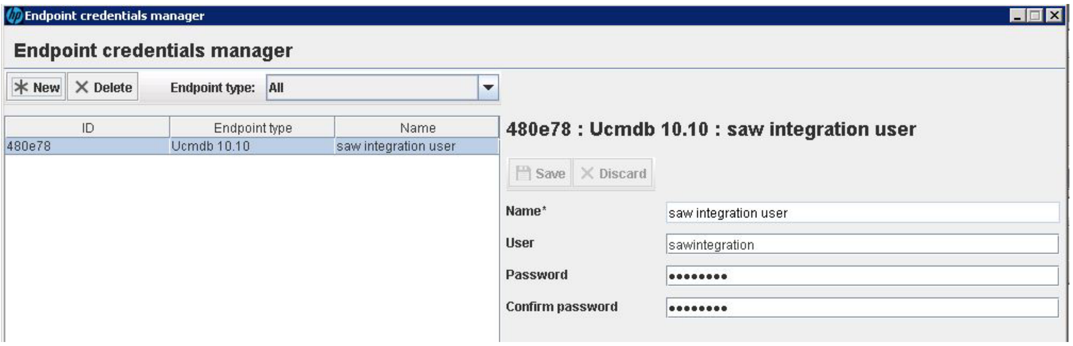


Endpoint credentials manager
Endpoint credentials manager
New
Delete
ID
Endpoint type
Name
New credentials
ProjectPortfolioManagement-1.0
Rest Executor Domain
OPB email integration domain
Ucmdb 10.10
Operations Orchestration Domain
OPB indexing domain

Endpoint type: All

Choose the target endpoint type: Ucmdb 10.10

c. Fill in the credentials for SAW to connect with UCMDB and click the **Save** button.



Endpoint type: All

ID	Endpoint type	Name
480e78	Ucmdb 10.10	saw integration user

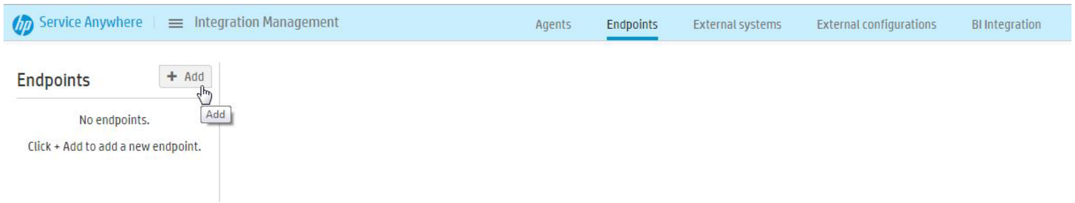
480e78 : Ucmdb 10.10 : saw integration user

Name* saw integration user
User sawintegration
Password ••••••••
Confirm password ••••••••

d. Navigate to **Start > Programs > HP > On-Premise Bridge Agent > Start On-Premise Bridge Agent**. The agent service starts.

4. Create a UCMDB endpoint.

   a. From the main menu, navigate to **Administration > Utilities > Integration > Endpoints** and click **+Add**.



No endpoints.

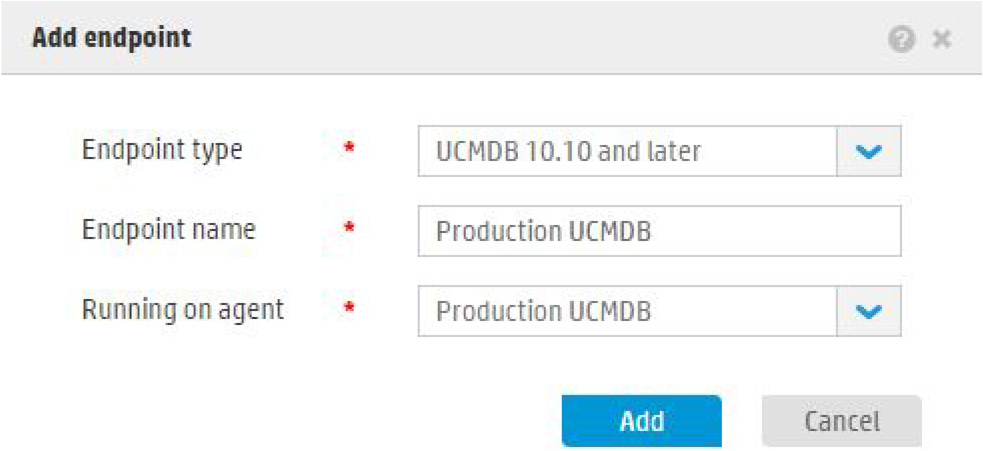
Click + Add to add a new endpoint.

   b. Enter the endpoint details.

> **Note:** You must complete all fields marked with a red asterisk *.

Field label	Description
Endpoint type (*)	Select the relevant UCMDB version
Endpoint name (*)	Type a name for the endpoint. Use only Latin letters and spaces.
Running on agent (*)	Select the agent (installed in step 1 of this task) from the drop-down list

   c. Click **Add**.



Endpoint type * UCMDB 10.10 and later

Endpoint name * Production UCMDB

Running on agent * Production UCMDB

5. Configure the endpoint.

   a. Click **Configure**. The Endpoint Configuration dialog box opens.

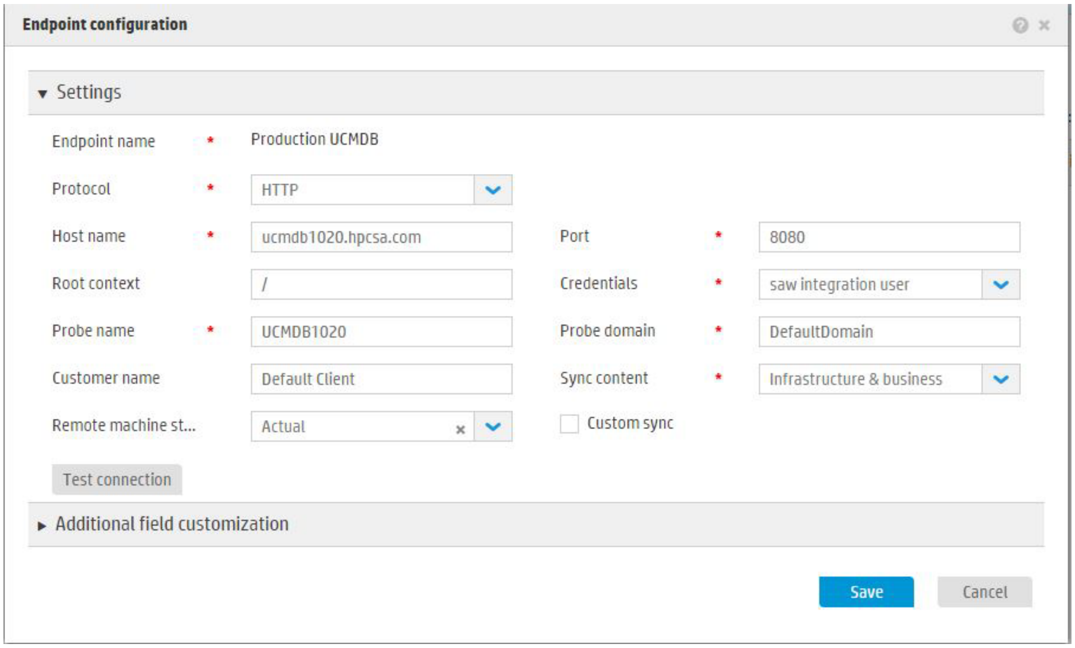
   b. Enter the endpoint details.

> **Note:** You must complete all fields marked with a red asterisk *.

Field	Description
Endpoint name (*)	Name of the endpoint **Note:** This field is read-only.
Protocol (*)	Select the protocol to be used for connecting to the on-premise UCMDB installation. Valid values are **HTTP** or **HTTPS**.
Host name	Type the name or IP address of the on-premise UCMDB server.
Port (*)	Type the number of the port listened to by the UCMDB API. The default is **8080**.
Root context	Type the root context value of the on-premise UCMDB installation. If no root context has been defined, leave this field with its default value.
Credentials (*)	Choose the credentials to be used to connect to the UCMDB installation from the drop-down list. The full credentials are those defined as part of the agent to which the endpoint is connected.
Probe name (*)	Type the name of the UCMDB probe on which to run the synchronization. The default is Integration **Service**.
Probe domain (*)	Domain of the probe as defined in UCMDB
Sync content (*)	Select whether to synchronize only infrastructure entities, or infrastructure and business entities.
Customer name	Type the customer name.
Remote machine state	Select the state with which you want to connect when integrating with multi-state UCMDBs. Valid values are **Actual State** or **Authorized State**. The default is **Actual State**.
Custom sync	Check this check box to run in custom synchronization mode. Automatic synchronization mode is the default mode.
Additional field customization	You can define additional fields to synchronize. Click **+Add** to add a row for each additional set of fields. Select the **Service Anywhere** record type and field from the drop-down lists on the left and enter the **UCMDB CI type** attribute name (not the display label) on the right. **Note:** The **Additional field customization** works for automatic synchronization only. To customize field mappings for manual

Field	Description
	synchronization, see *How to tailor custom synchronization* (https://mslon001pngx.saas.hp.com/v4/help/en/full/Content/1900_WebServices/wsManualSyncCustomization.htm).

c. Click **Save**.



Endpoint configuration

▾ Settings

Endpoint name *	Production UCMDB		
Protocol *	HTTP		
Host name *	ucmdb1020.hpcsa.com	Port *	8080
Root context	/	Credentials *	saw integration user
Probe name *	UCMDB1020	Probe domain *	DefaultDomain
Customer name	Default Client	Sync content *	Infrastructure & business
Remote machine st...	Actual	□ Custom sync	

6. Click **Sync Now**. The push job runs immediately.

   In addition, the push job runs according to the scheduler in UCMDB—the default that is set every hour.

   In UCMDB, the push adapter that is deployed and the integration point that is created include the tenant ID as a prefix—for example, **100000001_SACMPushAdapter and 100000001_test_endpoint**, where **100000001** is the tenant ID.

   When performing a synchronization with a Discovery probe (not an Integration Service) in UCMDB Version 10.10 or 10.11, proceed as follows:

   a. Click the **Sync Now** button and wait until it fails.

   b. Shut down the **Discovery Probe** service.

c. In the **UCMDB Discovery Probe** file system, go to the following folder: **DataFlowProbe\runtime\probeManager\discoveryResources\SACMPushAdapter** and delete the following files:

   i. **api-integration.jar**

   ii. **api-interfaces.jar**

d. Start the **Discovery Probe** service. Wait a few minutes for the probe to start.

e. In **Service Anywhere**, go to **Integration > Endpoints** and click **Sync Now**.

For subsequent on-demand synchronizations:

- If you want the agent to synchronize only the delta, click **Sync Now**.
- If you want a full synchronization, click **Request Full Sync**. This is equivalent to running the integration job within UCMDB.

You can see a record of the data pushed in the **fcmdb.push.all.log** file in the **<DataFlowProbe>\runtime\log** folder.

7. View broken relationships.

   A broken relationship occurs when the relationship was synchronized before data about one or both of its ends was available. The relationship is automatically synchronized to Service Anywhere once the missing data arrives.

To view the broken relationships from your synchronization:

1. On the **Endpoints** tab, select the endpoint used in your synchronization.
2. Click **More > View broken relationships**. The table displays the broken relationships.
3. If you do not expect a relationship to be synchronized, you can dismiss it. Select the relationships to dismiss and click **Dismiss from list**.
4. To view details about a broken relationship, in the **Details** column, click the **Show details** link.

Chapter 15: OMi – SAW Integration Configuration

This chapter includes:

Overview

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

The HPE Operations Manager i (OMi) Integration Pack for HPE Service Anywhere (SAW) enables you to automatically open Incidents in SAW when specific Events arrive at HPE OMi.

This new integration provides a framework to create Incidents in SAW based on Events in OMi. For example, you could use the integration to configure OMi events triggered by configuration item (CI) status alerts in OMi and SLM, or EUM alerts in APM (forwarded to OMi), to automatically open a corresponding Incident in SAW.

Alerts are mapped to Events using the Event template, so that each triggered alert forwards a corresponding Event to OMi. The OMi Event Management console determines which Events should generate Incidents and be added to an ITSM process to resolve the Incident and alert agents and end users.

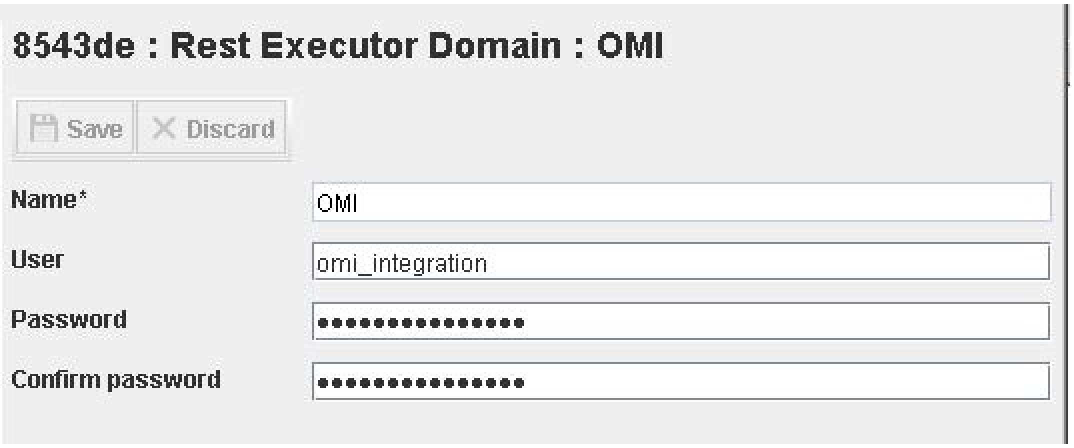
Configure the OMi Integration with SAW

> **Note:** Best Practices suggests creating a user account for the purpose of integrating OMi with SAW. Create a SAW integration user and log-in using the credentials you defined.
>
> This section provides instructions for IT Service Management functions using Software-as-a-Service (SaaS)-based SAW. For integrations using HPE Service Manager (SM), see "OMi – SM Incidents Exchange Integration" on page 48.

To configure the OMi integration with SAW:

1. Download and install the **On-Premise Bridge Agent** and use the **Endpoint Credentials Manager** to specify the OMi credentials.

   For more information, see *Download and install the On-Premise Bridge Agent* (https://msast002pngx.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbUseAgent.htm#DownAgent).

   8543de : Rest Executor Domain : OMI

   Name* OMI

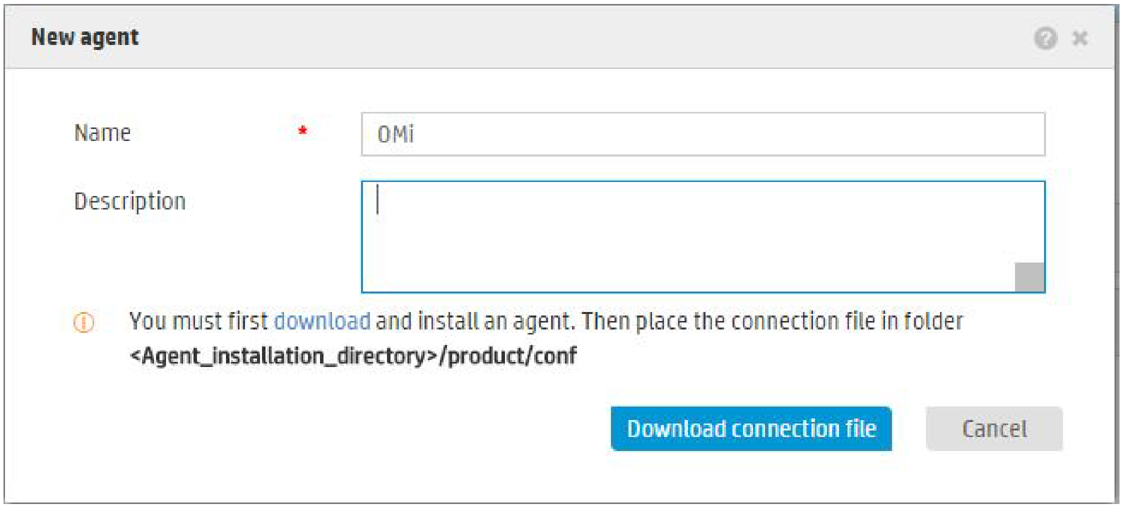
   User omi_integration

   Password ●●●●●●●●●●●●●●●

   Confirm password ●●●●●●●●●●●●●●●

2. Add an agent and deploy the agent's **server-connections.conf** file to the On Premise Bridge.

   For more information, see *Add an agent* (https://saw.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbUseAgent.htm#AddAgent).

   New agent

   Name * OMi

   Description

   You must first download and install an agent. Then place the connection file in folder <Agent_installation_directory>/product/conf

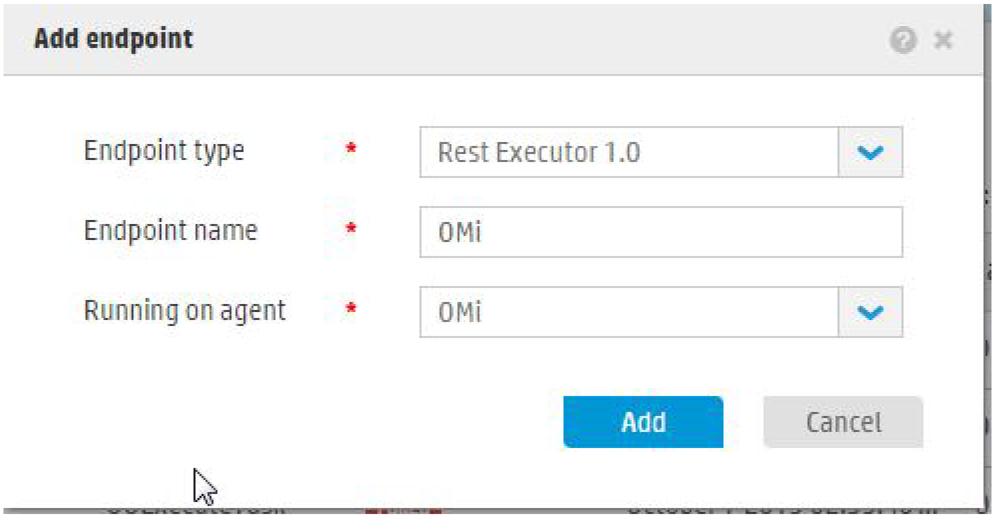
   a. Click the **Download connection file** button, and copy the downloaded file to the appropriate folder on the **On-Premise Bridge Agent** machine.

b. In **<Agent_installation_directory/product/util/opb>**, execute the **AgentAuthentication.bat** script to set up SAW credentials that will be used to authenticate the agent.

AgentAuthentication.bat setAuth –user <sample user name> -pass <sample password>

c. Restart **Agent Service**.

3. Create an endpoint and configure it. Select **REST Executor 1.0** as the endpoint type.



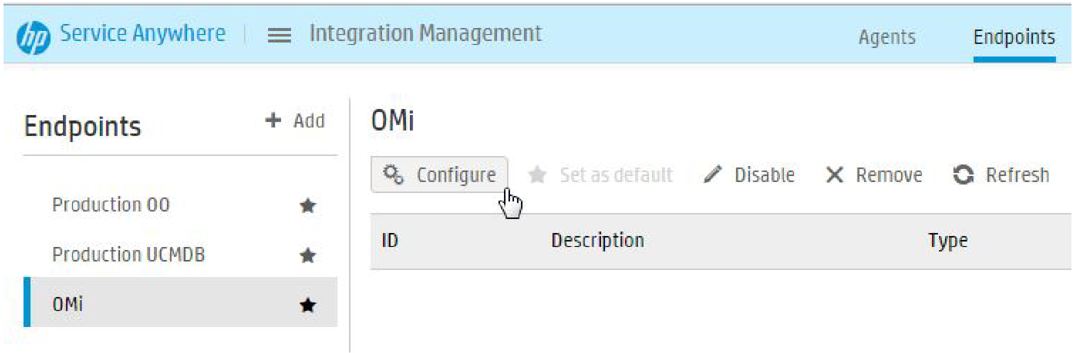
Add endpoint

Endpoint type * Rest Executor 1.0

Endpoint name * OMi

Running on agent * OMi

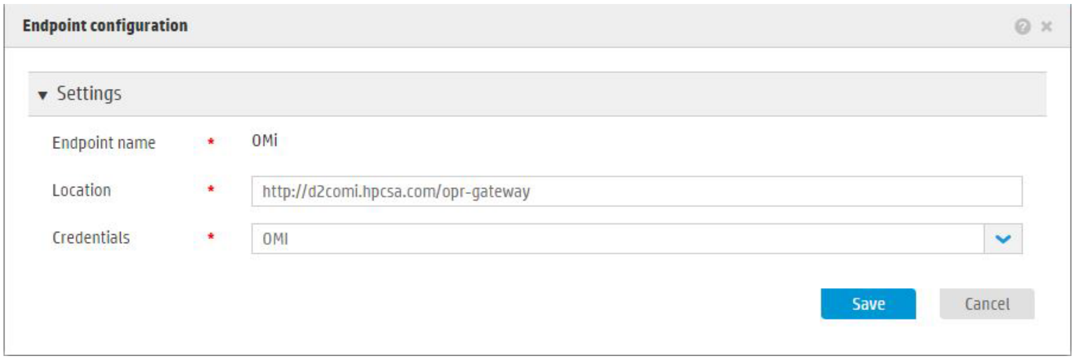
a. Click **Configure**.



b. For the **Location** field, enter the URL for the OMi server. The URL should end with **/opr-gateway/**—for example, **http://sample.omi.hostname/opr-gateway/**.

> **Note:** The available values for the **Credentials** field come from the credentials defined in the On-Premise Bridge. As a result, the drop-down list of values may not appear immediately.

For more information, see *How to use endpoints* (https://saw.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbUseEndpoints.htm).



Endpoint configuration

▾ Settings

Endpoint name * OMi

Location * http://d2comi.hpcsa.com/opr-gateway

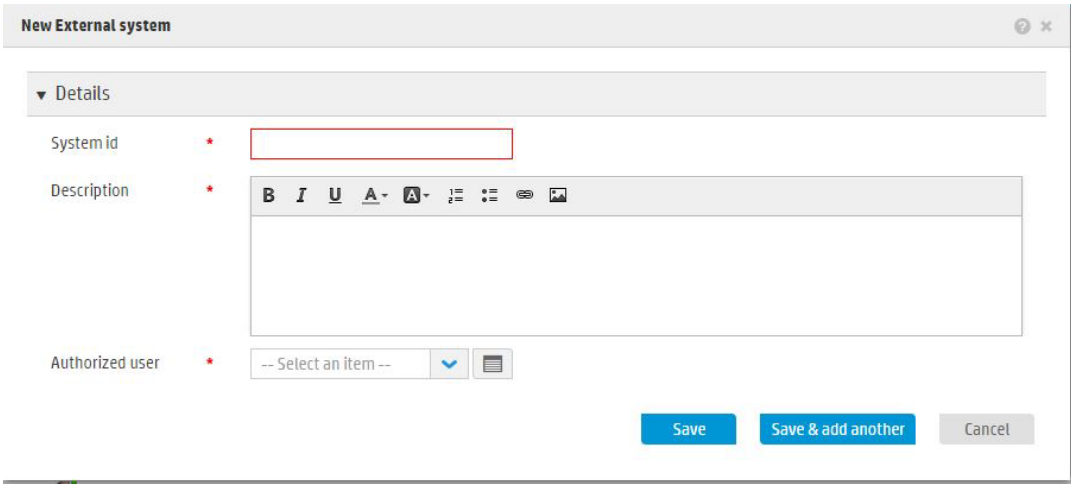
Credentials * OMI

4. Add an external system record for your OMi integration. For the Authorized user, select the user account for this integration.

   For more information, see *Working with external systems*

   (https://saw.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbHow2ExternalSystems.htm)
   .

   a. Go to **Integrations Management**. Select the **External Systems** tab and click the **New** button.



New External system

▾ Details

System id *

Description *

Authorized user * -- Select an item --

   b. Fill in the details and click **Save**.

5. Apply the external predefined configuration to the external system you created:

   a. Select the external system and click **Edit**.

   b. Select the endpoint created in step 3.

   c. Click **Apply configuration** and select the **OMi 9.2x** configuration. Click **Confirm**.

   d. Click **Save**. The changes to the external system are saved.

6. Download the **OMi Groovy** script and documentation from *HPE Live Network* (https://hpln.hpe.com/home).

   To download the script:

   a. Access the *HPE Live Network OMi page* (https://hpln.hpe.com/group/operations-manager-i-omi). You may need to log in with your HPE Passport.

   b. Under Integrations, select **HP Service Anywhere**.

   c. Click the **Download** button to download **ServiceAnywhereAdapter.groovy** (appropriate for OMi version in use).

   d. Select **OMI_SAW_integration.pdf** and **ServiceAnywhereAdapter_<your OMi version>.groovy** and download the files.

7. Edit the script for integration with SAW. The following table displays the parameters to be edited:

Parameter	Description	Required/Optional
SAW_TENANTID	Service Anywhere tenant ID	Required
EXTERNAL_ SYSTEM_ID	System ID of the OMi external system (which you entered when you defined the external system in Service Anywhere)	Required
BSM_ ADMINISTRATOR_ LOGIN_NAME	Default User Principal Name (UPN) to be used for the **RequestedBy** property of system-generated Incidents	Required
DESCRIPTION	Default description used for the created Incident when no description is entered for the Event	Optional
COMPLETION_ CODE	Completion code to use when posting a solution from the Event to the Incident. The default value is **SuccessfulDiagnosis**.	Optional
URGENCY	Defines the **Severity** of the Incident in SAW when the property is not specified for the Event	Optional
IMPACT_SCOPE	Defines the **Impact** of the Incident in SAW when	Optional

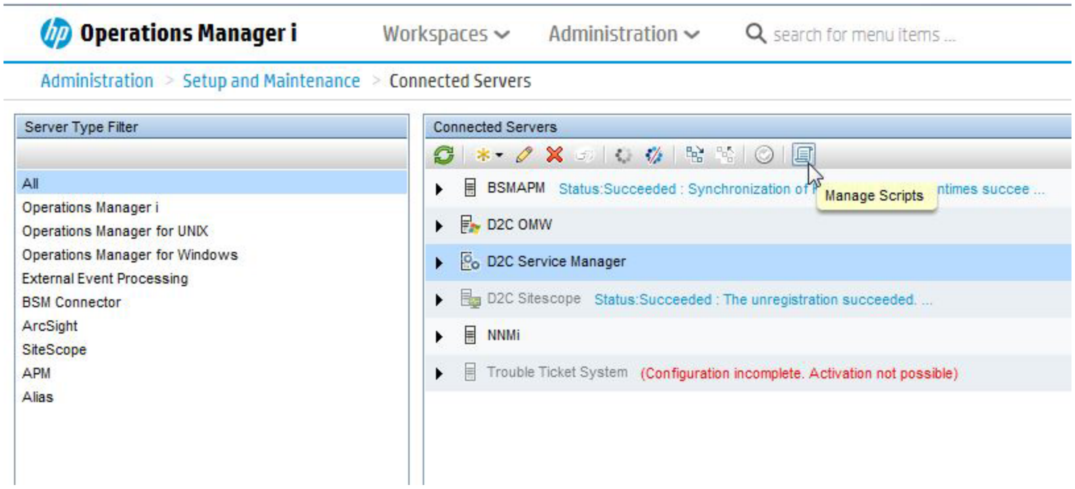
Parameter	Description	Required/Optional
	the property is not specified for the Event	
SERVICE	Defines the **Service** of the Incident in SAW when the property is not specified for the Event	Optional
SERVICE_DESK_ GROUP	Defines the **Service desk group** of the Incident in SAW when the property is not specified for the Event	Optional
CATEGORY	Defines the **Category** of the Incident in SAW when the property is not specified for the Event	Optional

8. Use this edited script to create a new **Groovy Script Adapter** within OMi.

   For more information, see the OMi documentation.

   a. In the OMi user interface, navigate to **Administration** > **Setup** > **Connected Servers** to view the Connected Servers configuration screen.

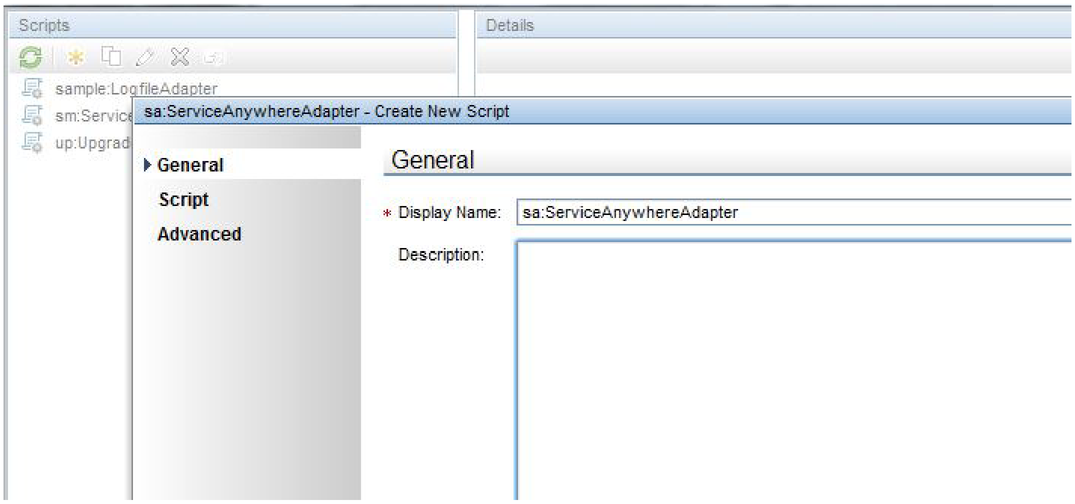
   b. In the Connected Servers pane, click the **Manage Scripts** icon.


Operations Manager i
Workspaces
Administration
search for menu items ...
Administration > Setup and Maintenance > Connected Servers
Server Type Filter
All
Operations Manager i
Operations Manager for UNIX
Operations Manager for Windows
External Event Processing
BSM Connector
ArcSight
SiteScope
APM
Alias
Connected Servers
Manage Scripts

BSMAPM Status:Succeeded : Synchronization of ... ntimes succee ...
D2C OMW
D2C Service Manager
D2C Sitescope Status:Succeeded : The unregistration succeeded. ...
NNMi
Trouble Ticket System (Configuration incomplete. Activation not possible)

   c. Click the **New Item** icon. The **sa:ServiceAnywhereAdapter – Create New Script** dialog box opens.

d. Enter the Display Name **sa:ServiceAnywhereAdapter** and click **Next**.



* Display Name: sa:ServiceAnywhereAdapter

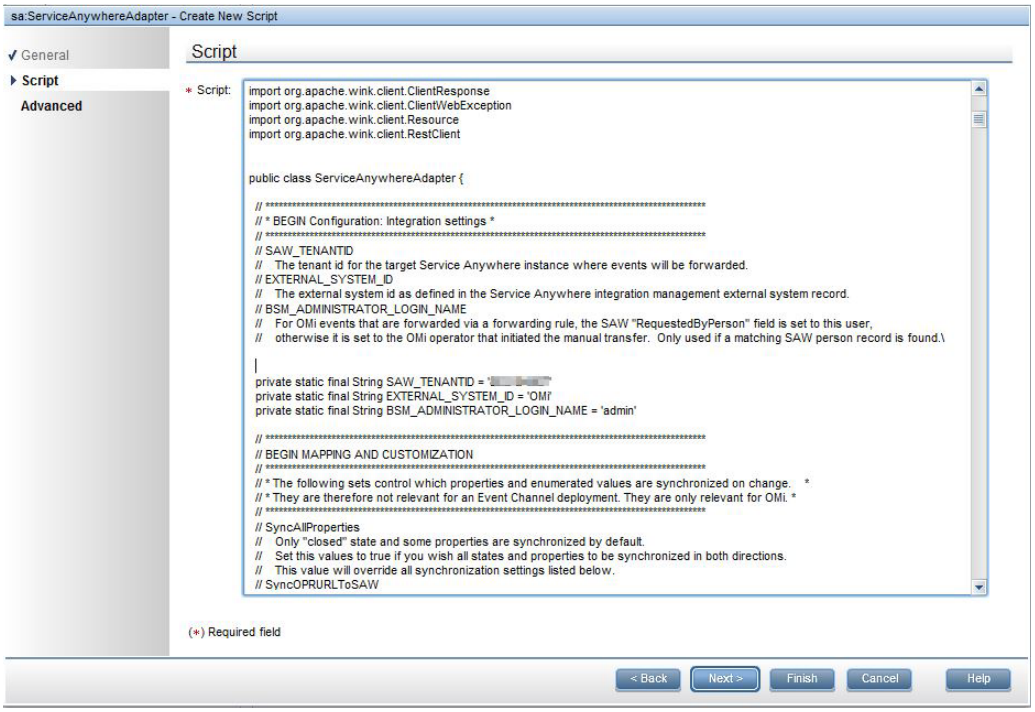
Description:

e. Replace the default script with the contents of the downloaded **ServiceAnywhereGroovyAdapter**.

f. Edit the following integration settings (located just after the import statements at the top of the script):

- **SAW_TENANTID.** Set to the Tenant ID of your Service Anywhere Instance. It is located at the bottom right corner of the Main Menu in Service Anywhere.

- **EXTERNAL_SYSTEM_ID.** Set to the System ID defined in the External System Record created in step 4a.



```
import org.apache.wink.client.ClientResponse
import org.apache.wink.client.ClientWebException
import org.apache.wink.client.Resource
import org.apache.wink.client.RestClient


public class ServiceAnywhereAdapter {

 // ******************************************************************************************
 // * BEGIN Configuration: Integration settings *
 // ******************************************************************************************
 // SAW_TENANTID
 //    The tenant id for the target Service Anywhere instance where events will be forwarded.
 // EXTERNAL_SYSTEM_ID
 //    The external system id as defined in the Service Anywhere integration management external system record.
 // BSM_ADMINISTRATOR_LOGIN_NAME
 //    For OMi events that are forwarded via a forwarding rule, the SAW "RequestedByPerson" field is set to this user,
 //    otherwise it is set to the OMi operator that initiated the manual transfer.  Only used if a matching SAW person record is found.\

 |
 private static final String SAW_TENANTID = '[redacted]'
 private static final String EXTERNAL_SYSTEM_ID = 'OMi'
 private static final String BSM_ADMINISTRATOR_LOGIN_NAME = 'admin'

 // ******************************************************************************************
 // BEGIN MAPPING AND CUSTOMIZATION
 // ******************************************************************************************
 // * The following sets control which properties and enumerated values are synchronized on change.    *
 // * They are therefore not relevant for an Event Channel deployment. They are only relevant for OMi. *
 // ******************************************************************************************
 // SyncAllProperties
 //    Only "closed" state and some properties are synchronized by default.
 //    Set this values to true if you wish all states and properties to be synchronized in both directions.
 //    This value will override all synchronization settings listed below.
 // SyncOPRURLToSAW
```

g. Click **Next**.

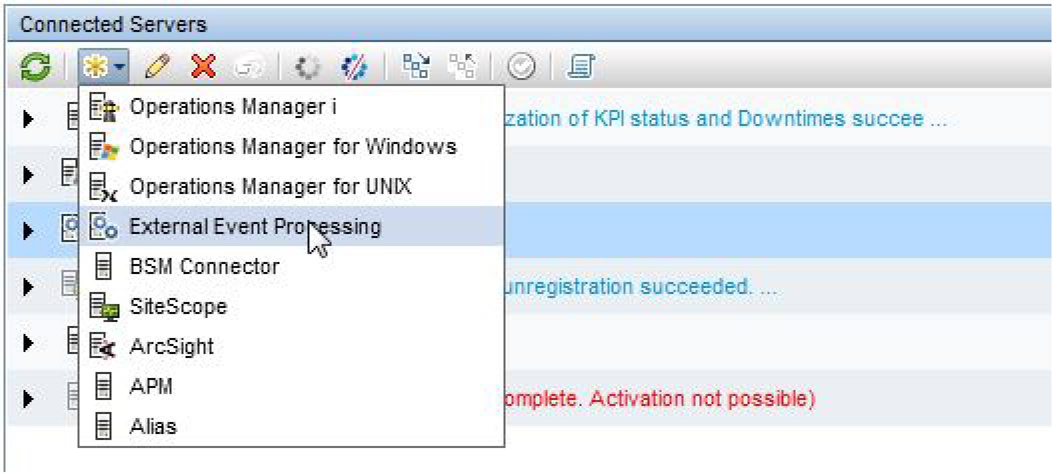
h. Set the Timeout to **6000ms** and click **Finish**.

9. In OMi, define Service Anywhere as a connected server. The outgoing connection credentials used should match the credentials of the authorized user in the external system record. The incoming connections credentials should match the credentials specified in the **Endpoint Credentials Manager** in step 1.

   The standard SSL ports and Service Anywhere SSL certificates should be used for a secure connection.

   a. In the OMi user interface, navigate to **Administration** > **Setup** > **Connected Servers** to view the Connected Servers configuration screen.

b. Click the **New** icon and select **External Event Processing**from the drop-down list.


Connected Servers
Operations Manager i
Operations Manager for Windows
Operations Manager for UNIX
External Event Processing
BSM Connector
SiteScope
ArcSight
APM
Alias
zation of KPI status and Downtimes succee ...
unregistration succeeded. ...
omplete. Activation not possible)

c. In the **Display Name** field, enter the desired name for Service Anywhere. By default, the **Name** field is filled automatically. For example, if you enter **Service Anywhere 1** as the Display Name for Service Anywhere, **Service_Anywhere_1** is automatically inserted in the **Name** field. You can specify a custom name in the **Name** field in place of the default name.

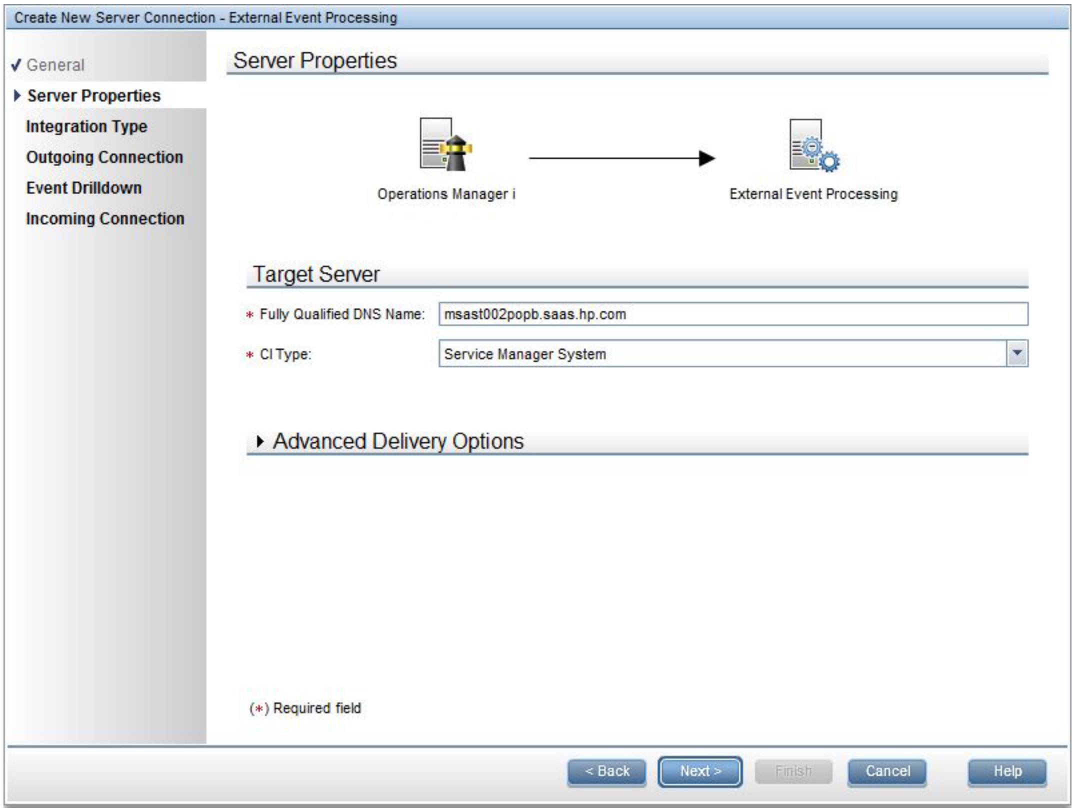
   Optional: Enter a description for the new target server.

d. Check the **Active** check box and click **Next**.

e. Fill in the Fully Qualified DNS Name (FQDN) for the Service Anywhere instance.

f. Review the **server-connection.conf** file for the hostname.

g. In **CI Type** drop-down box, select **Service Manager** and click **Next**.

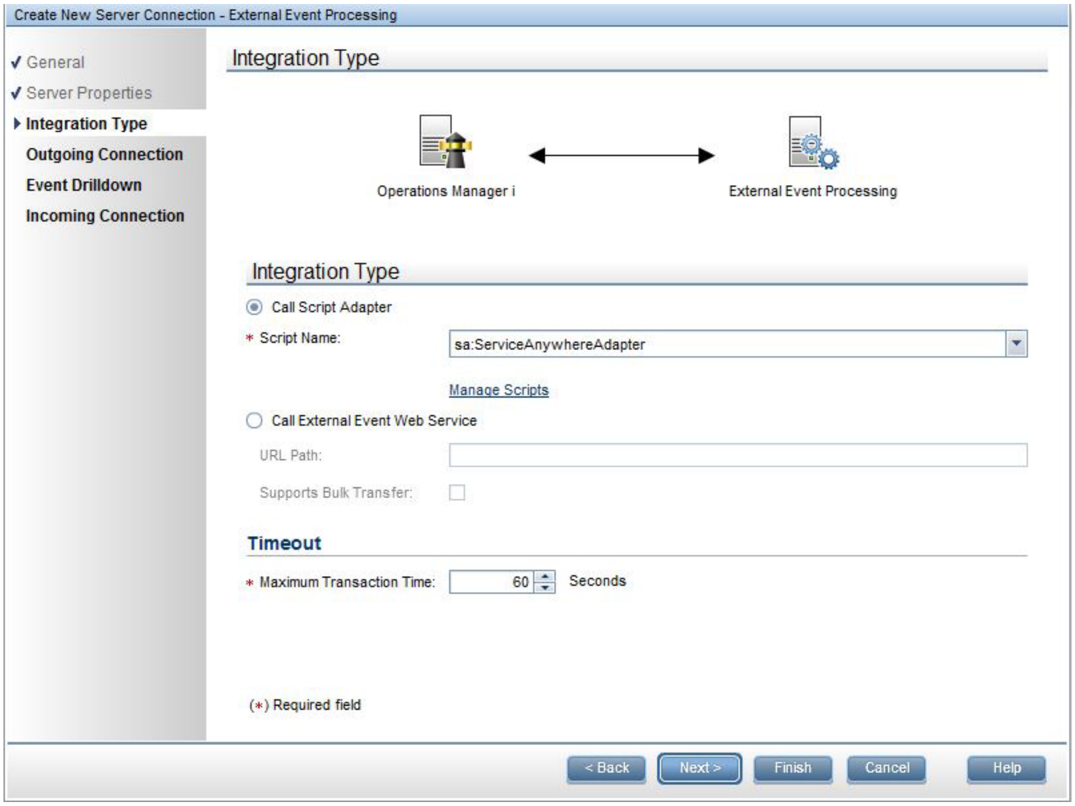


* Fully Qualified DNS Name: msast002popb.saas.hp.com

* CI Type: Service Manager System

(*) Required field

h. In the **Call Script Adapter** drop-down menu, select **sa:ServiceAnywhereAdapter** and click **Next**.



Create New Server Connection - External Event Processing

Integration Type

● Call Script Adapter

* Script Name: sa:ServiceAnywhereAdapter

Manage Scripts

○ Call External Event Web Service

URL Path:

Supports Bulk Transfer: □

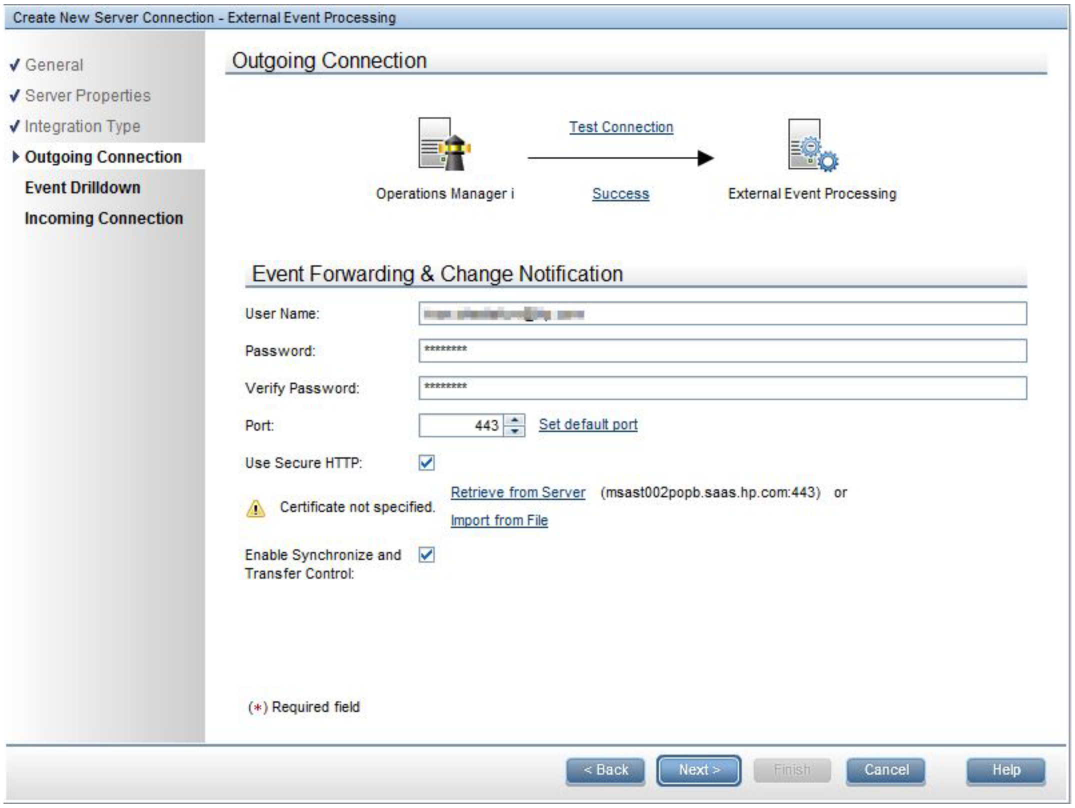
Timeout

* Maximum Transaction Time: 60 Seconds

(*) Required field

i. Fill in Service Anywhere credentials and click **Test Connection** found under **Outgoing Connection** above the arrow between the two servers.

If the test connection is successful (as shown in the screen shot that follows), check **Enable Synchronize and Transfer Control** and click **Next**.



Outgoing Connection

Event Forwarding & Change Notification

User Name: [redacted]

Password: ********

Verify Password: ********

Port: 443

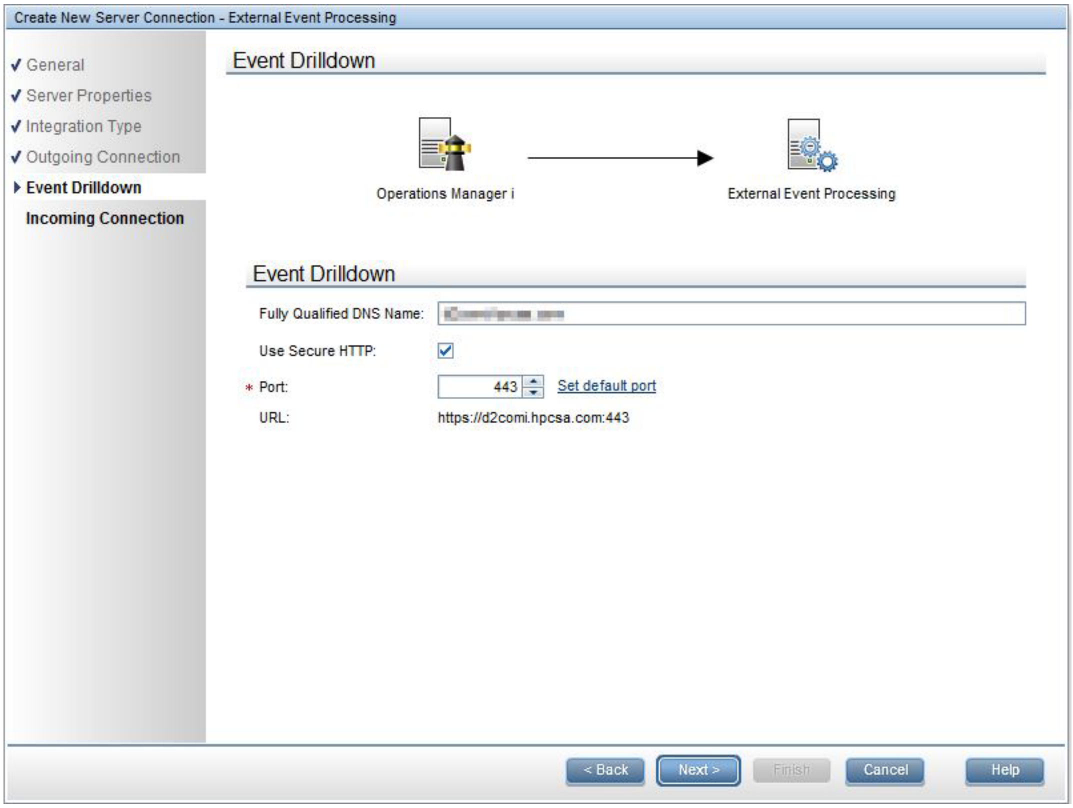
Use Secure HTTP: ☑

Certificate not specified. Retrieve from Server (msast002popb.saas.hp.com:443) or Import from File

Enable Synchronize and Transfer Control: ☑

(*) Required field

j. In the **Event Drilldown** dialog box, fill in the Service Anywhere host and select the appropriate port for access. The default is SSL enabled with Port 443.



Create New Server Connection - External Event Processing

Event Drilldown

Event Drilldown

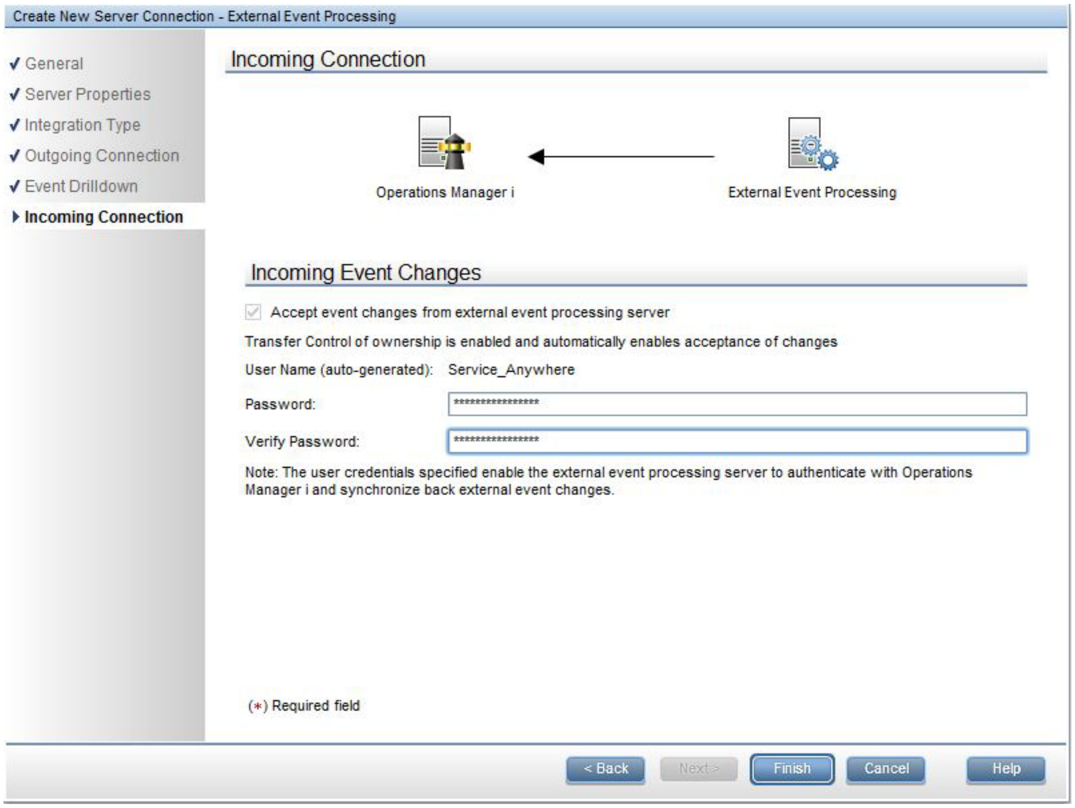
Fully Qualified DNS Name: [redacted]

Use Secure HTTP: ☑

* Port: 443 Set default port

URL: https://d2comi.hpcsa.com:443

k. In the **Incoming Event Changes** dialog box, fill in a password value for the auto-generated user name and click **Finish**.



Incoming Event Changes

☑ Accept event changes from external event processing server

Transfer Control of ownership is enabled and automatically enables acceptance of changes

User Name (auto-generated): Service_Anywhere

Password: ****************

Verify Password: ****************

Note: The user credentials specified enable the external event processing server to authenticate with Operations Manager i and synchronize back external event changes.

(*) Required field

l. In OMi, configure an **Event Forwarding Rule** that includes configuring a filter to determine which Events trigger Incidents in Service Anywhere.

m. When an Incident is created, you can click a link from the Event in OMi to launch Service Anywhere and go to the created Incident. Use your Service Anywhere credentials to log in.

> **Note:** If you make a change to an Incident in the **Resolution** metaphase in Service Anywhere, it will be reflected in OMi.
>
> In the **General** tab of the Incident, go to the **External assignment** section. Click the URL link next to the OMi remote system to launch OMi and go directly to the Event. The Event details should be updated.

Chapter 16: Execute HPE OO Flows from SAW

This chapter includes:

Overview

> **Note:** IT Service Management functions can be implemented using either an HPE Service Manager product (on premise) or using Software-as-a-Service (SaaS)-based HPE Service Anywhere.

The integration of HPE Operations Orchestration (OO) with HPE Service Anywhere (SAW) provides a robust solution for automation needs. The automation of task plans is now extended to include run book flows that execute on premise, including actions such as patch deployments, application execution management, system resets, user password resets, and more.

HPE OO provides the most robust run book automation solution in the industry, including out-of-the-box, ready-to-use, scenarios as well as an extensive automation flow creation editor.

This integration provides you with

- Direct access content from HPE Operations Orchestration and ability to execute flows as an automatic task in a record
- Simple configuration using business rules in any task plan—for example from Change, Incident, Catalog, Problem, and other Service Anywhere records
- Point-and-click configuration that maps Service Anywhere data into OO flow parameters
- Visual tracking of OO flow execution within the context of Service Anywhere task plans
- Mapping and use of OO flow output results as Service Anywhere task plan data

Import OO Content and Execute the Flows

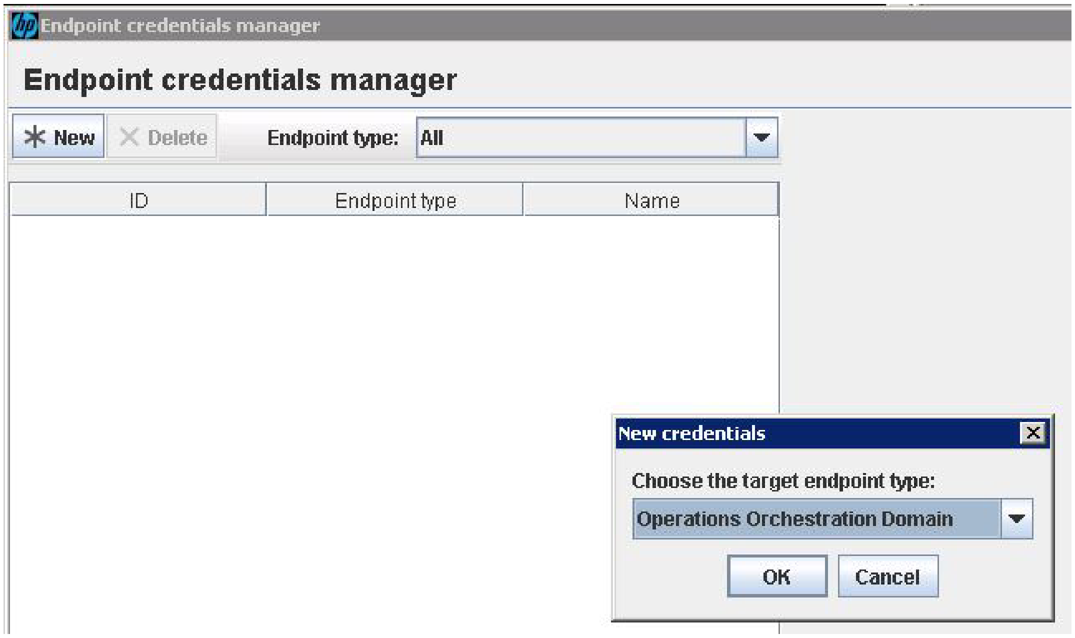
> **Note:** This section provides instructions for IT Service Management functions using Software-as-a-Service (SaaS)-based SAW. For integrations using HPE Service Manager (SM), see "Execute HPE OO Flows from SM" on page 68.

To import Operations Orchestration content and execute the flows:

1. Follow InstallAnywhere's instructions to download, install, and configure the **On-Premise Bridge Agent** for the integration.

   For more information, see How to use On-Premise Bridge agents to synchronize data (https://saw.saas.hp.com/v4/help/en/full/Content/Platform/plfrmOpbUseAgent.htm).

   a. In **Start** > **Programs** > **HP** > **On-Premise Bridge Agent**, open **Endpoint Credentials Manager** and add an endpoint with the **Operations Orchestration Domain** type.



Endpoint credentials manager

Endpoint credentials manager

ID	Endpoint type	Name

New credentials

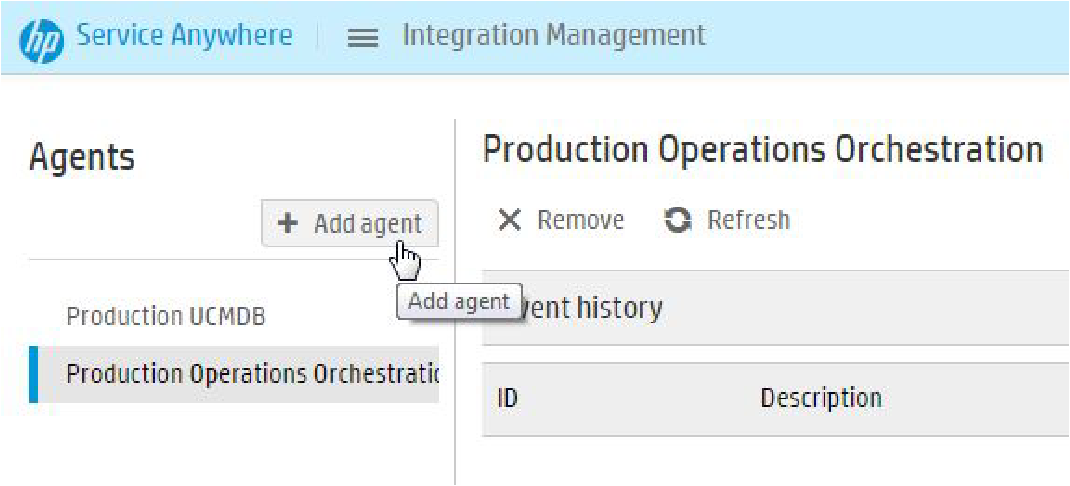
Choose the target endpoint type: Operations Orchestration Domain

   b. Fill in the credentials for the HPE OO user and click **Save**.

   c. Exit **Endpoint Credentials Manager**.

   d. In Service Anywhere's main menu, select **Administration** > **Utilities** > **Integration Management**.

e. Click the **Agents** tab. In the left pane, click the **Add Agent** button.



f. Fill in the agent's name and click the **Download connection file** button.

g. As instructed, copy the downloaded file to **On-Premise Bridge Agent** < **Agent_installation_directory>/product/conf**.

h. Navigate to **Start** > **All Programs** > **HP** > **On-Premise Bridge Agent** > **Start On-Premise Bridge Agent** and start the On-Premise Bridge Agent service.

2. If the HPE OO flow you are importing uses encryption, you must set up encryption between Service Anywhere and the On-Premise Bridge Agent before you perform the integration.

   For more information, see How to set up encryption for an Operations Orchestration integration (https://msast002pngx.saas.hp.com/v4/help/en/full/Content/1000_GettingStarted/gs_taskplans_OO_encryption.htm).

   a. Generate the encryption keys.

      In the On-Premise Bridge Agent machine, navigate to **C:\Program Files\HP\On-Premise Bridge Agent\product\util\opb directory** and run the following script:

      rsa_key_gen.bat

      The script generates a public key, **id_rsa.pub**, and a private key, **id_rsa.priv**. The keys are located in the same directory by default.

   b. Enter the public key in Service Anywhere.

      i. From the main menu, select **Administration** > **Utilities** > **Integration**. Click the **Agents** tab.

      ii. Click **Set encryption key**.

iii. Copy the public key you created, **id_rsa.pub**, and paste it in the Encryption key dialog box.

iv. Click **Save** to save the key.

c. Import the encryption keys on the On-Premise Bridge Agent machine(s).

i. In the **C:\Program Files\HP\On-Premise Bridge Agent\product\util\opb** directory on the On-Premise Bridge Agent machine, navigate to and run the following script using the keys as the parameters:

import_rsa_keys.bat –pub id_rsa.pub -priv id_rsa.priv

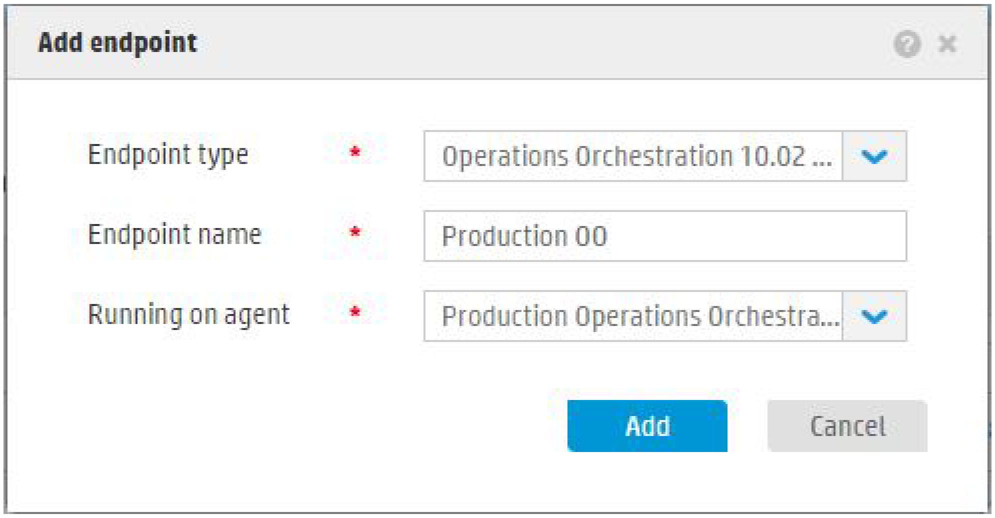
After you import the keys, restart the On-Premise Bridge Agent service.

3. In Service Anywhere, add an Operations Orchestration endpoint.

a. From the main menu, select **Administration** > **Utilities** > **Integration Management**.

b. Click the **Endpoints** tab.

c. Above the lists of endpoints in the left-hand pane, click the + Add button. The Add endpoint dialog box opens.



Add endpoint

Endpoint type * Operations Orchestration 10.02 ...

Endpoint name * Production OO

Running on agent * Production Operations Orchestra...

d. Enter the endpoint details. For the endpoint type, select **Operations Orchestration** and click the **Add** button.

4. Configure the endpoint.

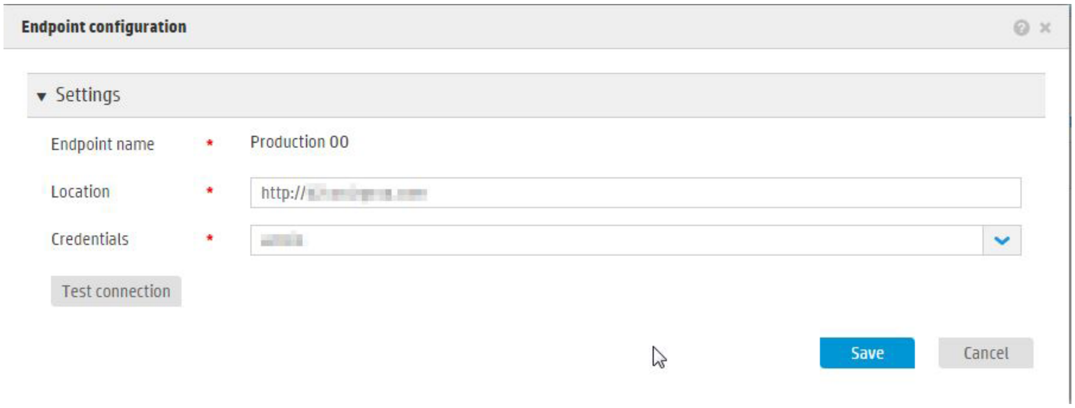
a. From the main menu, select **Administration** > **Utilities** > **Integration**. Click the **Endpoints** tab.

b. Click **Configure**. The Endpoint Configuration dialog box opens.

c. Enter the endpoint details.

d. Click the **Test connection** button to test the connection to the server.

You must complete all fields marked with a red asterisk *.



Endpoint name * Production OO

Location * http://[redacted]

Credentials * [redacted]

Field	Description
End point name (*)	The name of the endpoint. **Note:** This field is read-only.
Location (*)	Type the URL of the Operations Orchestration server in the format **http://<server>:<port>**
Credentials (*)	The list of credentials is populated automatically. Service Anywhere queries the OPB agent for the list of credential records that were created in the Endpoint Credentials Manager. If no credentials are received, there may be a problem with agent setup and authentication with Operations Orchestration.

Chapter 17: SM – SAW Incident Case Exchange

This chapter includes:

Overview

Some customers may be in a situation where there are several IT Service Management solutions implemented in an organization. This happens, for instance, when a specific line of business (LOB) uses HPE Service Anywhere (SAW) to manage IT processes, while others use HPE Service Manager (SM) for the same purpose.

For such scenarios, it is recommended to implement a mechanism that enables exchanging Incidents—specifically in the Detect-to-Correct context—between Service Manager and Service Anywhere instances.

This chapter provides instructions for configuring such an integration based on an out-of-the-box setup for both products.

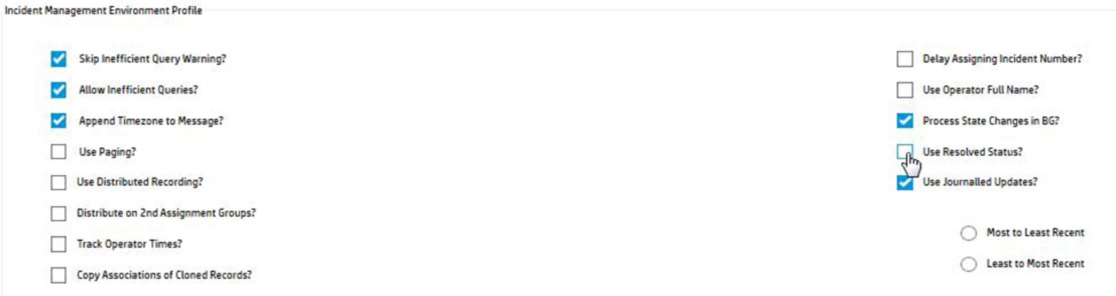
For more information, see the System Administration chapter in the Service Manager Help Server (https://softwaresupport.hpe.com/km/KM01824172).

Configure Incident Environment

We recommend that you enable the **Use Resolved Status** setting in the Service Manager system.

To enable the Use Resolved Status setting:

1. Go to **Incident Management > Administration > Environment**.
2. Select **Use Resolved Status?**



Incident Management Environment Profile

☑ Skip Inefficient Query Warning?
☑ Allow Inefficient Queries?
☑ Append Timezone to Message?
□ Use Paging?
□ Use Distributed Recording?
□ Distribute on 2nd Assignment Groups?
□ Track Operator Times?
□ Copy Associations of Cloned Records?

□ Delay Assigning Incident Number?
□ Use Operator Full Name?
☑ Process State Changes in BG?
□ Use Resolved Status?
☑ Use Journalled Updates?

○ Most to Least Recent
○ Least to Most Recent

3. Click **Save**.
4. Click **OK**.

Add an Integration Instance in SM

To add the Case Exchange integration between SM and SAW:

1. Click **Tailoring > Integration Manager**.

   The **Integration Instance Manager** opens.
2. Click **Add**. The **Integration Template Selection** wizard opens.
3. From the Integration Template list, select **CaseExchangeSM_SAW** and select the **Import Mapping** check box. Click **Next**.
4. Complete the fields on the **Integration Instance Information** page as necessary. Click **Next**.

5. On the **Integration Instance Parameters** page, configure the following settings in the **General** tab and use the default setup for all of the other settings.

   - **Base URL.** The base URL of the Service Anywhere API. The format of the URL is: **https://<SAAS Portal Server>**.
   - **Login URL.** The login URL of Service Anywhere. The format of the URL is: **<Base URL>/auth/authentication-endpoint/authenticate/login**.
   - **Tenant Id.** The Tenant Id of the Service Anywhere system. For more information about Tenant Id, refer to Service Anywhere documentation.
   - **User Name and Password.** The credentials of the Service Anywhere account for this integration.

6. Click **Next**.

   The **Integration Instance Fields** page opens.

7. Modify the fields in the **SM Fields** and **Endpoint Fields** tabs as necessary. Otherwise, go to the next step.

8. Click **Next**.

   The **Integration Instance Mapping** page opens.

9. Locate the **Service ID** of an existing service in SAW. Go to the **PostScript** tab and update **10019** with that **Service ID**, as displayed in the following out-of-the-box code. This will be used by default for Incident creation.

   ```
   if (context.outbound) {

       context.action = mapObj["ext_properties.Operation"];

       //set the default value of required Master Data when create the ticket

       if(context.action=="Create") {

           mapObj["properties.RegisteredForActualService"]="10019";

           //set the default service

   }
   ```

10. Click **Finish**.

Enable an Integration Instance in Service Manager

To enable the integration instance:

1. Click **Tailoring > Integration Manager**.

   The **Integration Instance Manager** opens.

2. Select the integration instance that you want to enable.

3. Click **Enable**.

4. Click **Yes**.

Configure Case Exchange Rule Sets

This section contains the following topics:

Before you start to configure a Case Exchange Rule Set, make sure the configuration of the fields mapping in the related integration instance is complete.

The Case Exchange Rule Set is introduced so that customers can easily trigger Case Exchange outbound events.

It is not supported to trigger Case Exchange activities by using Rule Sets that are not provided.

For more information about how to configure Case Exchange Rule Sets, see the following topics in **Online Help**:

- **System Administration > Application Setup > Process Designer > Create a rule set**
- **System Administration > Application Setup > Process Designer > Adding a rule > Add a Case Exchange rule**

The following is an example rule set that works in an out-of-the-box non-customized environment. In a customized environment, additional modifications will be required to achieve the desired behavior.

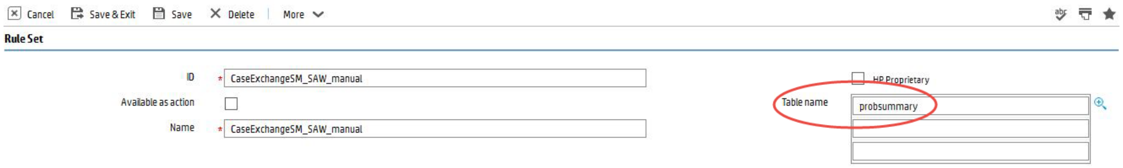
Add a Case Exchange Rule Set

To create a rule set that will define the Incident Case Exchange functionality:

1. **Navigate to Tailoring > Process Designer > Rule Sets**.
2. Enter the **ID** and **Name** for the rule set.

   > **Note:** Note these details for use later in the "Apply Customized Workflow to Incident Module" on page 154 module.

3. For the **Table name**, enter **probsummary**.



Rule Set

ID	* CaseExchangeSM_SAW_manual
Available as action	□
Name	* CaseExchangeSM_SAW_manual
	□ HP Proprietary
Table name	probsummary

4. Click the **Save** button.

Add Case Exchange Rules

This rule enables you to trigger certain activities for the Case Exchange integration.

To add a Case Exchange rule:

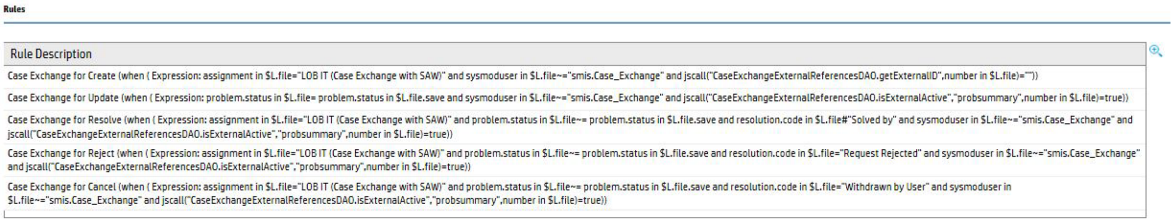
1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule as defined in "Add a Case Exchange Rule Set" above.
3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Case Exchange**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

   > **Note:** If you do not specify a condition, the value defaults to **Always**.

6. In the rule from the **Instance Name** drop-down list, select the Case Exchange integration instance that you want to apply.
7. Select an event from the **Event** drop-down list and select the fields you want to add.
8. Click **Finish** to add the new rule to the rule set.

Repeat steps 1-8 above to create additional rules to handle the various events.

The end result looks as follows:



Rules

Rule Description
Case Exchange for Create (when (Expression: assignment in $L.file="LOB IT (Case Exchange with SAW)" and sysmoduser in $L.file~="smis.Case_Exchange" and jscall("CaseExchangeExternalReferencesDAO.getExternalID",number in $L.file)=""))
Case Exchange for Update (when (Expression: problem.status in $L.file= problem.status in $L.file.save and sysmoduser in $L.file~="smis.Case_Exchange" and jscall("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true))
Case Exchange for Resolve (when (Expression: assignment in $L.file="LOB IT (Case Exchange with SAW)" and problem.status in $L.file~= problem.status in $L.file.save and resolution.code in $L.file#"Solved by" and sysmoduser in $L.file~="smis.Case_Exchange" and jscall("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true))
Case Exchange for Reject (when (Expression: assignment in $L.file="LOB IT (Case Exchange with SAW)" and problem.status in $L.file~= problem.status in $L.file.save and resolution.code in $L.file="Request Rejected" and sysmoduser in $L.file~="smis.Case_Exchange" and jscall("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true))
Case Exchange for Cancel (when (Expression: assignment in $L.file="LOB IT (Case Exchange with SAW)" and problem.status in $L.file~= problem.status in $L.file.save and resolution.code in $L.file="Withdrawn by User" and sysmoduser in $L.file~="smis.Case_Exchange" and jscall("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true))

The following table provides example outbound rules that work in the out-of-box Service Manager system. You may modify these rules according to the workflow in your system.

Condition (RAD expression)	Event
`assignment in $L.file="<external_assignment_group>" and sysmoduser in $L.file~="<smis_scheduler_name>" and jscall ("CaseExchangeExternalReferencesDAO.getExternalID",number in $L.file)=""`	Create
`problem.status in $L.file= problem.status in $L.file.save and sysmoduser in $L.file~="<smis_scheduler_name>" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true`	Update
`assignment in $L.file="<external_assignment_group>" and problem.status in $L.file~= problem.status in $L.file.save and resolution.code in $L.file#"Solved by" and sysmoduser in $L.file~="<smis_scheduler_name>" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true`	Resolve
`assignment in $L.file="<external_assignment_group>" and problem.status in $L.file~= problem.status in $L.file.save and resolution.code in $L.file="Request Rejected" and sysmoduser in $L.file~="<smis_scheduler_name>" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true`	Reject
`assignment in $L.file="<external_assignment_group>" and problem.status in $L.file~= problem.status in $L.file.save and resolution.code in $L.file="Withdrawn by User" and sysmoduser in $L.file~="<smis_scheduler_`	Cancel

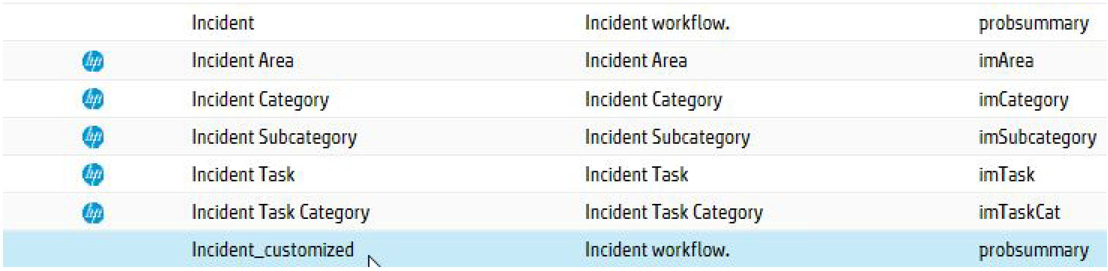
Condition (RAD expression)	Event
`name>" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true`	

Invoke Case Exchange Rule Sets

On a Service Manager system that has Process Designer implemented, you can invoke a Rule Set from a workflow phase. If Process Designer is not implemented, see the **Invoke Rule Sets from triggers** section in the Service Manager Help Server.

To invoke a Rule Set from a workflow phase:

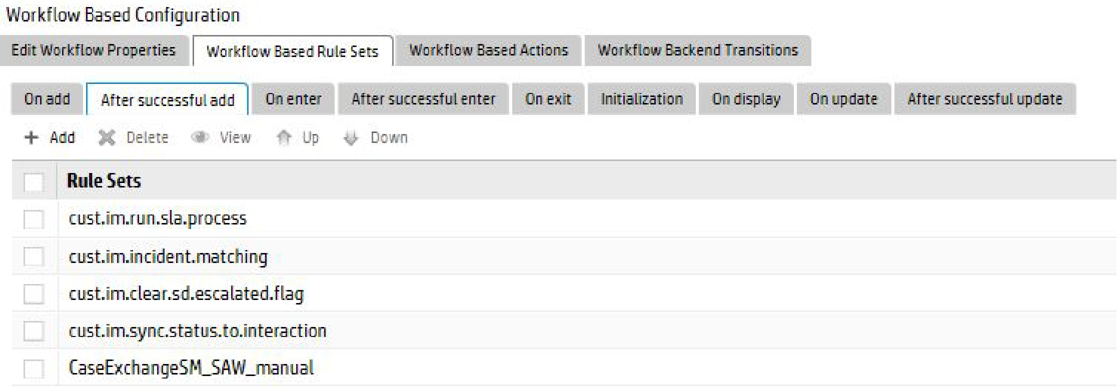
1. Click **Tailoring > Process Designer > Workflows** from the System Navigator. The workflows list opens.
2. Select the workflow in which you want to invoke a Rule Set. For Incident Management, select **Incident**, as it is an HP-provided rule, and save its copy with a different name—for example, **Incident_customized**.



Incident	Incident workflow.	probsummary
Incident Area	Incident Area	imArea
Incident Category	Incident Category	imCategory
Incident Subcategory	Incident Subcategory	imSubcategory
Incident Task	Incident Task	imTask
Incident Task Category	Incident Task Category	imTaskCat
Incident_customized	Incident workflow.	probsummary

3. Click the **Edit Workflow Properties** button and select the **Workflow Based Rule Sets** tab.
4. In the following tabs, according to your needs, add the Rule Set created in "Configure Case Exchange Rule Sets" on page 150.

> **Note:** In an out-of-the-box setup, **After successful add** and **After successful update** is suggested.



□	Rule Sets
□	cust.im.run.sla.process
□	cust.im.incident.matching
□	cust.im.clear.sd.escalated.flag
□	cust.im.sync.status.to.interaction
□	CaseExchangeSM_SAW_manual

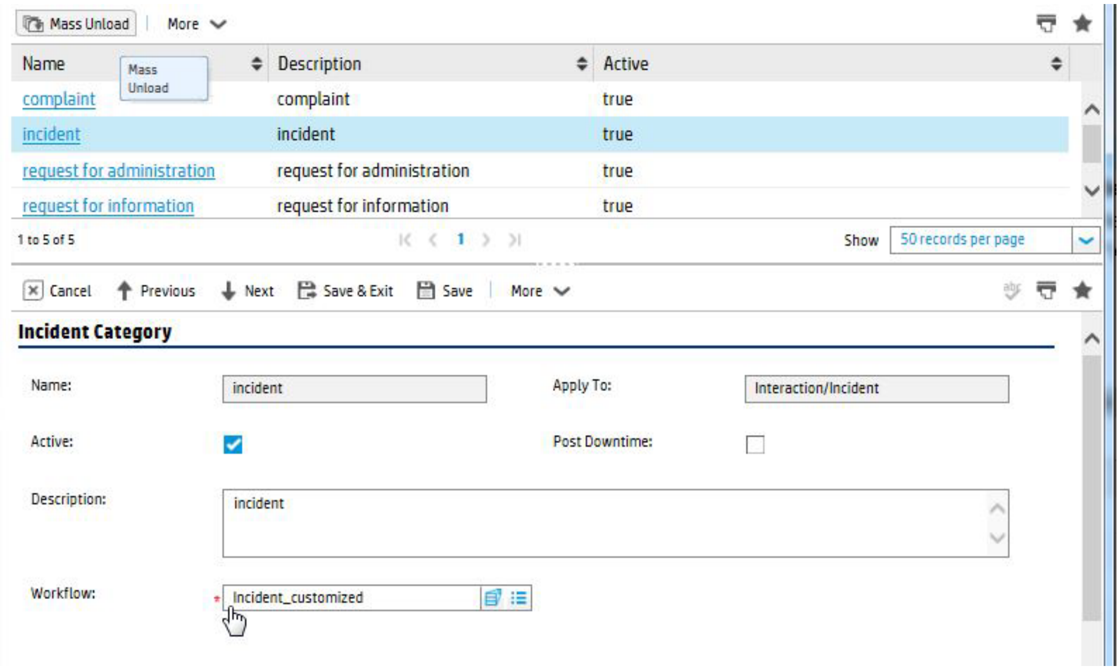
5. Save the workflow.

Apply Customized Workflow to Incident Module

The modified workflow that supports Case Exchange must be enabled for the appropriate Incident category. This example describes the settings for all Incidents.

To apply a customized workflow to an Incident Module:

1. In the main menu, select **Incident Management > Incident Categories**.
2. Search for **Incident**, and select the customized workflow created in "Configure Case Exchange Rule Sets" on page 150.



Name	Description	Active
complaint	complaint	true
incident	incident	true
request for administration	request for administration	true
request for information	request for information	true

1 to 5 of 5 — Show 50 records per page

Incident Category

Name: incident
Apply To: Interaction/Incident
Active: ☑
Post Downtime: □
Description: incident
Workflow: * Incident_customized

3. Click **Save & Exit**.

Configure an Integration Instance in SAW

Before you can exchange records between SM and SAW, perform the following configuration in SAW:

1. Confirm your user account has the **SACM Integration** role assigned.
2. Add an external system.

   In the Service Manager Case Exchange SMIS instance, an external system named **SM** is used by default for a SAW integration.

> **Note:** For the external system defined in Service Anywhere, if you use a name other than **SM**, you must make the following changes in Service Manager when you add the integration instance:
>
> - For the **Query** field on the **Inbound** tab, replace **SM** in **system=SM** with your new name.
> - For the values of the **Additional path** column on the **Outbound** tab, replace **SM** with your new name in **ExternalSystem**:**SM**.

3. On the **Groups** page, use the **External system** field to assign the external system to a group. This makes the group an external group.

After this configuration, you can select the external group for an Incident record in the Incident Management module. Once an external group is selected, a new section, **External Assignment**, is then added to the Incident page. You can then use that section to configure the record for data exchanging.

For more information about the external systems, groups, or user account roles in Service Anywhere, refer to the corresponding sections in the Service Anywhere documentation.

Validation

This section contains the following topics:

Test SAW to SM Incident Case Exchange

To test SAW to SM Incident Case Exchange:

1. Create a new Incident in SAW. Enter the mandatory details—such as **Title**, **Description**, **Impact**, **Urgency** and **Service**.
2. In the **Assignment group** field of the **Assignment** section of Incident details, enter the group that was associated with the Service Manager external system. Save the Incident record.
3. In Service Manager, observe the new Incident ticket that was opened and verify its details that correspond to those in Service Anywhere—such as **Title** and **Description**.

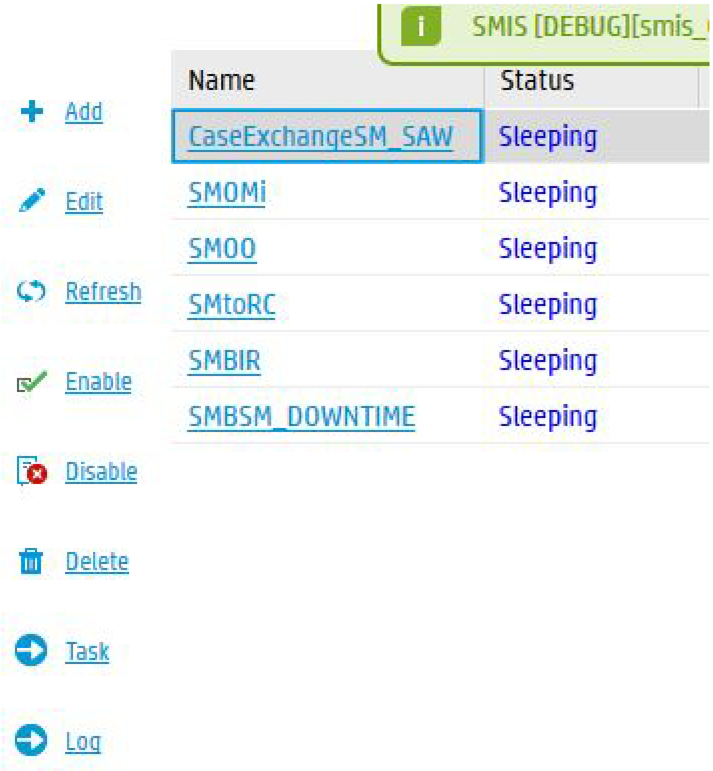
Test SM to SAW Incident Case Exchange

To test SM to SAW Incident Case Exchange:

1. In SM, create a new Incident and fill in mandatory details such as **Title**, **Description**, **Impact**, **Urgency** and **Service**.
2. Modify the **Assignment group** field to correspond with the value entered in **Create Rule Set** for **Create action <*external_assignment_group*>**, and save the Incident.

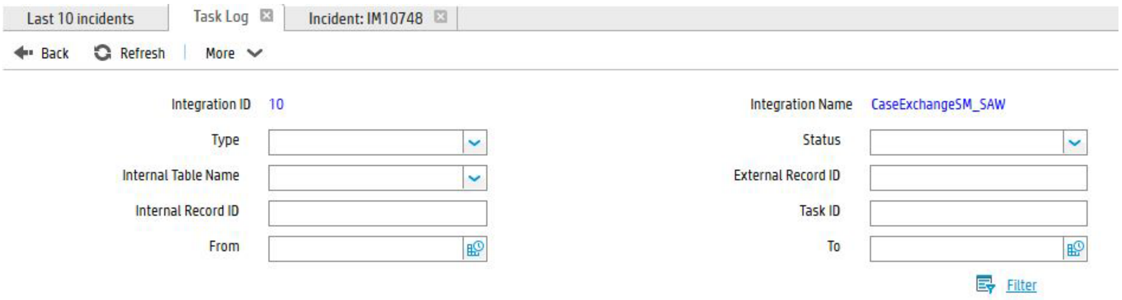
   > **Note:** Note the opened Incident number.

3. In Integration Manager, click the **Task** link to access a list of active integration tasks, or **Log** on to access processed entries.



Name	Status
CaseExchangeSM_SAW	Sleeping
SMOMi	Sleeping
SMOO	Sleeping
SMtoRC	Sleeping
SMBIR	Sleeping
SMBSM_DOWNTIME	Sleeping

4. Filter by entering the **Incident ID** in the **Internal Record ID** field and click **Filter**.



Integration ID 10

Integration Name CaseExchangeSM_SAW

Type

Status

Internal Table Name

External Record ID

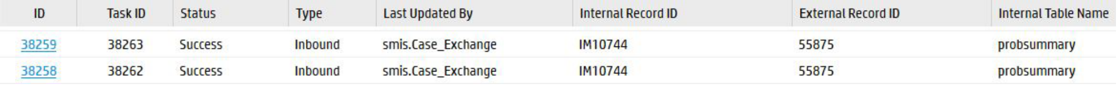
Internal Record ID

Task ID

From

To

5. Review the status task and note the **External Record ID**.



ID	Task ID	Status	Type	Last Updated By	Internal Record ID	External Record ID	Internal Table Name
38259	38263	Success	Inbound	smis.Case_Exchange	IM10744	55875	probsummary
38258	38262	Success	Inbound	smis.Case_Exchange	IM10744	55875	probsummary

6. Log on to Service Anywhere. In the main search field, enter the **External Record ID** from Step 5.

7. Verify that the Incident details—**Title**, **Description**, and so on—correspond with those in SM.

Troubleshooting

- When creating the integration instance in Service Manager, an error message about missing an SSL certificate may occur.

  To overcome this issue, import the SSL certificate of Service Anywhere into the trust store in SM.

  a. Use a browser to log on to a Service Anywhere instance and click the lock icon on the address page.

  b. Select the option to view certificates.

  > **Note:** The wording may differ between browsers.

  In the **Certificate Details** tab, click the **Copy to File** button and select **DER encoded binary x.509**. Next input the name for the stored certificate and complete the wizard.

  c. Copy the certificate file to the SM server. Open a command prompt and execute a command to import the certificate to the keystore used by Service Manager.

For example:

C:\HP\Service Manager 9.40\Server\RUN>.._jvm\bin\keytool.exe -import –keystore <<smtrust>> -file C:\saw-cer.cer

d. Replace **smtrust** with the name of the keystore and restart the SM server to complete this step.

e. If the problem persists, import the SAW certificate to SM Webtier application servers as well.

For example:

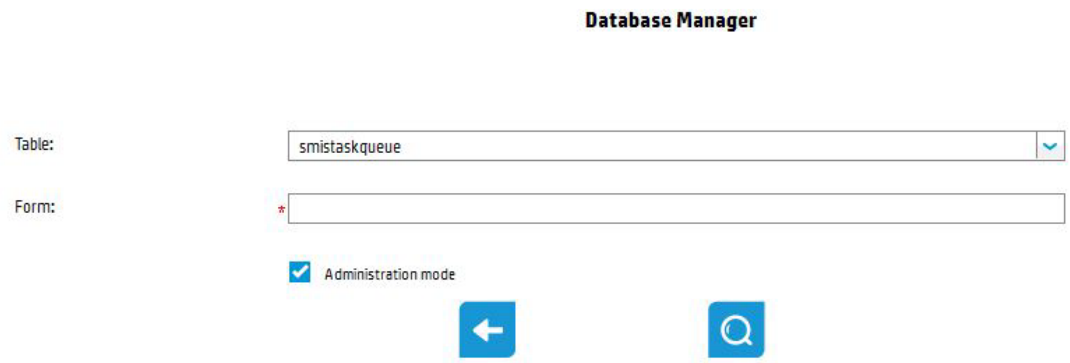
c:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\webtier-9.41\WEB-INF>keytool -importcert -keystore cacerts -storepass changeit -file c:\saw-cer.cer

Restart the Webtier server to complete this step.

- When there are tasks that will not finish and need to be cleared, it is possible to remove them using **Mass Delete** from the task queue table.

a. In the main **search** field, enter **db**.

b. In the Database Manager **Table** field, enter **smistaskqueue** and click the **search** 🔍 button. The **search** result contains two items—**SMISTaskQueue** and **SMISTaskQueue.list**.



Database Manager

Table: smistaskqueue

Form: *

☑ Administration mode

c. Select **SMISTaskQueue** and search for expired tasks.

d. On the pane listing the expired tasks, select either the **Mass Delete** tab to delete all of the tasks or select individual tasks and click the **Delete** tab.

Part III: Appendix

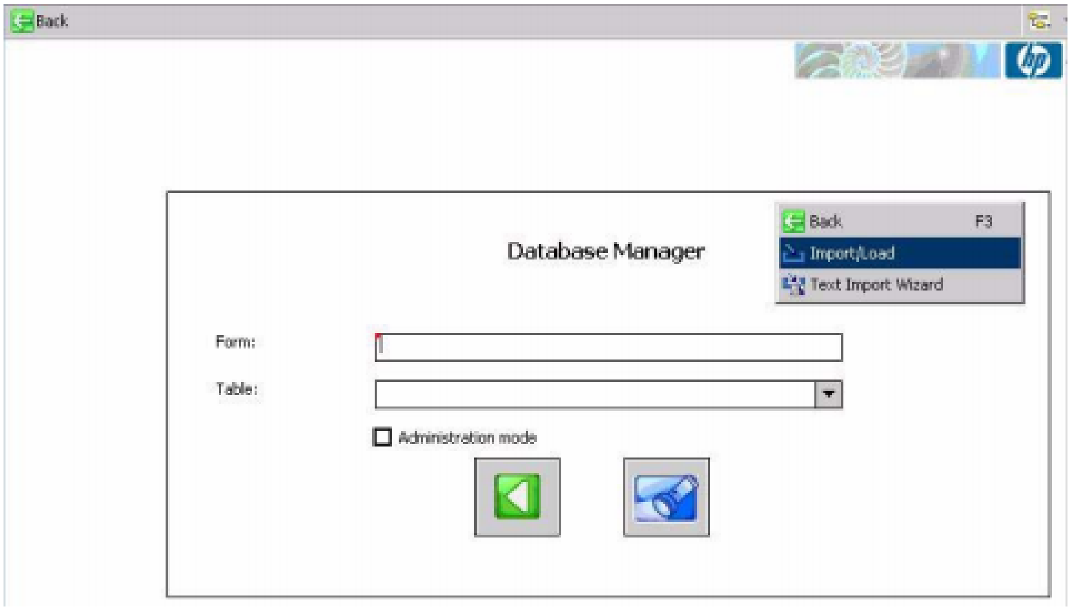
Appendix A: Importing Unload Files into Service Manager

This appendix includes:

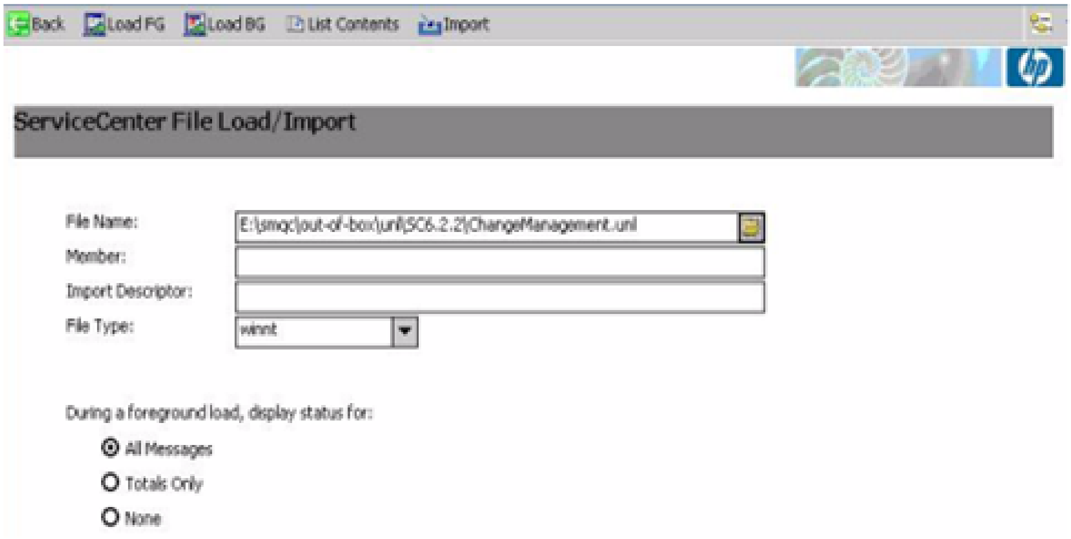
Importing Unload files into Service Manager

To import Unload files into SM:

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.



ServiceCenter File Load/Import

File Name: E:\smqc\out-of-box\unl\SC6.2.2\ChangeManagement.unl

Member:

Import Descriptor:

File Type: winnt

During a foreground load, display status for:

- ● 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: Adding BPM CIs and Events to OMi

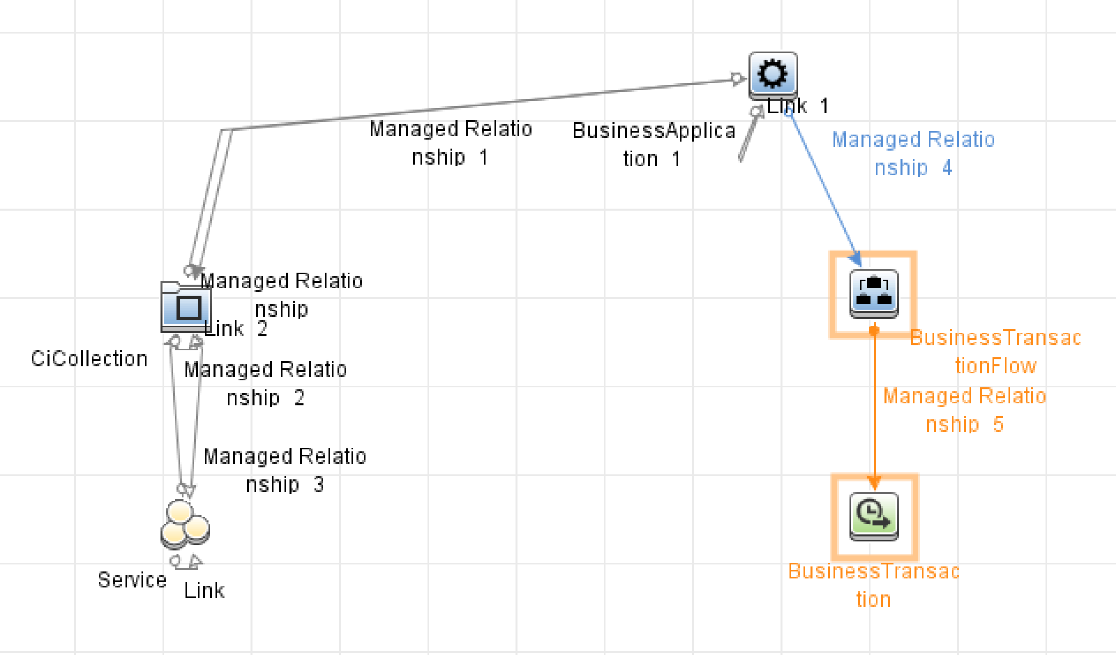
This appendix includes:

Task 1: Edit CI Synchronization to Include Additional Business Elements

The CI synchronization queries, provided by the OMi_integration package, omit **Business Transaction** and **Business Transaction Flow** CI types. To synchronize those CIs, modify the queries.

To modify the query:

1. In BSM, navigate to **Admin > RTSM Administration > Modeling > Modeling Studio**.
2. The query that synchronizes business CIs between BSM and OMi (either via standalone UCMDB or directly) is located in the **Integration > OMi_integration** folder and is called **OMi_Sync_Biz**. Edit this query to include **Business Transaction** and **Business Transaction Flow**, and their relations according to the following screen shot.



3. Save the changes to the query.
4. The next step depends on whether standalone UCMDB is implemented, or BSM is integrated directly with OMi.

> **Note:** More detailed information for the following steps can be found in the *HPE RTSM Best Practices Guide* (https://softwaresupport.hpe.com/km/KM01996511).

- For integration via UCMDB:
    i. In BSM, navigate to **Data Flow Management > Integration Studio**.
    ii. Locate the integration point which synchronizes data from BSM to UCMDB (if following the *HPE RTSM Best Practices Guide*, use **APM2UCMDB**) and verify the synchronization job includes the modified **OMi_Sync_Biz** query.
    iii. The CIs are synchronized from UCMDB to OMi using the **Push CIs to OMI** integration point (as described in the *HPE RTSM Best Practices Guide*).

- For a direct integration with OMi:

    i. In OMi, navigate to **Administration > RTSM Administration > Data Flow Management > Integration Studio**.

    ii. Locate the integration point which synchronizes CIs with BSM (if following the *HPE RTSM Best Practices Guide*, use **APM2OMi**) and verify that the synchronization job includes the modified **OMi_Sync_Biz** query.

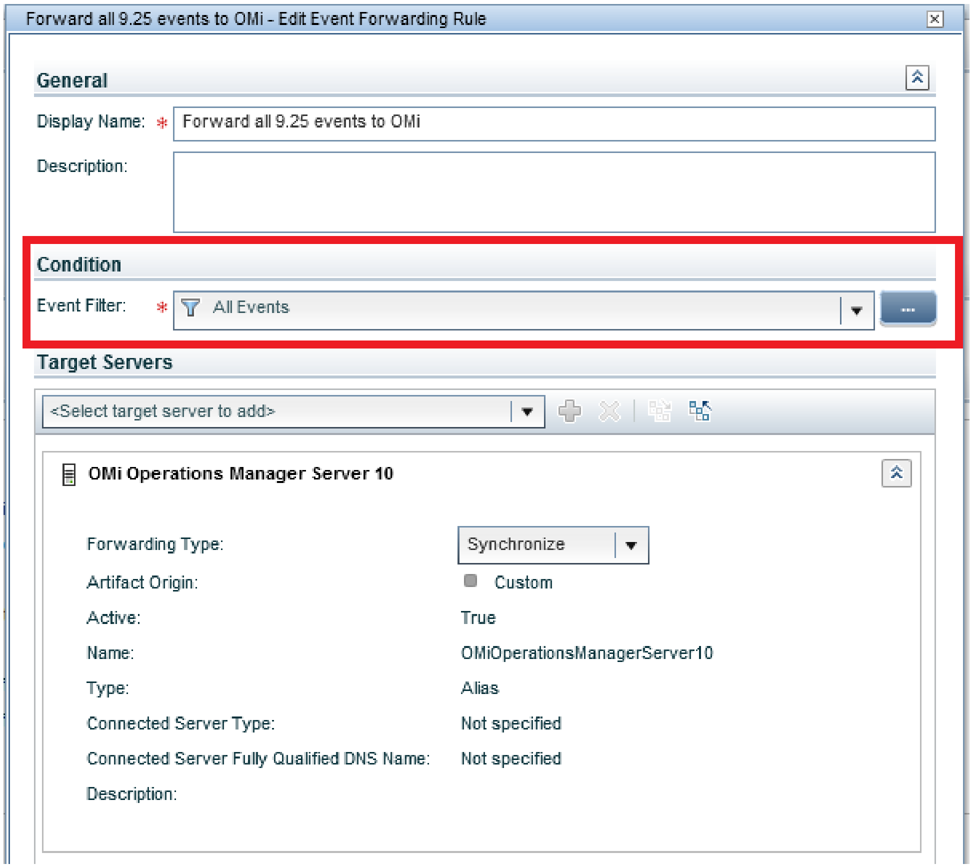
Task 2: Change the Event Forwarding Filter

The Event Forwarding Rule created by the Application Performance Management (APM) – Operations Manager i (OMi) integration wizard excludes Business Transaction and Business Transaction Flow events. To enable forwarding of events of all CI types, the Event forwarding filter in BSM must be changed so that it will not filter out BPM Events.

To change the Event Forwarding Filter:

1. In the BSM user interface, navigate to **Admin > Operation Management**. The Operation Management Administration page opens.
2. In the Operation Management Administration page, navigate to **Event Automation > Event Forwarding**.
3. In the Event Forwarding Rules pane, double-click **Forward all 9.25 events to OMi Rule**. The **Forward all 9.25 events to OMi - Edit Event Forwarding Rule** dialog box opens.

4. In the **Condition** section, click the **Event Filter** browse button and select **All Events**.



Forward all 9.25 events to OMi - Edit Event Forwarding Rule

General

Display Name: * Forward all 9.25 events to OMi

Description:

Condition

Event Filter: * All Events

Target Servers

<Select target server to add>

OMi Operations Manager Server 10

Forwarding Type:	Synchronize
Artifact Origin:	Custom
Active:	True
Name:	OMiOperationsManagerServer10
Type:	Alias
Connected Server Type:	Not specified
Connected Server Fully Qualified DNS Name:	Not specified
Description:	

5. Click **OK**.

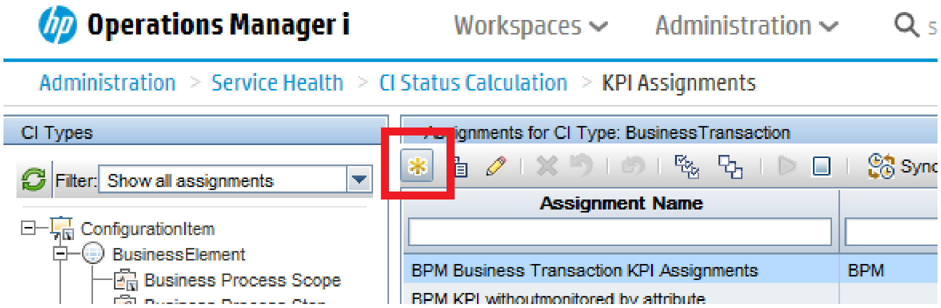
Task 3: Add KPI Assignments for BPM CIs

The appropriate KPI, with its related Health Indicator (HI), must be assigned to the BPM configuration items (CIs) in OMi, thus allowing BPM Events to affect the BPM-related CI status in the OMi dashboard.

To add KP assignments for BPM CIs:

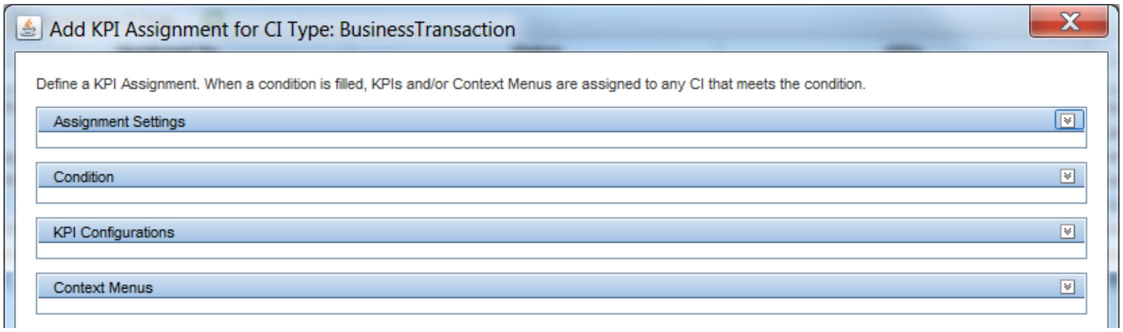
1. In OMi, navigate to **Administration > ServiceHealth > CI Status Calculation > KPI Assignments**. The KPI Assignments page opens.
2. In the CI Types pane, navigate to **ConfigurationItem > BusinessElement** and select the **BusinessTransaction** CI type.

3. In the Assignments for CI Type: BusinessTransaction pane, click **New** .


Operations Manager i
Workspaces
Administration
Administration > Service Health > CI Status Calculation > KPI Assignments
CI Types
Filter: Show all assignments
ConfigurationItem
BusinessElement
Business Process Scope
Assignments for CI Type: BusinessTransaction
Sync
Assignment Name

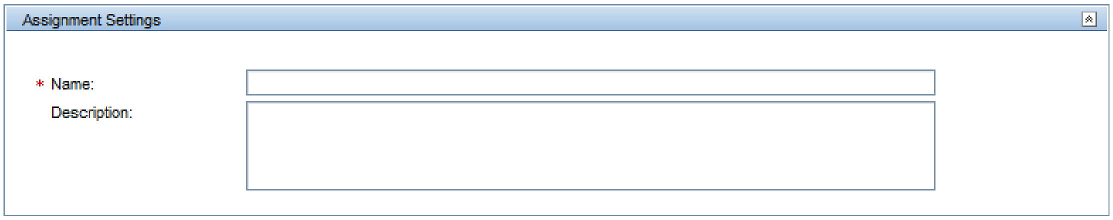
BPM Business Transaction KPI Assignments | BPM
BPM KPI withoutmonitored by attribute

The **Add KPI Assignment for CI Type: BusinessTransaction** dialog box opens.



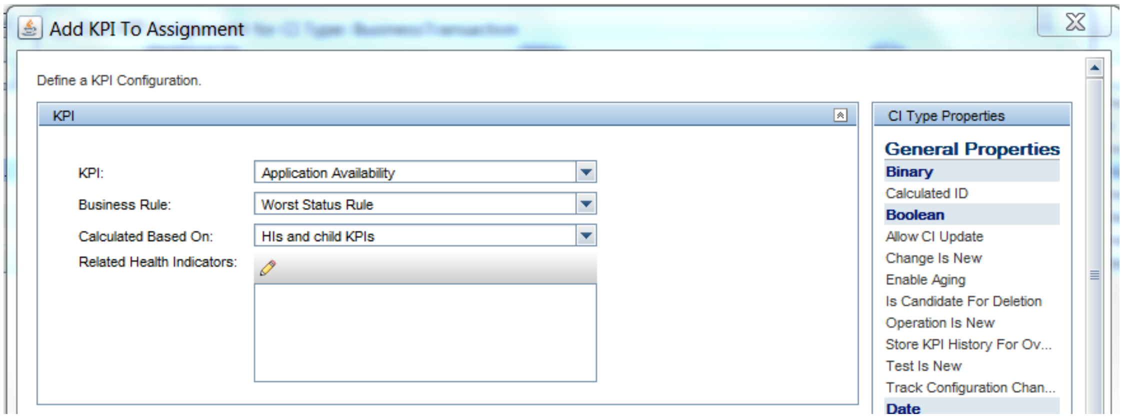
Define a KPI Assignment. When a condition is filled, KPIs and/or Context Menus are assigned to any CI that meets the condition.

4. In the **Add KPI Assignment for CI Type: BusinessTransaction** dialog box, go to **Assignment Settings** and provide the name **New BPM KPI Assignment**.



5. Go to **KPI Configurations** and click **New** . The **Add KPI to Assignment** dialog box opens.

6. In the **Add KPI to Assignment** dialog box, add the **Application Availability** and **Application Performance** KPI assignments.



Add KPI To Assignment

Define a KPI Configuration.

KPI

KPI: Application Availability

Business Rule: Worst Status Rule

Calculated Based On: HIs and child KPIs

Related Health Indicators:

CI Type Properties

General Properties

Binary

Calculated ID

Boolean

Allow CI Update

Change Is New

Enable Aging

Is Candidate For Deletion

Operation Is New

Store KPI History For Ov...

Test Is New

Track Configuration Chan...

Date

a. For **Application Availability**, select the following:

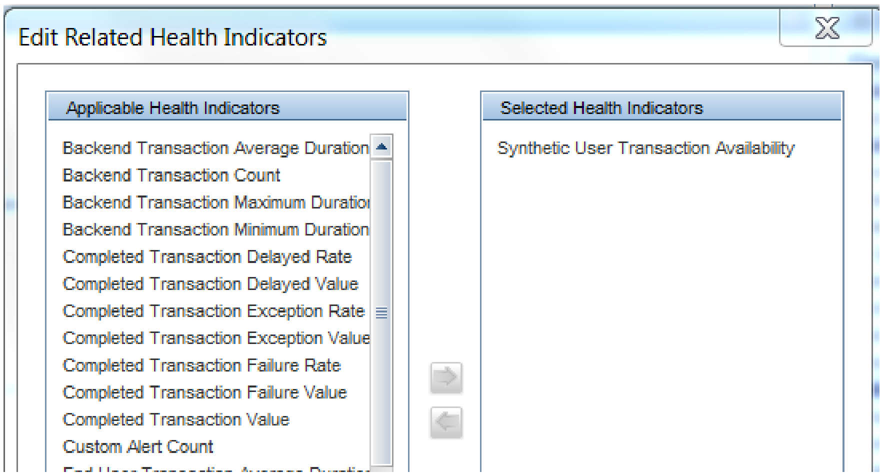
i. **KPI.** Application Availability

ii. **Business Rule.** Worst Status Rule

iii. **Calculated Based On.** HIs and child KPIs

iv. **Related Health Indicators.**

A. Click **Edit** . The **Edit Related Health Indicators** dialog box opens.



Edit Related Health Indicators

Applicable Health Indicators

Backend Transaction Average Duration
Backend Transaction Count
Backend Transaction Maximum Duratio
Backend Transaction Minimum Duration
Completed Transaction Delayed Rate
Completed Transaction Delayed Value
Completed Transaction Exception Rate
Completed Transaction Exception Value
Completed Transaction Failure Rate
Completed Transaction Failure Value
Completed Transaction Value
Custom Alert Count

Selected Health Indicators

Synthetic User Transaction Availability

B. From the **Applicable Health Indicators** field, select the **Synthetic User Transaction Availability** HI and click the **Move to Selected Health Indicators** button.

C. Click **Save**.

b. For **Application Performance**, select the following:

   i. **KPI.** Application Performance

   ii. **Business Rule.** Worst Status Rule

   iii. **Calculated Based On.** HIs and child KPIs

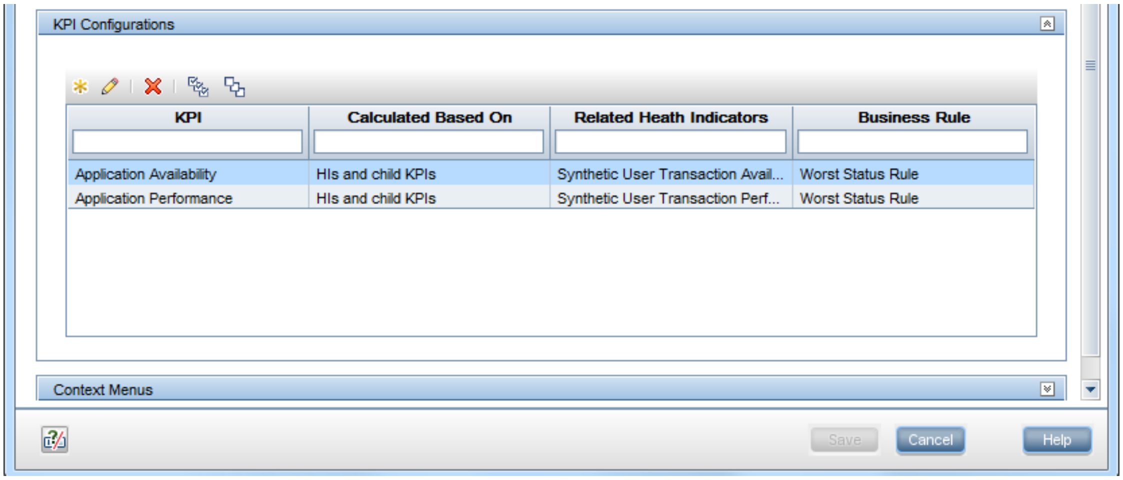
   iv. **Related Health Indicators.**

      A. Click **Edit** ✎. The **Edit Related Health Indicators** dialog box opens.

      B. From the **Applicable Health Indicators** field, select the **Synthetic User Transaction Availability** HI and click the **Move to Selected Health Indicators** ➔ button.

      C. Click **Save**.

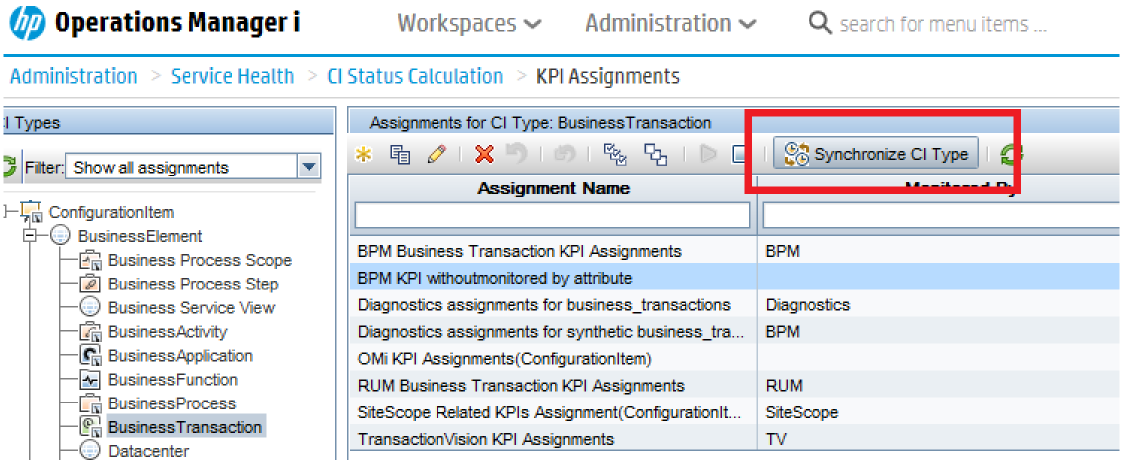
The KPI Configurations section now looks as follows:



KPI	Calculated Based On	Related Heath Indicators	Business Rule
Application Availability	HIs and child KPIs	Synthetic User Transaction Avail...	Worst Status Rule
Application Performance	HIs and child KPIs	Synthetic User Transaction Perf...	Worst Status Rule

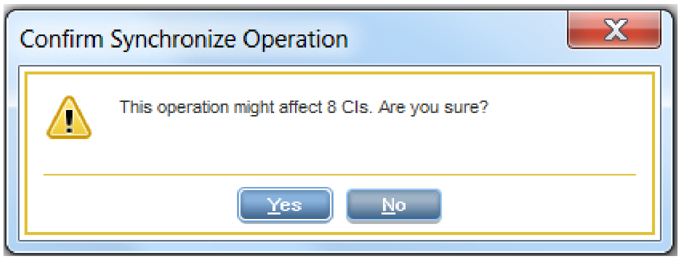
7. In the **Add KPI Assignment for CI Type: BusinessTransaction** dialog box, click **Save**.

8. In the Assignments for CI Type: BusinessTransaction pane, click the **Synchronize CI Type** button.



Assignment Name	Monitored By
BPM Business Transaction KPI Assignments	BPM
BPM KPI withoutmonitored by attribute	
Diagnostics assignments for business_transactions	Diagnostics
Diagnostics assignments for synthetic business_tra...	BPM
OMi KPI Assignments(ConfigurationItem)	
RUM Business Transaction KPI Assignments	RUM
SiteScope Related KPIs Assignment(ConfigurationIt...	SiteScope
TransactionVision KPI Assignments	TV

9. In the **Confirm Synchronize Operation** dialog box, click **Yes**.



This operation might affect 8 CIs. Are you sure?

Note: This operation affects all of the CIs of the **BusinessTransaction** CI Type. If you are already running an environment with BPM monitoring in your OMi Version 10.x, consult with HPSW Support before changing KPI assignments.

Appendix C: Downtime Exchange Between OMi and SM

This appendix includes:

Overview

This chapter explains how to implement a downtime exchange between Operations Manager i (OMi), Business Service Management (BSM), and Service Manager (SM) via Universal CMDB (UCMDB).

For other implementations, see "Downtime Forwarding from Service Manager to OMi (RTSM)" in Chapter 21 in *HPE Operations Manager i Version 10.10 OMi Integrations Guide* (https://softwaresupport.hpe.com/km/KM01914041).

The downtime integration between OMi and SM includes information exchanges in both of the following directions:

1. **SM > OMi**. 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 OMi.

   In this scenario, you install and set up a downtime adapter on your UCMDB/CMS. The RFC creates a planned downtime CI in the CMS, and the adapter translates the planned downtime CI to a downtime in OMi.

2. **OMi > SM (and BSM)**. When you define downtimes using OMi (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 OMi are translated to Events, which create corresponding Incidents in SM. In parallel, these downtime

events are forwarded to BSM. During the defined outage period, all related CI events are suppressed.

In this scenario, when a downtime starts, OMi generates an Event. Using the Event Forwarding mechanism, the Event generates an Incident in SM. In parallel, these downtime events are forwarded to BSM. During the defined outage period, all related CI events are suppressed. 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 OMi > SM, a separate Event is sent for each CI in the downtime.

> **Note:**
>
> - Following the initial integration, a large amount of data may be communicated from SM to OMi. We recommend that you perform the integration during off-hours to prevent negative impact on system performance.
> - The integration consists of two main parts: **SM > CMS** and **CMS > OMi**. 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 part, and then wait a long time before setting up the CMS > OMi adapter part, the number of downtimes communicated to OMi initially may be extremely high.

Prerequisites

For a downtime exchange between OMi and SM, you must have the Detect to Correct (D2C) Value Stream up and running.

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

- **Universal CMDB.** Server is installed. Data flow probe is connected and running (on a different server than the OMi server).
- **Service Manager.** Server, Client, Help Server, Web Tier, and Knowledge Management are installed and running.
- **Operations Manager i.** Server is installed and running. OMi machine has the data flow probe connected and running.
- **Business Service Management.** Server is installed and running. BSM machine has the data flow probe connected and running.

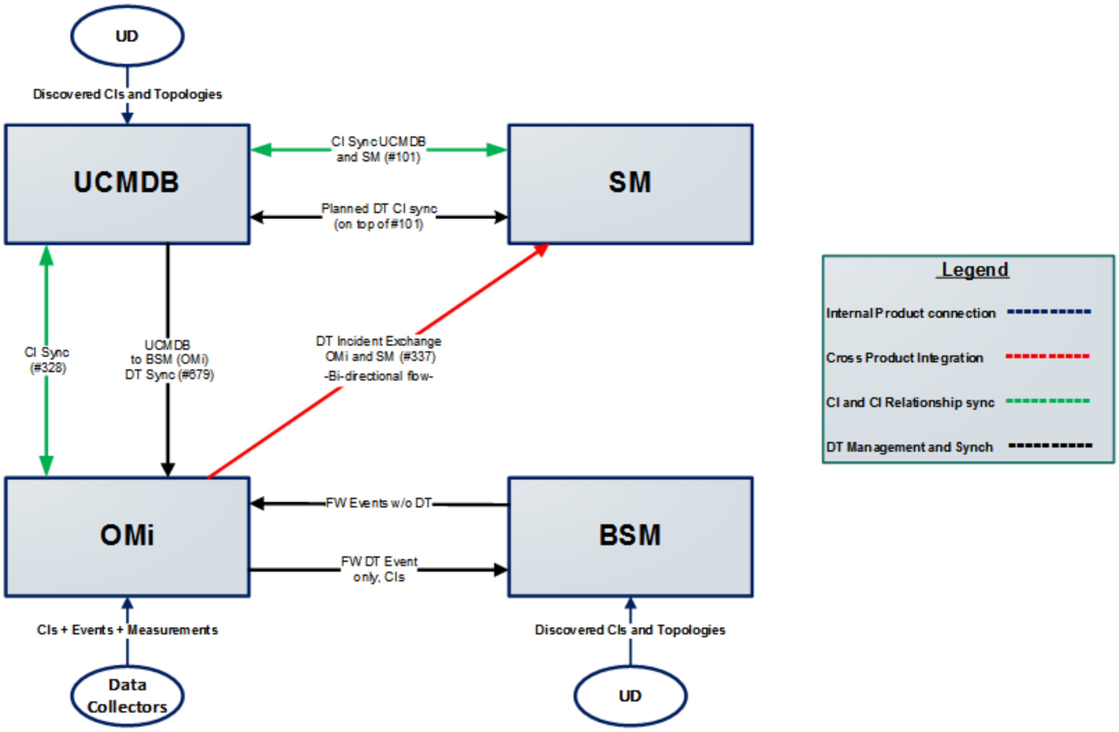
Global ID Generator

To enable the downtime integration, you must have a Global ID Generator configured in your UCMDB and OMi environment.

The Global ID Generator configuration is described in the *HPE RTSM Best Practices Guide* (https://softwaresupport.hpe.com/km/KM01996511).

Downtime Exchange Between OMi and SM Diagram

The following diagram shows a typical deployment of the downtime exchange between Operations Manager i (OMi) and Service Manager (SM).


UD
Discovered CIs and Topologies
UCMDB
CI Sync UCMDB and SM (#101)
SM
Planned DT CI sync (on top of #101)
CI Sync (#328)
UCMDB to BSM (OMi) DT Sync (#679)
DT Incident Exchange OMi and SM (#337) -Bi-directional flow-
OMi
FW Events w/o DT
BSM
FW DT Event only, CIs
CIs + Events + Measurements
Data Collectors
Discovered CIs and Topologies
UD
Legend
Internal Product connection
Cross Product Integration
CI and CI Relationship sync
DT Management and Synch

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

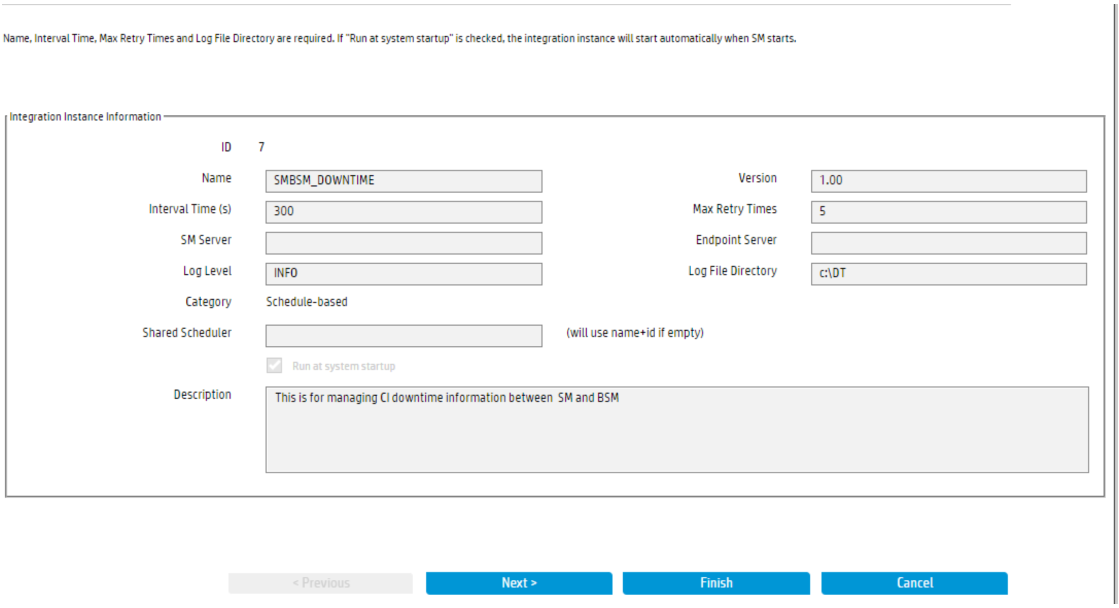
This section contains:

Task 1: Create an SMIS SMBSM_DOWNTIME integration

To create an SMIS SMBSM_DOWNTIME integration:

1. Log on to the SM system as **System.Admin**.
2. Navigate to **Tailoring > Integration Manager > Add** to add an 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**.

6. Fill in the data for the **Log File Directory** and 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

ID	7		
Name	SMBSM_DOWNTIME	Version	1.00
Interval Time (s)	300	Max Retry Times	5
SM Server		Endpoint Server	
Log Level	INFO	Log File Directory	c:\DT
Category	Schedule-based		
Shared Scheduler		(will use name+id if empty)	
	☑ Run at system startup		
Description	This is for managing CI downtime information between SM and BSM		

> **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.

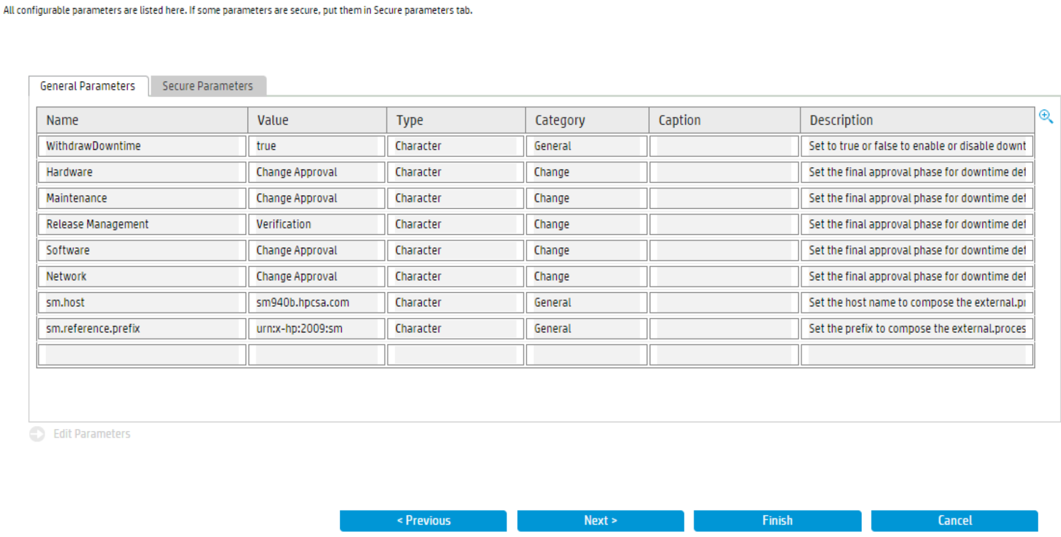
      If your category work flow has multiple paths with different final approval phases, use a semicolon "**;**" to separate them.

      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.



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

Name	Value	Type	Category	Caption	Description
WithdrawDowntime	true	Character	General		Set to true or false to enable or disable downt
Hardware	Change Approval	Character	Change		Set the final approval phase for downtime def
Maintenance	Change Approval	Character	Change		Set the final approval phase for downtime def
Release Management	Verification	Character	Change		Set the final approval phase for downtime def
Software	Change Approval	Character	Change		Set the final approval phase for downtime def
Network	Change Approval	Character	Change		Set the final approval phase for downtime def
sm.host	sm940b.hpcsa.com	Character	General		Set the host name to compose the external.pı
sm.reference.prefix	urn:x-hp:2009:sm	Character	General		Set the prefix to compose the external.proces

e. Click **Next**, **Next**, **Finish**.

f. Select the **SMIS**.

g. Click **Enable**.

h. Click **Yes**.

Task 2: Exchange SM RFC downtimes with UCMDB

To 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 **SM CLIP Down Time Population 2.0** TQL, and another named **DT Relationship** based on **SM CI Connection Down Time CI 2.0** TQL.
5. Log on as **System.Admin**. 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 **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.

Task 3: Exchange SM downtimes with OMi (via UCMDB)

To exchange SM downtimes with OMi (via UCMDB):

1. To enable downtimes defined in SM to be sent to OMi, you must add an integration adapter to the UCMDB where downtimes are defined as follows:
   a. From **C:\HPBSM\odb\conf\factory_packages** in the OMi 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.zip** file 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 into BSM adapter** .

c. Enter the following information for the adapter:

   i. **OMi hostname** and **port**

   ii. **integration point credentials**

   iii. **communication protocol**

   iv. **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 OMi 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 OMi. If no communication problem is found, restart the MercuryAS process.

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

Task 4: Enable Initial KPI Status and OMi Downtime Synchronization with APM

To enable OMi to sync downtimes to APM:

1. On the OMi server, navigate to **Administration > Setup and Maintenance > Connected Servers**.
2. Double-click your APM connected server to open the **Edit Server Connection** wizard.
3. Click the check box to the left of **Step 3: Synchronization**.

This triggers:

a. the initial synchronization of all KPI states for all APM CIs,

> **Note:** This initial synchronization is necessary if you want to see the current state on the APM system.

b. the continuous downtime definition synchronization of OMi to APM.

4. **Optional:** Click the **Synchronize Downtime** box if you want OMi to synchronize downtime in APM. Since downtime is currently set in OMi, this setting is especially useful when BPM/SiteScope is used in APM.

> **Note:** Verify you have the same integration user and recipient in both OMi and APM/BSM.

Appendix D: HPE Product Integrations

This appendix includes:

Overview

The following integrations, while not strictly necessary for the end-to-end flow of the Detect to Correct Value Stream, allow the customer to leverage the breadth and depth of HPE Products for added value from domain-specific monitoring tools, such as with OMI Event Feeding and APM Data Collectors, or integrating Operations Analytics to collect and analyze the monitoring data from those tools, which allows more effective troubleshooting for complex issues.

OMi Event Feeding

- ID#344 Network to BSM / OMi integration (OMi-NNMi)

  The HPE Network Node Manager i (NNMi) to HPE BSM/OMi integration forwards NNMi management events as SNMPv2c traps to the BSM Connector on the NNMi management server. The BSM Connector filters the NNMi traps and forwards them to BSM/OMi.

- ID#812 View NNMi UI components within OMi

  This integration enables you to view NNMi user interface components within HPE Operations Manager i (OMi), using the OMi user interface Mashup technology.

- ID#648 Event Lifecycle: Event/Incident submission from OM for Windows to OMi (OMW-OMi)

  This integration allows Event forwarding from OM for Windows to OMi and bidirectional synchronization of forwarded events; as well as starting automatic actions, operator action, and tools from the OMi console, and delegating the action request to OM; and retrieves node and service objects from OM and imports these CIs into OMi's RTSM.

- ID#198 Event Lifecycle: Event/Incident submission from OM for UNIX or Linux to OMi (OMU-OMi)

  This integration allows Event forwarding from OM for Unix to OMi and bidirectional synchronization of forwarded events; as well as starting automatic actions, operator action, and tools from the OMi console, and delegating the action request to OM; and retrieves node and service objects from OM and imports these CIs into OMi's RTSM.

- ID#412 Event forwarding from SiteScope to OM (Sitescope-OMi)

  HPE SiteScope can communicate with Operations Manager using the Operations Agent, which is installed on the SiteScope server, in order to send events to OMi. This is the same integration used to integrate SiteScope with OM for Windows or OM for Unix.

APM Data Collectors

- ID#460 Diagnostics to APM (Diagnostics-APM)

  Diagnostics can be integrated with Application Performance Management to provide information to help you understand and improve the performance of your J2EE and .NET applications.

- ID#498 RUM for monitoring (RUM-APM)

  HPE Real User Monitor (RUM) offers the unique capability of correlating application traffic to the network layer. Each version of RUM must connect to a suitable Application Performance Management (APM) system for the user to be able to view, manage, and analyze the traffic monitored by RUM.

- BPM-APM

  Business Process Monitor (BPM) is one of the Business Service Management (BSM) data collectors. BPM proactively monitors enterprise applications in real time, identifying performance and availability problems before users experience them.

- HPELN OMi Management Pack for vPV

  The OMi Management Pack for HP Virtualization Performance Viewer (HP vPV) works with OMi and enables you to view the HP vPV alerts, topology, and performance graphs on OMi.

Operations Analytics Data Collection

- ID#702 Operations Analytics - SiteScope Data Collection integration (OpsA-SiS)

  This integration enables users to collect monitoring information from SiteScope for use with HPE Operations Analytics.

- ID#703 Operations Analytics - Business Process Monitor Data Collection integration (OpsA-BPM)

  This integration enables users to collect metrics related to application transaction response time from BPM for use in Operations Analytics.

- ID#706 Operations Analytics - Network Node Manage iSPI Performance for Metrics Data Collection integration

  This integration enables users to collect interface and node component performance information from HPE NNM iSPI Performance for Metrics for use with Operations Analytics.

- ID#725 Operations Analytics - Operations Manager Data Collection integration

  This integration enables users to collect events generated by Operations Manager Software for use in Operations Analytics.

- ID#726 Operations Analytics - HPE Operations Agent Data Collection integration

  This integration enables users to collect global system information on the host that is running the HPE Operations Agent. This data is then available for use with Operations Analytics.

- ID#832 Operations Analytics - RUM Data Collection integration

  This integration enables users to collect real user monitor metrics for use with Operations Analytics.