HP Service Manager

Software Version: 9.41

For the supported Windows® and UNIX® operating systems

Integrations help topics for printing

Document Release Date: September 2015
Software Release Date: September 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For a complete list of open source and third party acknowledgements, visit the HP Software Support Online web site and search for the product manual called HP Service Manager Open Source and Third Party License Agreements.

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 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 HP sales representative for details.

Support

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

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

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

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

Most of the support areas require that you register as an HP Passport user and 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.

HPSW Solutions Catalog accesses the HPSW Integrations and Solutions Catalog portal website. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not

be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Integrations

You can extend the services available to your HP Service Manager installation by integrating to other products. Out-of-box, HP Service Manager allows you to integrate to the following products without needing any additional integration software:

- SAP Solution Manager
- HP Project and Portfolio Management Center (PPM)
- HP Quality Center (QC)
- "HP Universal CMDB" on page 152
- "HP Release Control (RC)" on page 123
- "HP Operations Orchestration (OO)" on page 173
- "HP Business Service Management (BSM)" on page 209
- HP Operations Manager i (OMi)
- Third-party survey tools

You can also integrate data from other sources using tools such as HP Connect-It, SCAuto, Web Services API, and Case Exchange. Contact HP Customer support for information or instructions on integrating data from sources outside of HP Service Manager.

Note:

1. Plug-ins are deprecated as of Service Manager 9.20 and will not be supported in upcoming releases.
2. To check for recent updates of the embedded PDF manuals in this chapter, or to verify that you are using the most recent edition of a document, go to:

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

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

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

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

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

Service Manager integration methods and tools

In addition to the integrations provided by Service Manager and other HP products, you can use several utilities and methodologies to create your own Service Manager integrations.

Method or Tool	Description
"Web Services" on the next page	Allows you to connect to and consume external Web Services and to publish Service Manager tables as Web Services. For example, you might use web services to query external Web Services to validate an email address or a phone number when updating a contact record or automatically perform an Internet search using the brief description of the Service Desk interaction.
"HP Connect-It (CIT)" on the next page	Provides connectors that synchronize static data elements by simple data copying and by data transformation from source to destination. For example, you could use Connect-It to synchronize employee data from HP Asset Manager to Service Manager though Web Services.
"HP ServiceCenter Automation (SCAuto)" on page 19	Consists of a collection of automation products which enable external applications to integrate with Service Manager. For example, you might use SCAuto to open records, notify someone that their record has closed, or manage email between external mail programs.
"Event Services" on page 19	Is a background processor that Service Manager uses to receive information generated from and to send information back to external systems. exchange of dynamic, "event-based" information. For example, you must use Event Services with SCEmail, Connect-It, SCMail, and SCAuto.
"Dynamic Data Exchange (DDE)" on page 62	Provides DDE client support in a Service Manager RAD (Rapid Application Development) application. For example, you might create a script to call Service Manager from a Windows application such as Microsoft® Excel.
"BDM Mapping Management" on page 104	Allows you to configure BTO Data Modle (BDM) mapping records. BDM is intended to be used as a standard data model for integrations between HP BTO products, for example, HP Service Manager and HP Business Service Management (BSM) . In Service Manager, a BDM mapping is a mapping between a Service Manager object (associated to a file in Service Manager) and a BDM object (predefined in BDM). A BDM mapping consists of three parts: field mapping, value mapping, and atom mapping.

Web Services

HP Service Manager Web Services provide interoperability between software applications running on disparate platforms. By using Simple Object Access Protocol (SOAP) technology to establish a standard messaging framework, web services enable developers to access objects within multiple and customized data fields. Open architecture allows for real-time integration and exposure of objects to external applications.

Key features and benefits:

- Uses open standards and protocols
- Allows reuse of services and components
- Can combine multiple web services
- Uses HTTP/HTTPS to work through common firewall security measures without requiring changes to the firewall filtering rules
- Facilitates open integration to other systems
- Provides a standard framework with a consistent and dynamic application program interface (API) architecture for process-based integration

The *HP Service Manager Web Services Guide* is available from the help.

HP Connect-It (CIT)

HP Connect-It is an integration platform that exposes technology infrastructure data as common business objects. The HP Connect-It family of connectors leverages industry-standard protocols and connects with third-party information systems in order to integrate technology infrastructure products with external information systems to align business processes and synchronize relevant data.

Key features and benefits:

- Integrates ITSM solutions with almost any data source
- Leverages industry-standard protocols
- Helps Managers make informed business decisions

- Improves data quality and integrity
- Includes built-in best practice integrations
- Reduces implementation time
- Provides the power of an enterprise application integration (EAI) tool at the cost of a gateway

For more information, refer to the Connect-IT documentation suite, available on HP Support's Software Product Manuals site.

HP ServiceCenter Automation (SCAuto)

SCAuto is a suite of interface products that integrate HP Service Manager to network and systems management tools such as HP Operations and HP Network Node Manager. The SCAuto interface sends event messages to a Service Manager server over a TCP connection. SCAuto links service workflows in HP Service Manager to automated event collection tools, providing better and more proactive management and control. SCAuto allows for proactive incident prevention because network events can be detected often before a problem is noticed or reported by the business. You can use the SCAuto software development kit to build integrations to nearly application.

Key features and benefits:

- Integrates to nearly any application
- Uses an event-driven architecture
- Provides efficient resource overhead

Each SCAuto product requires a separate license.

See the *HP ServiceCenter Automate (SCAuto) Software Development Kit (SDK)* for more information.

Event Services

HP Service Manager Event Services is an interface between HP Service Manager and external systems. It is the preferred mechanism for interfacing HP Service Manager to external systems. It runs on Microsoft Windows and Unix platforms, does not require an existing client session to operate, and can be configured to run as a background processor.

Event Services overview

Event Services provides standard applications to:

- Open, update, and close HP Service Manager incidents
- Open, update, and close HP Service Manager calls
- Add, update, and delete Configuration Items
- Open, update, approve, and close changes and requests

Standard applications are available within HP Service Manager to generate outbound information, such as e-mails. Standard applications come with out-of-box forms, or you can tailor both forms and operations to meet your needs. You can also modify Event Services to perform any HP Service Manager operation on any HP Service Manager table.

Supported products

HP Service Manager Event Services interfaces with other internal and external products which include:

- IBM Tivoli NetView® Automated Problem Applications (NAPA)
- HP Service Manager Mail (JavaMail), which sends Service Manager e-mail to other mail systems
- SCMail (for Unix) and SCMapi (for Windows), which supports bi-directional e-mail with other e-mail systems
- SCAutomate, which links HP Service Manager to external products such as IBM Tivoli® and HP Network Node Manager
- Customized SCAutomate applications
- Get-It
- Connect-It, which uses Event Services for input events and HP Service Manager for output events

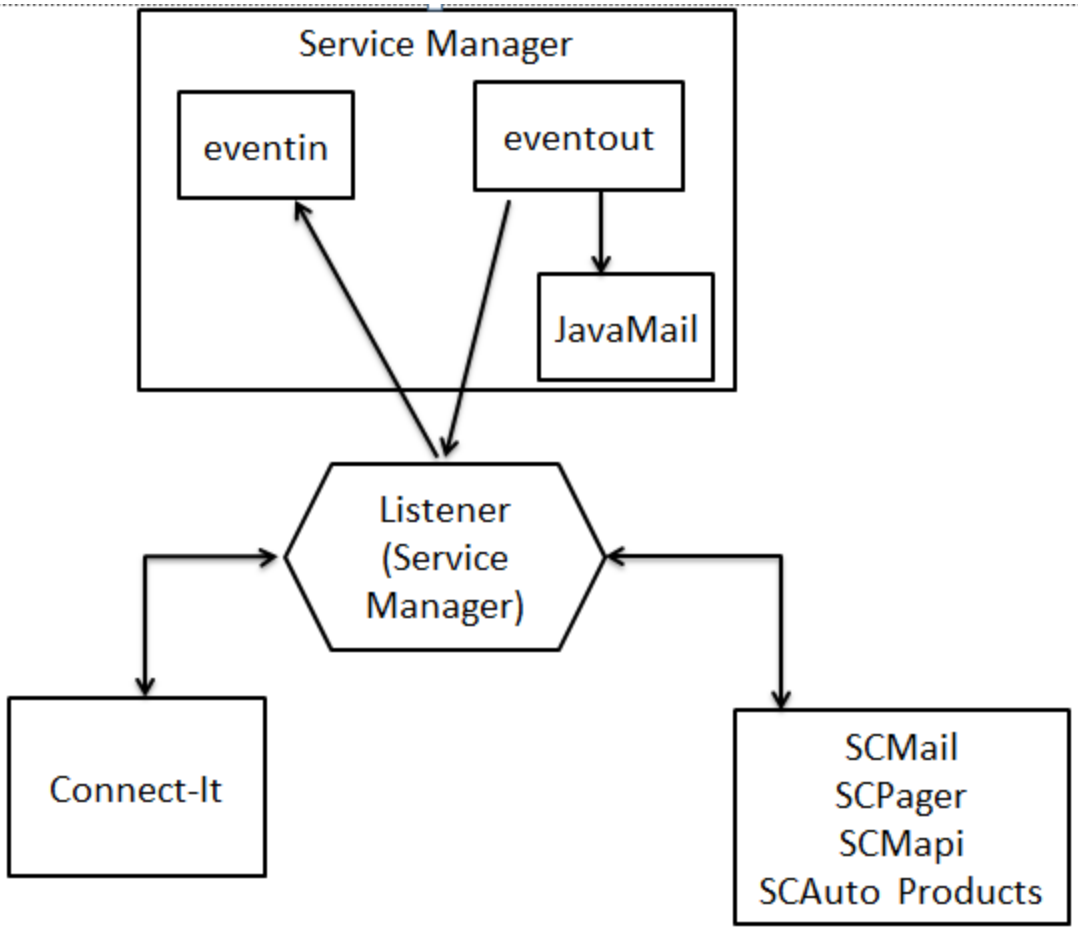
Communication with external systems

To accomplish the communication between products, you must establish a connection between HP Service Manager and the external system. Some type of TCP/IP connection is required, depending on the

product and environment. The connection may also involve the sm listener.

Event Services routing

Event Services routes Events entering and exiting HP Service Manager differently depending on the external system communicating with HP Service Manager. For some products, Event Services routes information in one direction only. For others, events flow in both directions.



Routing events with internal and external products

The following table describes how the following products route events using Event Services.

Product	Internal/External product	Routing direction	Description
IBM Tivoli NetView® Automated Problem Applications (NAPA)	External	Inbound events only	Information is routed from NetView® using VSAM. A HP Service Manager

Product	Internal/External product	Routing direction	Description
			internal application reads a record from an existing VSAM data set and writes a corresponding eventin record. The capability to read VSAM data sets residing on another machine is native to Service Manager. Because the Service Manager server runs on a Unix or Microsoft Windows platform, you must configure a connection between the Service Manager server and the machine where the VSAM data set resides using the SC3270 product.
HP Service Manager e-mail (JavaMail)	Internal	Outbound events only	HP Service Manager uses an eventout record to route information to JavaMail. JavaMail connects directly to the server, responds to, and processes only email eventout records.
Connect-It	External	Inbound events only	Connect-It establishes a client connection to the HP Service Manager server through a listener (sm) and information is routed bi-directionally through the connection. Connect-It requires inbound information to go through Event Services. However, outbound information can be read directly. Connect-It can read the outbound data from the eventout queue.
Get-It	External	Inbound and outbound events	Get-It establishes a client connection to the HP Service Manager server through a listener (sm) and information is routed bi-directionally through the connection. Get-It inbound and outbound information uses Event Services eventin and eventout tables.
SCMail SCMapi SCAutomate products	External	Inbound and outbound events	These products establish a client connection to the HP Service Manager server through a listener (sm) and information is routed bi-directionally through the connection.

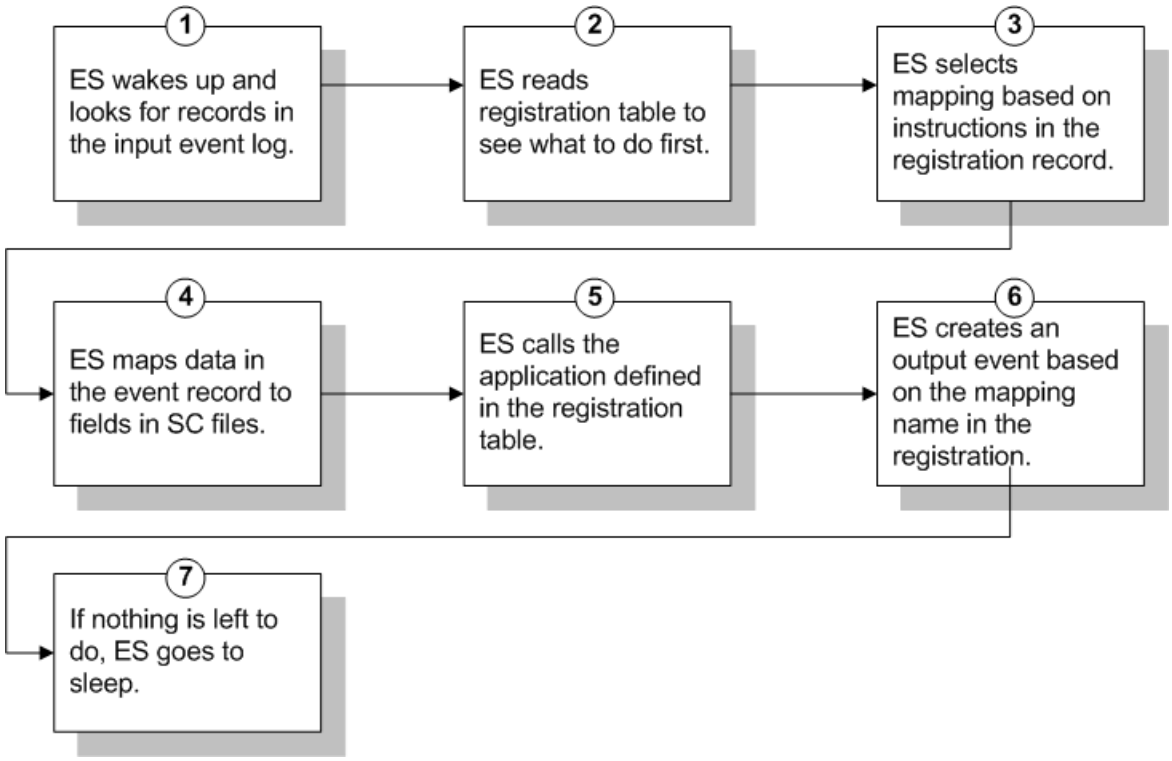
Event Services tables

Event Services uses the following tables.

Table name	Description
eventregister	Defines the events that exist in the system. Event registration records also specify the eventmaps used to process events and defines the RAD application used for processing.
eventin	Table used to move information into HP Service Manager from an external system. If a corresponding input eventregister record exists, external or internal applications can write records to the eventin table.
eventout	Table used to move information from HP Service Manager into an external system. A specific type of an eventout record can be written only if a corresponding output eventregister record exists.
eventmap	Defines how information is parsed. Eventmaps define individual fields and create condition statements for eventin and eventout records. Many eventmap records can exist for each eventregistration record.
eventfilter	Prevents duplicate events. Filters block incoming events based on defined criteria to prevent external systems from creating many eventin records for the same item in a short amount of time. Filters can block events by time frame, item, or location.

Event Services workflow

HP Service Manager Event Services has the following workflow:



Phase	Details related to the phase
1	Event Services (ES) uses a scheduler called event. You start and stop the event scheduler like any other HP Service Manager scheduler and process events in background or asynchronously.
2	The event registration file contains all of the information Event Services needs to determine what to do with each event.
3	Mapping records contain instructions to move data from the eventin record to fields in HP Service Manager files.
4	Based on instructions in the mapping records, a data structure is built.
5	A multi-purpose call routine is issued to the application named in the registration record, along with any necessary variables.
6	When the application has completed, an output event is created and added to the queue, if instructed by the registration.
7	If Event Services has nothing left to do, it sleeps for an interval, then reawakens to look for more work.

Event Services operations

Event Services has the following actions.

Action	Description
Review Agents	Opens the Event Scheduler and displays the details of scheduled system events.
Send Email	Initiates an e-mail event.
Write an Output Event	Initiates the event create script and prompts you to select the type of external event: Incident, Inventory or Generic (message).

Registered events

Each event has a record in the eventregister table. Each event record includes a unique event code and a sequence number. A single event can start a series of applications. Each event record also contains initialization statements, mapping information and instructions for calling the HP Service Manager application. Registration is necessary for all input events that external applications process.

Example

Records in the eventregister table contain unique identification codes. The *pmo* code identifies opening an incident. When a pmo event occurs, Event Services calls the axces.apm application if the condition is true. The event parameters are passed by name and value. The Map Name identifies the event map to use when mapping the information into HP Service Manager tables.

The event registration record contains expression statements that create different queries, depending on the source of data. For example:

```
$ax.query.passed=nullsub("flag=true and network.name=\""+2 in $axces.fields+"\"",
"false")


if (index("axmail", evuser in $axces)>0) then ($ax.query.passed=nullsub("flag=true
and logical.name=\""+1 in $axces.fields+"\"", "false"))
```

The query uses network.name to select open incidents for update. The SCAuto mail incident event uses logical.name.

The pmo event registration record instructs Event Services to:

- Select a record from the probsummary file (based on the query in $ax.query.passed).
- Map data from the eventin record ($axces) based on the incident open (evmap in $axces.register) map record.
- Open an incident.

In most standard Event Services input applications, the first two parameters passed are the event record and the name of the event map. An exception in standard HP Service Manager SCAuto applications is e-mail, which passes the mail record and the delimiter character.

View registered events

Applies to User Roles:

System Administrator

To view registered events:

1. Click **Tailoring** > **Event Services** > **Registration**.
2. Click **Search**.
3. Select an event registration record to view its details.

Add a registered event

Applies to User Roles:

System Administrator

To add a registered event:

1. Click **Tailoring** > **Event Services** > **Registration**.
2. Complete the top-portion of the Event Registration form.
3. Provide the appropriate information on each tab: Expressions, Basics, Application.
4. Click **Add**.

Note: You can delete any registered events added by administration users, but you cannot delete any out-of-box events.

Input events

The eventin table contains input event log records. It contains a record for every event detected, but not filtered, by SCAutomate external applications. Each record contains the event code, a unique system ID and a time stamp. During the input event, data passes to HP Service Manager in a character string using a delimiter character to separate fields.

Input event processing

An external application inserts all records in the eventin table and external programs manipulate the eventin records. For example, SCAutomate supports an event named email. External sources can send electronic mail and pass it to HP Service Manager mail. The sources for electronic mail can be external e-mail systems, alert monitors, or other programs that can send messages. The external SCAutomate application packages the data in a standard format and stores it in the eventin file. Eventmap records specify the format of the data.

Processed records in the eventin table do not contain a First Expiration value. Normally, Event Services deletes event records after they are processed unless they are filtered or an exception occurs during processing. There is a condition set in the eventregister table that controls the delete flag.

If an error occurs due to Format Control processing, event processing terminates for that event and Event Services writes the specific error message to the eventin Messages log and to the HP Service Manager msglog file.

After you install and test SCAutomate, do one of the following:

- Set all delete flags in the eventregister records to true.
- Use the HP Service Manager purge/archive routines to schedule cleaning up the eventin table on a regular basis.

View Event Services input events

Applies to User Roles:

System Administrator

To view Event Services input events:

1. Click **Tailoring** > **Event Services** > **Input Events**.
2. Click **Search**.

3. Select an input event record.

Output events

The eventout table contains output event log records. It contains one record for each event processed by Event Services applications and instructions that the external software uses. This type of data passes to external applications in a character string with a delimiter character to separate fields.

Output event processing

External programs manipulate the eventout records.

Expired events

Processed records in the eventout table do not contain an expiration date. Normally, Event Services deletes events from the eventout table after processing unless an error occurs. You can manipulate a flag in the external IPAS or SCAutomate software to cause record deletion after a read operation; however, because multiple SCAutomate processes can read the same record, it is not always feasible to delete the record after each read operation. HP recommends that you use scheduled HP Service Manager purge/archive routines to clean up the eventout table on a regular basis.

View Event Services output events

Applies to User Roles:

System Administrator

To view Event Services output events:

1. Click **Tailoring** > **Event Services** > **Output Events**.
2. Click **Search**.
3. Select an output event record.

Generic events

Generic event options enable you to manage outgoing event records into Connect-It, including:

- Editing eventout information generation
- Exporting configuration records
- Exporting database dictionary structures

E-mail events

A standard e-mail event that HP Service Manager creates is the opening of a problem with a valid Contacts field. This event can notify individuals of a problem in their area of expertise. You also can create e-mail events using the User Services Send Mail function.

In addition to the standard creation of e-mail events in HP Service Manager, any RAD application can create an event. An example of this is implementing e-mail notification for problems that reach a specified status.

Mapping events

After creating an eventregister record for an input or output event, a mapping record in the eventmap table describes the process to manage the event. The event mapping record directs the event and its associated data to create results that are used within HP Service Manager or in an external application.

Mapping also allows complete flexibility of data manipulation during the mapping process. Because Event Services runs as a background task, no input/output routines are available for online validation with user feedback, but you can check field values and make substitutions based on processing statements.

Event mapping process

The eventmap table contains event mapping information. There are two types of maps: input maps and output maps. Input maps have information about moving data from the External Information String (evfields) field for the eventin record to the target table. Output maps have information about moving data from the source file to the External Information String field for the eventout record.

The purpose of event mapping is to relate elements in a list to fields in a record. An external event, such as SCAutomate or SCAuto for NetView, passes data in the HP Service Manager eventin file to a field called fields. Each element is separated from the others with a delimiter, or separation character. In the following example, the ^ character separates the five fields.

```
john@hp^falcon^toby;al;joe^Meeting today^Tue 12 Aug
```

Internally, Event Services converts this string to a list ($axces.fields).

```
john@hp
falcon
toby;al;joe
Meeting today
Tue 12 Augcol
```

The event processor assumes that fields with a type of date/time are in the time zone of the HP Service Manager system (that is, the time zone defined in the System Wide Company Record). If the event background process has an operator record, that time zone for that operator is used. For synchronous processing, the session processing the event handles the date/time in the time zone where it is defined.

Mapping defines the link between the elements in the internal list (evlist) and fields in a HP Service Manager file. The first field, john@hp, is mapped to the user.to field for the mail file.

Standard event maps

Out-of-box event maps describe standard events. Changing the relative position of data in the information exchanged between HP Service Manager and the external applications may cause standard events to fail. It is better to create new maps for non-standard events rather than modifying existing maps.

View event maps

Applies to User Roles:

System Administrator

To view event maps:

1. Click **Tailoring** > **Event Services** > **Maps**.
2. Click **Search**.
3. Select an event map.

Using event maps

Each record in the eventmap table describes a single field for an input or output event.

For an input event, Event Services uses information in the eventmap record to map data from an external source that it can import into a HP Service Manager table.

For an output event, Event Services uses information in an eventmap record to map data in HP Service Manager tables into a sequence of delimited fields that it can export to external applications.

Example

When a HP Service Manager user sends e-mail, specific fields in the HP Service Manager mail file are populated. These include user.to, user.from, user.array, subject and text. The event map describes the information in these fields in a standard, defined sequence to ensure that the SCAutomate mail application can translate it to external programs. When SCAutomate receives mail from an external program and posts it to an eventin record, the Event Services event map describes how to populate the required fields in the HP Service Manager mail file.

For example, the user.from field in the HP Service Manager mail record is in the second position. Through mapping instructions, it becomes the second field in the delimited text string written to the eventin record. For output, Event Services puts the contents of the user.from field in the HP Service Manager mail record into the second position in the External Information String field of the eventout record and changes the Type field to output.

If you have custom mapping records for e-mail and they are deleted, HP Service Manager uses the out-of-box e-mail eventmap record.

Mapping an array of structures

The following example shows an event string that maps information into an existing Change Management task. The last portion of the string maps data to the parts and labor array of structures fields in the cm3t table. The vertical bar (|) array separator delimits each array. Each portion of the array with the | delimiter has another subdivision using the grave accent structure separator (`).

```
T^^update^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
 ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
 ^^^THIS IS A TEST^^^^^^^^^^^^^^^^^^^20^01/01/0112:41:23`AAAA`
 11111`|```|02/02/02``22222`^03/01/02` falcon`3.5`DEFAULT US`
```

Mapping to multiple tables

Event Services also handles mapping to multiple tables. For example, SCAutomate for NetView and SCAutomate can send inventory information that is stored in more than one table. Configuration Management applications use two tables to describe each device: the entity table and the attribute table. The entity table is named device; the attribute file depends upon the device type, and is identified by the type field in the entity table. When Configuration Management information is gathered using discovery processes in external applications, Event Services passes the data to HP Service Manager using SCAutomate and updates both tables.

Example: Mapping to multiple tables

This example describes how to map to the device and attribute tables. Remember the roles of these Event Services tables:

- **The eventregister table:** Contains one record for every pre-defined event.
- **The eventmap table:** There are several out-of-box event maps for adding a new device named inventory add. Each inventory add map contains the instructions to map data for one field.

To view the inventory add map records:

1. Click **Tailoring** > **Event Services** > **Maps**.
2. Type `inventory add` in the blank **Map Name** field.
3. Click **Search**.

   HP Service Manager displays a list of out-of-box event maps named inventory add.
4. Select the inventory add event map record where the **Position** is 9 and the **Field Name** is type.
5. Click the **Expressions** tab. The following expression in the Post Map Instructions identifies the attribute table.

   ```
   $attribute.file=type in $axces.target
   ```

   This instruction sets the variable $attribute.file to the value in the type field of the device record.

If you view the first inventory add event map records, The **Sequence** is 1, and the **File Name** in the map record is device. Notice that each record identifies a different field to be mapped. Until all fields are mapped to the device file, the **Sequence** remains 1 and **File Name** remains device.

After the last field for the initial file is mapped, the record is added or updated and a new file is initialized based on the value of $attribute.file.

While $axces.target and$axces.field have special meaning within Event Services, $attribute.file is an arbitrary global variable name.

When all fields are mapped into the device file, the next map record has a Sequence of 2, the File Name is different and a Query is supplied.

- File Name now contains the value assigned to the $attribute.file variable.
- Query tells Event Services how to select the record to update from the file identified by $attribute.file. The query can be either a literal statement (as shown in the previous example) or a variable set in previous Post Map Instruction or Initialization fields.

The first mapping for the new file is logical.name, which is stored in Position 1 (as shown in the previous example) of the evfields array field, which is represented by the $axces.fields variable in the eventin record.

Subsequent map records move data from the eventin record to the new file. When updating an existing record, Event Services substitutes the value in the original record for a null value passed from the eventin record.

Build an event map

Applies to User Roles:

System Administrator

To build an event map:

1. Click **Tailoring** > **Event Services** > **Build New Map** to open the Build Event Mapping form.
2. Type the map name and source table name, and click **Next**.
   Once you have selected a table, HP Service Managerdisplays a screen that allows you to build the event map for the table you selected. A list of field names and data types for the table you selected is displayed.
3. To delete a field before building the map, select the field from the list, and click **Remove Field**.

   Note: If an array field is part of your mapping, delete the second instance of the field in the list presented when building a new map, leaving only the array field.
4. To view the details of the event map, click **Select Map**.
5. Click one of the following options to build a map:
   - **Build Input:** Builds the records that map information from the eventin file to the selected HP Service Manager table.

- **Build Output:** Builds the records to map information from the selected file to a formatted string to be passed to SCAuto using the eventout table.

Using expressions in event maps

You can check field values and make substitutions based on processing statements.

For example you can use the following expression to check field values and make substitutions based on processing.

```
if (logical.name in $axces.target="UNKNOWN")
then (logical.name in $axces.target=network.name in $axces.target)
```

or

```
if (logical.name in $axces.target=NULL
then (logical.name in $axces.target="?"+str(tod()))
```

In this example, the value the value in network.name replaces logical.name if logical.name is UNKNOWN. The second statement sets logical.name to a constant if it is NULL.

Other common uses for expressions are to set the value of a field to the current date and time and to calculate a value based on information in the record. Event Services applications handles data type and case conversions as long as the Field Type field is correctly identified and the data is written to the descriptor structure.

You can use a single Format Control record named login.event to establish initial global variables (such as lists of valid operators) when the event agent is started, just as you can for users when they log into HP Service Manager.

If you are writing data to a field whose name exists in more than one structure in a record, you must explicitly name the field. For example, if you add a field named assignment to the middle structure of your incident database dictionary record and you want to manipulate that field, you must identify it as middle,assignment. The field must exist in the target file before any instruction can manipulate it. Ensure the data type is correctly identified.

Mapping and Configuration Management

While HP Service Manager provides both an entity file (device) and attribute files (for example, server), it is not necessary that both files exist to represent the characteristics of every device type. You can often fully describe a device using only the fields in the device file.

The map record for the type field (field #9 in standard events) defines how HP Service Manager selects and displays information about a device once the data is added. The type field in the device file refers

directly to the associated attribute file of each device. If no attribute file associated with a device, the type field must contain device or be empty (NULL).

Similarly, the format.name field in the device record defines the name of the form that displays the device within HP Service Manager and, by extension, the name of the join file that temporarily stores information for review and update. The formatctrl record for the format name stored in the device record must contain device as the file name for all device types that do not have associated attribute files.

If an external agent detects an unknown device type, HP Service Manager processes the event, updating the device file with the information provided. If no attribute file exists for that device type, a Warning message is written to the Message list for the event but the device is still added or updated in the HP Service Manager data repository. If event mapping indicates processing in more than one table, but the number of fields passed to the event is less than the position of the first field in the second table, there is no attempt to open the second table.

Considerations for Configuration Management maps

While HP Service Manager provides both an entity file (device) and attribute files (for example, server), it is not necessary that both files exist to represent the characteristics of every device type. You can often fully describe a device using only the fields in the device file.

The map record for the type field (field #9 in standard events) defines how HP Service Manager selects and displays information about a device once the data is added. The type field in the device file refers directly to the associated attribute file of each device. If no attribute file associated with a device, the type field must contain device or be empty (NULL).

Similarly, the format.name field in the device record defines the name of the form that displays the device within HP Service Manager and, by extension, the name of the join file that temporarily stores information for review and update. The formatctrl record for the format name stored in the device record must contain device as the file name for all device types that do not have associated attribute files.

If an external agent detects an unknown device type, HP Service Manager processes the event, updating the device file with the information provided. If no attribute file exists for that device type, a Warning message is written to the Message list for the event but the device is still added or updated in the HP Service Manager data repository. If event mapping indicates processing in more than one table, but the number of fields passed to the event is less than the position of the first field in the second table, there is no attempt to open the second table.

Rules for building maps

For best results when building new maps that use array fields, follow these guidelines:

- Select the first instance of any array fields (such as user.array in the mail file) so the proper type is built for the field.
- Only scalar and array fields can be directly mapped; all other types must be manipulated using expressions.

If possible, build maps first and then design external applications to use the maps.

Filtering events

Event filtering information is stored in the eventfilter file. This file instructs SCAuto when to block incoming events. If an event is not blocked, filters also can prevent opening incident records based on recurrence intervals and counts, and on incident intervals.

The number of filters available for external blocking is unlimited. The external process (SCAuto) reads the eventfilter file to select records with the same Event Code and User Name (or User Name=NULL) and with Block Events?=true until it finds one that satisfies the criteria for the event being processed. If none is found, the event is inserted in the eventin file.

Once records are added to the eventin file, Event Services assumes the filtering task using Internal Filters. Event Services first selects the filter with the same Event Code as that of the event being processed and with a Network Name of SCAuto. This filter must contain all internal blocking conditions. If an eventin record satisfies one of the Block Conditions, it is updated to reflect a Status of blocked. The event action (for example, incident open or inventory add) does not take place.

With incident open event types (pmo), the Additional incident Filters take effect if no blocking condition exists. This filtering mechanism is available only when opening new incidents.

View event filters

Applies to User Roles:

System Administrator

To view event filters:

1. Click **Tailoring > Event Services > Filters**.
2. Click **Search**.
3. Use the External Filters, Internal Filters, or Additional Incident Filters tab to view the appropriate filter types.

Event blocking

The external SCAuto application use the External Filters tab of the filter record to prevent the insertion of eventin records in the HP Service Manager database. The contents of the User Name field must either match that of the external process or be empty (NULL).

The Block Events? condition must be set to true to prevent records from being added to the eventin file. The Start Blocking at and End Blocking at values are optional, however they allow for a block to be placed over a specified time frame allowing a more customized administration.

Event blocking with conditions

You can also prevent the insertion of events for specific network devices, domain names and error types by using the Index, Value, and Condition fields. Use these fields independently or in conjunction with the Start Blocking at and End Blocking at fields to populate other fields on the form.

- Index refers to the position of the data in the event message.
- Value refers to the actual data contained at that position.

For example, a pmo event contains the following message:

```
hp^hp^^6 58916865^Node Down^^^^SNMP
Trap(IPAS)^net.hware^^^^^^^^^^
```

The caret (^) character separates fields in the message. The first field, which references the logical name of the device, contains hp. To block the insertion of all incident open events reported for the device hp, type pmo in the Event Type field, 2 in the first Index field and hp in the first Value field.

Note: Only Index values of 2 or 3 are supported for incident open actions.

Example: Event blocking with conditions

This is an example of event blocking from two servers, hp and falcon.

To block incident open events from both hp and another server named dolphin, select or in the Condition field, 2 in the second Index field and dolphin in the second Value field on the External Filters tab. If you specify a condition (AND or OR), then you must complete both Index and both Value fields.

To prevent insertion of records in the eventin file, the Block Events? field must be true (checked).

To specify a time range for blocking, set the Start Blocking at and End Blocking at fields. In this example, use 08:00 for start blocking and 17:00 for end blocking.

With these settings, all inventory add (icma) events are blocked between 08:00 and 17:00 if they come from either the hp or dolphin server. This action avoids unnecessary adds and updates if installation activity is scheduled to occur on the network during this time.

Selecting filters

Filters are selected using the following search criteria and in the order listed:

- The Event Type is the same as that of the event being processed . The Network Name is the same as the network name specified in the eventin record. The Cause Code is the same as the cause code specified in the eventin record.
- The Event Type is the same as that of the event being processed. and the Network Name is the same as the network name specified in the eventin record.
- The Event Type is the same as that of the event being processed and the Network Name is AXCES and the Cause Code is the same as the cause code specified in the eventin record.
- The Event Type is the same as that of the event being processed and the Network Name is AXCES.

Example: Selecting filters

This example demonstrates how you can set up filters on the Additional Incidents Filter tab to block events.

The following is the event example:

```
hp^hp^^6 58916865^Node Down^^^^SNMP
Trap(IPAS)^net.hware^^^^^^^^^^
```

The queries are:

```
evtype="pmo" and evnetnm="hp" and evcode="6 58916865"
evtype="pmo" and evnetnm="hp"
evtype="pmo" and evnetnm="AXCES" and evcode="6 58916865"
evtype="pmo" and evnetnm="AXCES"
```

You can permanently block problem open by entering a Network Name or Cause Code. This has the same effect as a Block Condition except that the status in the eventin record is filtered rather than blocked.

For example, using hp for Network Name and SNMP 2.0 for Cause Code. This prevents any events from server hp with cause code of SNMP 2.0 from opening a problem.

You can further refine the filter by entering an Event Interval and Recurrence Count. For example, if you set Event Interval to ten minutes and Recurrence Count to 3, the filter prevents any events from server hp with cause code of SNMP 2.0 from opening a problem unless three events are received within a ten minute interval.

Event Services and Change Management

The Change Management application of HP Service Manager is fully supported by Event Services. This allows users outside of the HP Service Manager system to perform all standard functionality of Change Management from an external system, for example, SAP or PeopleSoft. The Event Services implementation is bidirectional, allowing external systems to synchronize with the HP Service Manager system.

With Event Services, HP Service Manager uses input and output events to transfer data in and out of Change Management.

You should have an administrator level of knowledge of Change Management and Event Services to use Event Services with Change Management.

Change Management input events

A correctly formatted eventin record must be created within HP Service Manager to use an external system to produce an action within the HP Service Manager Change Management application. You can format the eventin record with an SCAutomate product.

Change Management eventin fields

The eventin record fields specific to the Change Management implementation are:

Field	Description
Event Code (evtype)	Name of the corresponding Event Registration record to use for this event. This must always be cm3rin for changes and cm3tin for tasks.
User Name	User name in this field is interpreted as the operator for this event. The Change

Field	Description
(evuser)	Management environment used depends on which user is entered in this field.
External Information String (evfields)	Delimited data fields that correspond to a specific event mapping.

Change Management input event registration

Change Management uses events cm3rin and cm3tin for input events. One of these two event codes must appear in the eventin record, depending on whether the event is related to a change or a task.

External information string

The external information string, or EIS, is the evfields field of the eventin record. This field carries the specific data of the change or task into the HP Service Manager system. These fields are placed in a single string with a user-specified separation character (the default is the ^ character). The first four fields contain specific functions that determine which change/task is being processed and what action the system should take. These fields are passed in a specific order.

Sequence	Field Description
1	Change/Task number of the object to be acted upon. This field is blank when opening a change or task.
2	The foreign ID. This field is the identifier of the change or task used by the external system. This field is used if a different number is used outside of HP Service Manager.
3	Action Token indicates which logical action to take, either: open, update, close, reopen, approve, unapprove, disapprove.
4	The Change Group or operator performing an approval action. It is only used for approve, unapprove, or disapprove.

The data fields in the EIS contain field-level data that Event Services uses to populate the change or task record being processed. If the action performed is not an open, these fields write over any existing data in the change or task. If a field in the EIS is blank, the existing data in the change or task is used. The exact field that each piece of data corresponds to can be determined by examining the proper input event map for changes (cm3r) or tasks (cm3t).

External information string fields

The first two external information string (EIS) fields determine the unique identifier of the change or task both in HP Service Manager and in an external system (if applicable).

The first field contains the unique number that corresponds to the number field in the cm3r or cm3t database dictionary. This field is blank if the action is open.

The second field of the EIS corresponds to the foreign.id field of the change or task. This field specifies the unique identifier of the change or task in the external system that is sending the request. If the HP Service Manager number is not specified, the system attempts to find the correct record by comparing the foreign.id to this field.

External information string actions

Event Services uses the third field of the external information string (EIS) to determine what type of action to perform on the specific change or task specified by one of the first two fields. The following table describes the supported actions.

Action	Description
approve	Approve a change or task.
disapprove	Disapprove a change or task.
unapprove	Unapprove a change or task.
open	Create a new change or task.
update	Update an existing change or task.
close	Close current phase and advance to the next phase, if applicable.
reopen	Reopen a change or task in the current phase.

When the action is an approval action (either an approve, disapprove, or unapprove), the Change Management Group or Operator Name that is performing the approval action must be specified in the fourth field of the EIS. The group or operator specified must match one of the approval groups specified in the change or task record for the approval action to complete properly.

Synchronizing with an external system

When HP Service Manager is used with a separate external system, the changes and tasks must be synchronized between the two systems. Event Services supplies two methods of sending output to the

external system for this task.

First, a simple acknowledgment can be sent to the external system. This acknowledgment contains enough data to map the HP Service Manager change or task number to the unique ID used in the external system, along with enough messages to determine if the input event was successful.

Alternatively, a complete output event may be sent to an external system in order to synchronize every piece of data between the two systems.

Acknowledgement events

The cm3rinac and cm3tinac event registrations are used as acknowledgement events to synchronize the unique numbers of each system when HP Service Manager is used with an external system.

Event Code	Input/Output	Event Map	Application	Description
cm3rinac	Output	cm3ack	axces.write	Used for changes.
cm3tinac	Output	cm3ack	axces.write	Used for tasks.

Both event types use the cm3ack event map definition. The following table shows the mapping passes the fields in the external information string (EIS) of the eventout record.

Sequence	Field description
1	The change or task number of the object being acknowledged.
2	The foreign ID. This is the identifier of the change or task used by the external system. This field is used if a different number is used outside of HP Service Manager.
3	Action Token indicating which action was performed on this object (open or update, for example).
4	The status of the eventin record created by the original event. This field may be used to determine if there were any errors encountered when processing the original event.
5	An array of up to five messages sent during the original event (example: Change 15 updated, Location XXX is invalid). These messages can be used to determine if a Format Control or validation error occurred during the original event.

The acknowledgment events can be turned on or off in the cm3rin or cm3tin Event Registration records by modifying the value associated with the boolean1 parameter on the application tab. When this parameter value is set to true an acknowledgment event is sent out each time an input event is processed, while a setting of false keeps the acknowledgment event from being sent.

Change Management output events

The standard output events for Change Management are triggered by the cm3messages file. When the change scheduler processes a cm3message, the value is checked in the Event Services Reg (axces.out) field in the corresponding cm3message record. If the value matches an output event (most likely cm3rout or cm3tout), that event is processed and an eventout record is written. This gives an administrator great flexibility when deciding what types of events (opens or alerts, for example) cause the output event to be written.

The output maps used for these events are cm3r and cm3t. These maps correspond to their related input maps with the exception of the third and fourth fields. The third field contains the name of the event that caused the event to process (for example, cm3r open or cm3t update). The fourth field is used as a place-holder to keep the data fields of the input and the output event synchronized and always contains the words not used.

Example: Open a change

This example uses the following parameters:

- category for adv-nam-desk-101 - Hardware
- external foreign ID - CM01
- requested by - System.Administrator
- assigned to - Servicedesk.Agent

The change contains a simple description while letting all other fields use default values.

The event register has the following specific fields:

- evtype is cm3rin
- evuser is System.Administrator

The external information string (EIS) is:

```
^CM01^open^^^Hardware^^^System.Administrator^^^^Servicedesk.Agent^^^^^^^^^^^^^^^^^^
^^^^
^^^^^^^^Move HP Pavilion M9160Elite to Mike's
office.^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^adv-nam-desk-101^^^...
```

The field positions correspond to the cm3r input event map as follows:

Position	Field name	Value
2	foreign.id	CM01
3	actiondummy	Open
6	category	Hardware
9	requested.by	System.Administrator
13	assigned.to	Servicedesk.Agent
42	description	Move HP Pavilion M9160Elite to Mike's office.
76	logical.name	adv-nam-desk-101

Event agents

Automatic monitors within HP Service Manager, known as agents, can be set to collect data and create events appropriately within the system. You can use the Event Scheduler to set up these agents, or you can activate them automatically or manually (by user input).

Event scheduling

The schedule table contains a record for each SCAuto agent. It contains instructions indicating how often the agent reads a queue and which application to execute if the read returns records. You use the Event Schedule form to manage event agent operations.

When the event agent starts, the event schedule record must have a class of event (or the name you specify for the event scheduler) and must have an expiration earlier than the current time. Set the expiration to the current date and time before starting the scheduler.

Since the event scheduler is a serial process, you may want to have more than one scheduler read events in the event queue, particularly when inventory activity is high, preventing incident management activity.

Use the Query field to further define what type of event to select from the eventin file. The user-specified query entered in the schedule record is appended automatically to the default event scheduler query, evtime<=tod(), to form a more specific query. If the Query field is left blank, only the default query is applied.

Note: The system always places the time portion of the query in front of the user-specified query.

If you define a query for use against the eventin file, ensure it is fully-keyed for maximum performance.

The agent processor attempts to restart any applications that ended while running (that have a status of application running). If you change for one of your agents, ensure there are no other agents with the same schedule class and a status of application running.

View event schedules

Applies to User Roles:

System Administrator

To view event schedules:

1. Click **Tailoring> Event Services > Review Agents**.
2. Select an agent from the list to open the Event Scheduler for the agent.

Agent status

From Event Services you can start and stop any SCAuto or event agent without respect to your client status as long as the HP Service Manager problem agent is active. Using this feature, agents are scheduled to start, and the problem agent is their activation agent. The specific agents controlled from this option include:

- Event
- Axces
- NAPA
- SCAuto Server
- SCEmail

View Event Services agent status

Applies to User Roles:

System Administrator

To view Event Services agent status:

Click **Miscellaneous** > **System Status**.

The **event** process shows a Last Expiration time and an Idle time. The Last Expiration time is the initialization time for the agent; the Idle time is the amount of time elapsed since the agent last woke up to check for work.

If an agent is inactive, there is no Last Expiration or Idle time, and the Start button is available.

View system startup information

Applies to User Roles:

System Administrator

To view system startup information:

1. Click **System Administration > Ongoing Maintenance > System > Startup Information**.
2. Type `startup` in the Type field.
3. Click **Search**.

Service Manager email solutions

The following table describes how the following products handle Service Manager emails.

Service Manager email solution		Internal/External Product	Running Environment	Connection to SM server	Routing Direction	OS	Fetch data from	Supported email format
JavaMail		Internal	In Service Manager Server	Connects directly to the SM server	Outbound events only: sends SM email to other email systems	Windows & Unix	eventout table	Plain text, HTML email
SCAuto Mail	SCMail	External	Outside Service Manager Server	Establishes a client connection to the SM server through SM	Inbound and outbound events: supports bi-directional email	Unix	eventout & eventin tables	Plain text

				SCAuto Listener	with other email systems			
	SCMapi	External	Outside Service Manager Server	Establishes a client connection to the SM server through SM SCAuto Listener	Inbound and outbound events: supports bi-directional email with other email systems	Windows	eventout & eventin tables	Plain text

JavaMail

JavaMail provides a monitor to handle HP Service Manager e-mail events. This monitor connects HP Service Manager into standard e-mail facilities and allows HP Service Manager operators and applications to send HTML emails. Any mail system that supports Simple Mail Transfer Protocol (SMTP) or has an SMTP gateway or bridge can receive e-mail from JavaMail.

Note: Only messages enclosed within HTML tags can be sent out as HTML emails, otherwise messages are sent as plain text.

JavaMail and SCAuto Mail

JavaMail is not the same product as SCAutomate Mail. JavaMail only sends mail from HP Service Manager; it does not receive mail from external mail applications. JavaMail runs as a stand-alone application; SCAutomate Mail is an SCAutomate client adapter.

Event Services and Service Manager e-mail

The Service Manager Mail Utility checks the operator file for valid operator names before allowing mail to be sent. The Event Services version of this application expands the checking for valid users to those defined in the Service Manager contacts file.

The purpose of checking is to obtain the e-mail address from the e-mail field for the operator or contacts file. If the name for the addressee does not select a record from either file, Service Manager

assumes that there is no such addressee and does not send mail. You can override this default by creating a login.event Format Control record and, in the Calculations section, setting the add condition to true and the calculation expression to the following: `$email.noaddr.ok=true`.

This causes Service Manager to assume that whatever name is passed to the e-mail event as the addressee is the complete e-mail address and attempts to send mail using that address.

Emailout parameters in the sm.ini file

JavaMail requires the setup of Emailout parameters in the sm.ini file before it takes effect. The system administrator must set these parameters from the HP Service Manager server's OS command prompt or from the initialization file (`sm.ini`). The following example shows desired Emailout parameters for JavaMail:

- smtphost: specifies the name of the SMTP server host for client requests.
- smtpport: defines the communications port SMTP uses.
- smtpusername: defines the account name of the SMTP server.
- smtppassword: identifies the password the HP Service Manager server uses to bind to the SMTP server.
- smtpTLS: defines whether SMTP requires Transport Layer Security (TLS) authentication to send emails.
- smtpEnableSSL: defines whether SSL should be used for SMTP operations.
- smtpSSLPort: defines the port number for SSL connection.
- mailFrom: specifies the descriptive name or other identifier of the sender of an e-mail. This parameter should be set in the format of email address. Service Manager processes this parameter as follows:
    - If the mailFrom parameter is configured in the `sm.ini` or `sm.cfg` file, Service Manager always uses this value as the Mail From address for all outbound emails.
    - If the mailFrom parameter is not configured in the `sm.ini` or `sm.cfg` file, Service Manager always uses the value of the Mail From value of the eventout record as the Mail From address, without checking if the value is a valid email address.

  - If there is no mailFrom value configured in `smi.ini` or `sm.cfg` and no Mail From value in the eventout record, Service Manager logs an exception in sm.log.

- mailThreadCount: specifies the number of threads to send emails. The default value is 10.
- mailBCC: specifies a list of blind carbon copy (BCC) recipients to all emails. The value of this parameter is a comma-delimited list of user email accounts.
- SMIMEKeystore: specifies the name of the certificate in PKCS12 format placed in the server's RUN folder for enabling S/MIME signatures.
- SMIMEKeystorePass: specifies the password that is used when generating SMIMEKeystore.
- SMIMEKeyAlias: specifies the alias that is used when generating SMIMEKeystore.

Append an S/MIME digital signature to outbound emails

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a method of exchanging emails securely. With the S/MIME technology, a digital signature can be appended to email messages to ensure non-repudiation and data integrity.

Starting with SM 9.33, you can enable a mechanism in Service Manager to allow for the signing of outbound email messages using the S/MIME technology. Once you enable this feature, the recipients can verify the signature on their mail system (for example, Microsoft Outlook), to make sure that the email messages are truly originated from Service Manager without being intercepted in transit.

Prerequisites

Your system must contain the unlimited strength jurisdiction policy files for JDK to support the S/MIME signature feature.

Server platform	Actions
• Windows • Linux	No actions required. The unlimited strength jurisdiction policy files are already in the server's embedded JRE.
• HP-UX • Solaris	1. Download the JCE unlimited strength jurisdiction policy files from the Oracle website. 2. Replace `local_policy.jar` and `US_export_policy.jar` under `%java_`

Server platform	Actions
	home%\jar\lib\security with the policy files you have downloaded.
IBM AIX	1. Download the JCE unlimited strength jurisdiction policy files from: http://www.ibm.com/developerworks/java/jdk/security/index.html 2. Replace local_policy.jar and US_export_policy.jar under %java_home%\jar\lib\security with the policy files you have downloaded.

Steps to enable S/MIME signatures

To enable an S/MIME digital signature for outbound emails from Service Manager, you need to obtain or generate a PKCS12 certificate and then specify three server parameters in the sm.ini file or the emailout parameter: SMIMEKeystore, SMIMEKeystorePass, and SMIMEKeyAlias.

The following is an example of enabling S/MIME digital signatures for outbound emails:

1. Generate the keystore in PKCS12 format. For example, with the OpenSSL toolkit, you can use the following openssl command:

   ```
   keytool -genkey -keystore smemailkey.p12 -storepass smemailkeystorepass -alias smemailkeyalias -storetype pkcs12
   ```

2. Place the generated keystore file (smemailkey.p12) in the <SM Server>/RUN directory.

3. Configure these parameters in sm.ini:

   ```
   SMIMEKeystore:smemailkey.p12

   SMIMEKeystorePass:smemailkeystorepass

   SMIMEKeyAlias:smemailkeyalias
   ```

   Tip: An alternative way to set these parameters is to add the parameters to the emailout process in sm.cfg, as shown in the following example:

   ```
   sm -emailout -mailFrom:xx -smtphost:xx -smtpport:xx -
   SMIMEKeystore:smemailkey.p12 -SMIMEKeystorePass:smemailkeystorepass -
   ```

```
SMIMEKeyAlias:smemailkeyalias
```

4. Restart the Service Manager server.

JavaMail background processor

You can use these optional parameters when starting the JavaMail background processor.

Parameter	Description
-keepmail	Do not delete mail events once sent successfully.
-sleep <n>	Number of seconds to sleep between checking for events and mail. Default is 10 seconds.
-debug	Print more diagnostics to sm.log. This also turns on -keepmail.
-clean	Don't put extraneous headers in mail. Example: `HP Service Manager Operator: falcon`

JavaMail also processes the sm.ini file for additional parameters and can pass the parameters on the command line (for example, -log:file places the JavaMail diagnostics in a different file).

SCAuto Mail

ServiceCenter Automate (SCAuto) provides event management services through a collection of automation products which enable external applications to be integrated with Service Manager. SCAuto Mail provides email integration with Service Manager. It can run on both Windows and Unix.

SCMapi

SCMapi is SCAuto Mail running under Windows. SCMapi sends and receives mail using the Messaging Application Program Interface (MAPI).

SCMail

SCMail is SCAuto Mail running under Unix. SCMail sends and receives mail using the standard Unix sendmail program. SCAuto Mail can deliver mail to any address that Unix can deliver to.

For more information about SCAuto Mail and its configuration, see *HP SCAuto Applications User's Guide*.

Format Control and eventout records

When incidents are opened, updated or closed by Event Services, a record is written to the eventout file. This record contains information from the incident (described in the output eventmap record for the event) that is passed to an external process via the SCAuto/IPAS external interface. You can elect to write to the eventout file when Service Desk operators open and close records so that the information is passed to the external interface.

The axces.write application creates a character string of fields from a structure and writes them to eventout. An Event Registration record identifies the event type and the name of the Event Map records used to define which fields will be selected from the record. The application should be called as a Format Control Subroutine passing two parameters:

- The record from which data will be mapped.
- The Event Type, as defined in the Event Register.

To write to eventout on incident close, the Format Control record is attached to the `problem.equipment.close` form using the following values:

Field	Value
Application	axces.write
axces.write	true

Name	Value
record	$file
name	pmc

Note: This procedure is not specific to Incident Management. You can write eventout records for other applications, such as Configuration Management or Change Management.

Generating email messages

SCAutomate supports a generic e-mail function. Use the Format Control RAD function, message.fc, to write e-mail events to the eventout file.

Out-of-box events

HP Service Manager delivers out-of-box events with the Event Services application. HP Service Manager Event Services uses these events to open, update, and close incidents or requests. They are also used to update configuration items or change requests. You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Change Management events

Event	Event type	Description
cm3rin	input	Use this event for all incoming change events.
cm3rinac	output	This is sent if the write eventout is set to true. This returns failed events so the calling application receives notification when an error occurs.
cm3rout	output	This is created when a cm3 message is created and you enter cm3rout in axces.out.
cm3tin	input	Use this for all incoming change tasks.
cm3tinac	output	This is sent if the write eventout is set to true. This returns failed events so the calling application is notified when an error occurs.
cm3tout	output	This is created when a cm3 message fires and you enter cm3tout in axces.out.

You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Configuration Management events

Event	Event type	Description
icma	input	This event adds or updates inventory items to the device file if filter criteria are satisfied.
ICMapplication	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMcomputer	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
icmd	input	This event marks an inventory item for deletion if filter criteria are

Event	Event type	Description
		satisfied by placing inactive in the status field.
ICMdevice	input	Use this event type when you add data records to the device file. These events use the icm device eventmaps.
ICMdevicenode (1)	input	Use this event type to add or update information about a network node (a device that appears as a discrete item in a network) to the Inventory Configuration Management application. These events use the icm networkcomponents mappings.
ICMdevicenode (2)	input	If you use the ICMdevicenode event to send information to HP Service Manager, after the initial database operation completes, this secondary event registration causes a logging record to write to the eventout table.
ICMdisplaydevice	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMexample	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMfurnishings	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMhandhelds	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMmainframe	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMnetworkcomp	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMofficeelec	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMserver	input	Use this event type to add or update information about a server to the Inventory Configuration Management application. These events use the icm computer mappings (since servers are a subtype of computers, you can reuse the mappings.
ICMsoftwarelicense	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
ICMstorage	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
icmswa	input	This event adds or updates inventory items (that ServerView or StationView discovers) to the device file if filter criteria are satisfied.

Event	Event type	Description
icmswd	input	This event marks an inventory item (that ServerView or StationView discovers) for deletion in the pcfiles file if filter criteria are satisfied.
ICMtelecom	input	HP Service Manager inventory regulation event when a device of this type is added to the system.
icmu	input	This event updates inventory items if filter criteria are satisfied.
IND	input	An event that adds or updates inventory items to the device file.
prgma	input	This adds or updates a software inventory item to the pcfiles file that an external agent (other than ServerView or StationView) discovers if filter criteria are satisfied.
prgmd	input	This deletes a software inventory item from the pcfiles file that an external agent (other than ServerView or StationView) discovers if filter criteria are satisfied. The default updates the estatus field as deleted rather than removing the record from the database.

You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Incident Management events

Event	Event type	Description
epmosmu	input	This event opens an incident from a call.
epmosmu	output	This event writes the record after an incident opens from a call.
pmc	input	This event closes an incident if filter criteria are met. It uses the same path as manually closing the operation.
pmc	output	This event writes after an incident is closed.
pmo	input	This event opens an incident if filter criteria are met. It uses the same path as manually opening the incident.
pmo	output	This event writes after an incident is opened.
pmu	input	This event updates an incident if filter criteria are met. It uses the same path as manually updating the incident.
pmu	output	This event writes after an incident is updated.

You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Request Management events

You can use event registration to view details of registered events, which are stored in the `eventregister` table. The table below lists some of the out-of-box events for Request Management.

Note: This list is not all-inclusive.

Event	Event type	Description
rmlarchwaystatus	input	Used to update the backend status of a field in a line item.
rmlin	input	Provides access to Request Management line items.
rmlineitemupdate	input/output	Used to update the `quantity.returned` field of a line item.
rmoappr	input	Provides access to Request Management order approval.
rmoarchwaystatus	input	Used to update the `backend.status` field of an order.
rmoin	input	Provides access to Request Management order input.
rmorder	output	Used by Asset Manager.
rmorderupdate	output	Used by Asset Manager.
rmqappr	input	Provides access to Request Management quote approval.
rmqin	input	Provides access to Request Management quote input.
rmreceiveline	input	Used to receive a line item.

Service Desk events

Event	Event type	Description
esmin	input	This event opens a call in Service Desk.
esmin	output	This event writes a record once a call opens in Service Desk.
smin	input	Service Desk incoming service request or help issue.
smout	output	This event writes once an incoming request or help issue enters the system.

You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Service Level Management events

Event	Event type	Description
outageend	input	This event performs updates to outage records, which are part of the service level agreement (SLA) application.
outagestart	input	This event performs updates to outage records, which are part of the SLA application.
slaresponse	output	This is a request from an external application to enter a response time metric against a device with an SLA.

You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Standard events

HP Service Manager event registration currently supports events enabling integration with ERP, SAP, and other external system interfaces. The events listed in the following table provide a brief description of the event.

Standard event	Event type	Description
approval	input	This event processes approvals for Request Management and Change Management.
approval	output	This event sends approvals for Request Management and Change Management.
CTSCPY (1)	output	This event to SAP uses eventmap cm3tctsc. It is a generated message to SAP to copy a CTS Transport from one system to another.
CTSCPY(2)	input	This event from SAP uses eventmap cm3tctsc. It processes the acknowledgment of SAP CTS Copy messages.
CTSIMP (1)	output	This event to SAP uses eventmap cm3tctsi. It builds a message to request a specific SAP Instance perform an Import of a given Transport.
CTSIMP (2)	input	This event from SAP uses eventmap cm3tctsi. It processes the Input acknowledge message from SAP regarding Import of Transport.
CTSIMP2	output	This event handles scheduling of Output Import events to SAP using eventmap cm3tctsi.
CTSRQCLS (1)	input	This event to SAP uses eventmap cm3rcts. It sends a message to a SAP

Standard event	Event type	Description
		instance instructing it to release a transport.
CTSRQLS (2)	output	This event from SAP uses eventmap cm3rcts. It is a message received message from SAP acknowledging a transport release.
CTSRQOPN (1)	output	This system event sent to SAP uses the cm3rcts eventmap. It sends a message to a SAP instance instructing it to open a SAP Transport Request with specific HP Service Manager-supplied data.
CTSRQOPN (2)	input	This event from SAP uses eventmap cm3rcts. It is a received message from SAP acknowledging Transport Request creation. It closes the first phase of the Change and updates fields with data returned from SAP.
CTSRQOPN (3)	input	This input event from SAP uses eventmap cm3rctso. It is a received message from SAP sent when a Transport Request opens on the SAP side without first opening within HP Service Manager. It causes a Change to open within HP Service Manager with data received from SAP.
CTSRQUPD (1)	output	This event to SAP uses eventmap cm3rcts. It sends a message to a SAP Instance to update specific Transport Request data elements.
CTSRQUPD (2)	input	This is an Input event from SAP. It uses eventmap cm3rcts. It is a received message from SAP sent when a Transport Request has been updated on the SAP side. It is either an acknowledgment of a HP Service Manager originated request or a notification of a SAP originated action.
CTSTKCLS (1)	output	This event to SAP uses eventmap cm3tcts. It sends a message to SAP to close a Transport Task within SAP.
CTSTKCLS (2)	input	This event from SAP uses eventmap cm3tcts. It is a received message from SAP that a Transport Task closed on the SAP side. It is either an acknowledgment of a HP Service Manager-originated request or a notification on a SAP-originated action.
CTSTKOPN (1)	output	This is event to SAP uses eventmap cm3tcts. It sends a message to SAP indicating that a Transport Task opened within SAP.
CTSTKOPN (2)	input	This event from SAP uses eventmap cm3tcts. It is an acknowledgment message from SAP indicating that a Transport Task closed on the SAP side.
CTSTKOPN (3)	input	This event from SAP uses eventmap cm3tctso. This message indicates that a Transport Task opened on the SAP side within the Change Management application using data supplied from the SAP system.
CTSTKUPD (1)	output	This event to SAP uses eventmap cm3tcts. It is sent from HP Service Manager to SAP to update a Transport Task on the SAP side to match changes on the HP Service Manager side.

Standard event	Event type	Description
CTSTKUPD (2)	input	This event from SAP uses eventmap cm3tcts. It is a message received from SAP when a Transport Task update on the SAP side. It can either be an acknowledgment of a HP Service Manager- originated update or notification of a SAP-originated update.
dbadd	input	This adds an item to a specified HP Service Manager file when you satisfy the filter criteria. It updates the file if the item already exists.
dbdel	input	This deletes an item from a specified HP Service Manager file if the filter criteria are satisfied.
dbupd	input	This updates an item to a specified HP Service Manager file when you satisfy the filter criteria.
email	output	This is the standard interface to convert HP Service Manager mail to standard e-mail format.
email	input	This is the standard interface to receive external e-mail and convert to HP Service Manager mail.
epmc	input	This event uses the problem close map to initiate the problem close process associated with the Get-It interface.
epmc	output	This event uses the problem close map to initiate the problem open process associated with the Get-It interface.
epmo	input	This event uses the problem open map to write that the problem opened in association with the Get-It interface.
epmo	output	This event uses the problem open map to initiate the problem open process associated with the Get-It interface.
epmu	input	This event uses the problem open map to initiate the problem update process associated with the Get-It interface.
epmu	output	This event uses the problem update map to write that the problem updated in association with the Get-It interface.
ERPHR (1)	input	This event establishes contact with the ERP system using eventmap contactserp.
ERPHR (2)	output	This event uses eventmap contactserp.
ERPSTATES (1)	input	This event determines the state of the ERP system using eventmap stateerp.
ERPSTATES (2)	input	This event uses eventmap stateerp.
gie	input	Both Asset Manager and HP Service Manager use the Generic Input Event (GIE).

Standard event	Event type	Description
HotNews	output	HotNews defines an eventout type of HotNews.
opera	input	This event adds or updates a new user to HP Service Manager if filter criteria are satisfied.
operd	input	This event deletes a user from HP Service Manager if filter criteria are satisfied.
operu	input	This event updates items specified in a HP Service Manager file if filter criteria are satisfied.
page	output	This event registration allows HP Service Manager to create eventout records with the evtype=page.
pageclose	input	This event uses a condition statement (evfiends in $axces)#"pm".
pageresp	input	This event updates an incident with an acknowledgment or message received as response to a page. It uses a condition statement (evfiends in $axces)#"pm".
pcsoftware	input	This event allows desktop inventory products to update HP Service Manager.
PSSDELETE	input	This event deletes selected records from a HP Service Manager file.
SALESQUOTE	input	This event moves an eventin record to the eventout file and changes the evtype.
SAPGRT	output	This goods receipt Output event calls no application. It submits receipt notification to SAP system for processing.
SAPGRT	input	This goods receipt event calls submits receipt notification to SAP system for processing.
SAPGTE	input	This event updates existing line items.
SAPHR (1)	input	Event processing edits to contact file originating in HP Service Manager, routed through SAP, and returned to HP Service Manager.
SAPHR (2)	output	This event routes contact file changes to SAP.
SAPHRMD	input	This event processes SAP-originating contacts file changes.
SAPORD	input	This sales order event from SAP breaks events into appropriate constituent parts.
SAPORD	output	This sales order event to SAP calls no application. It routes order information to SAP for processing.
sapordl (1)	output	This event routes order information to SAP for processing.

Standard event	Event type	Description
sapordl (2)	input	This event routes order information to SAP for processing.
SAPORDQ	input	This is the header component of the SAPORD event.
SAPQTE	input	This sales quote event from SAP breaks events into constituent parts.
SAPQTE	output	This sales quote event from HP Service Manager calls no routine.
sapqtel (1)	output	This event is the Output quote line item component of the SAPQTE event. It uses this registration to identify which eventmap to use for message formatting.
sapqtel (2)	input	This event is the detail portion of the SAPQTE event.
SAPQTEQ	input	This is the header component of the SAPQTE sales quote.
saprecl (1)	output	This event is the output goods receipt line item component of the SAPQTE event. It uses this registration to identify which eventmap to use for message formatting.
SAPREQ	input	This purchase requisition event is from SAP.
SAPREQ	output	This purchase requisition event from HP Service Manager calls no application.
sapreql (1)	output	This event is the output request line item component of SAPREQ. It uses this registration to identify which eventmap to use for message formatting.
sapreql (2)	input	This event is the detail portion of the SAPREQ event.
SAPREQO	input	This event is a SAPREQ component from SAP.
ScAcBrand	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager vendor file to the corresponding Asset Manager file.
ScAcCompany	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager company file to the corresponding Asset Manager file.
ScAcContacts	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager contacts file to the corresponding Asset Manager file.
ScAcDept	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager department file to the corresponding Asset Manager file.
ScAcDevice	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager device file to the corresponding

Standard event	Event type	Description
		Asset Manager file.
ScAcLocation	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager location file to the corresponding Asset Manager file.
ScAcModel	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager model file to the corresponding Asset Manager file.
ScAcModelBundle	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager model file to the corresponding Asset Manager file.
ScAcModelVendor	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager modelvendor file to the corresponding Asset Manager file.
ScAcVendor	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager vendor file to the corresponding Asset Manager file.
ScAcVendorBACK	input	This event allows HP Service Manager and Asset Manager to integrate data from the HP Service Manager vendor file to the corresponding Asset Manager file.
submit	output	This event submits a job for processing.
sysbull	input	This event adds a new System Bulletin to HP Service Manager if filter criteria are satisfied.

You can use event registration to view the details of each registered event, which are stored in the eventregister table.

Dynamic Data Exchange (DDE)

Create DDE client support in a Service Manager RAD (Rapid Application Development) application.

DDE support in Service Manager works two ways: create a DDE script to call against Service Manager from a Windows application or create a script using the DDE script panel to make a DDE call within Service Manager. The difference is which application originates the call. For example, a Service Manager client in a Windows environment can push information to Microsoft® Excel or Excel can pull from Service Manager.

Note: Prior to version 9.30, Service Manager used client-side DDE to export data to Excel. As of version 9.30, the Export to Excel functionality has been redesigned so that the Service Manager server process exports the data as a CSV (comma separated file) on the server side and transports the file to the client side. The Service Manager client saves the file on the client system and launches Microsoft Excel to display the content of the file. With this redesigned functionality, the Service Manager server and client performance are both improved by using file exchange and eliminating XML exchange for exported data.

Service Manager DDE server support provides an interface to applications outside Service Manager, allowing the use of DDE functions like poke and execute.

Architecture

In the case of Service Manager Telephony (standard system), the following occurs when a phone call comes in to the Windows client (Web Client):

- RTE (Java telephony applet) generates a ReceiveInteraction event

  Note: In the Web client, the Java telephony applet prompts the user to save before receiving the call.

- RTE (Java telephony applet) passes the event to the System Event Handler (SEH)
- SEH starts the us.router RAD application in a new RAD thread

When you make a phone call, the RAD application sends a MakeCall event to the SEH, which invokes an RTE function (Java telephony applet).

While system events are normally communicated between the application layer and the RTE (Java telephony applet), they can also pass events between RAD applications and between RTE (Java telephony applet) functions.

To send a system event from RAD, use the event.send RAD Command panel. You must use -2 as the Thread ID. Fill in the Event Name with the name of the event and pass any parameters in the Names and Values arrays. Since each event is arbitrary, so are the parameters it requires.

When receiving a system event in a RAD application, use the event.name() and event.value() functions to get the event name and parameters for that event.

DDE client

There are six different actions associated with a DDE client conversation that initiate from a DDE RAD panel. The actions are the standard DDE actions:

- Initiate
- Advise
- Request
- Poke
- Execute
- Terminate

Note: Constructing a DDE RAD application requires you follow RAD conventions. For a complete description of programming in RAD, along with requirements for any RAD application to function, refer to the System Language help in the Tailoring module.

DDE RAD panel

The DDE RAD panel performs DDE commands. The RAD start panel sets variables referenced on this panel and later in the RAD application.

DDE server

Integration with external Windows applications is achieved using the DDE server functionality of the HP Service Manager 32-bit Windows client.

Applications that implement the Microsoft Windows DDE server permit external applications to get and set data, as well as execute commands. Typical use of get and set is to inspect and change data that is part of a document. For example, Excel allows the contents of spreadsheet cells to be read and written. Use the DDE execute facility to issue commands such as File > Save. There is little standardization between DDE server applications either in capabilities offered or the formatting of the commands sent over the DDE link.

DDE clients contact DDE servers using an application and topic name. The application name must be unique on the machine and the topic is typically the name of a document or the “Actions” topic.

Implementation—system events

System events permit HP Service Manager to react to events on client platforms external to the HP Service Manager system. System events are an arbitrary set of events that are sent to and from either RAD or the RTE. They are used to start new RAD applications.

DDE server implementation provides the DDE execute facility. HP Service Manager’s DDE service name is "HP_Service_Manager" and the topic name is "Actions". The DDE execute facility initiates HP Service Manager system events.

For example, the CTI implementation creates a system event to start a RAD application when the phone rings to handle the call. RAD programs written to extract the system event parameters and act upon them handle system events. With the DDE server functionality, an external application such as Excel, Access, or Delphi, connects to HP Service Manager using application HP Service Manager and topic Actions to trigger system events.

Editable events

Access to editable system events is through the pmtapi file that can be configured to pass any user-defined field value to an external application.

Event Name	pmtapi Record	Routing Application	Application Called
ReceiveInteraction	incident	us.router	cc.first
ReceiveInteractionList	incident list	us.route.list	cc.list.incident
ReceiveIncident	problem	us.router	apm.first
ReceiveIncidentList	problem list	us.route.list	apm.list.problems
ReceiveRequest	ocmq	us.route	ocmq.access
ReceiveRequestList	ocmq.list	us.route.list	ocmq.access

Events in the standard system

The standard system provides a number of predefined system events. These events are of two types:

- Hard coded
- Editable

Executes

Executes are the DDE mechanisms for requesting that an application process data or perform an action. Service Manager provides two execute capabilities:

- Transact
- SetFocus

Transact

The Transact execute function directs Service Manager to execute a transaction as though a user had pressed a function key or button. The Transact execute function requires one operand that designates the number of the function key or button ID of the button that was pressed. This example in Visual Basic for Applications shows how to tell Service Manager that the “fill” key was pressed:

```
DDEExecute nChannel, “[Transact( ““9”” )]” ’issue a fill command
```

SetFocus

The SetFocus execute function directs Service Manager to place the focus in a named widget (using the field’s input property as the name). This example in Visual Basic for Applications shows the focus set to the file name input field in the data base manager format:

```
DDEExecute nChannel, “[SetFocus( ““file.name”” )]” ’
```

FrameRestore option

The FrameRestore option directs Service Manager to take the focus when a DDE advise hot link updates. For example, if the FrameRestore parameter is added to an advise DDE RAD panel, a software telephone being used by an agent to receive a call takes the focus. This allows the agent to answer the call without searching for the soft phone application.

To activate the FrameRestore option in RAD, enter FrameRestore as the fifth input value parameter in the appropriate DDE advise panel.

Hard-coded events

There are currently 12 hard coded system events whose parameters are not user definable. These events exchange data with applications external to Service Manager through the use of Dynamic Data Exchange (DDE) conversations.

The following hard coded system events pass predetermined field values to external applications:

Event Name	Application Called	Parameter
EditChange	dde.editcm3request	Number
EditChangeTask	dde.editcm3task	Number
EditInteraction	dde.editincident	Number
EditOCMLineItem	dde.edit.ocm.lineitem	Number
EditOCMQ	dde.editocmq	Number
EditOCMRequest	dde.edit.ocm.request	Number
EditIncident	dde.editproblem	Number
ListChanges	dde.listcm3r	Query
ListIncidents	dde.listproblems	Query
ShowChangePages	dde.show.change.pages	Number
ShowPages	dde.showpages	Number
ShowTaskPages	dde.show.task.pages	Number

PassFocus option

The PassFocus option directs Service Manager to pass the focus when a DDE terminate command issues. For example, if the PassFocus parameter is added to a terminate DDE RAD panel, the focus stays on the receiving application and focus does not return to Service Manager. Without the Passfocus command, Service Manager gains the focus.

To activate the PassFocus option in RAD, type PassFocus as the second argument of a DDE terminate panel.

Process panel

A process panel is a type of RAD panel that initializes or sets variables used later in your RAD application. Process panels also process expressions.

Requests and pokes

Requests and Pokes are DDE mechanisms for obtaining a copy of or setting the value of named items. Service Manager uses the widget's input property to name the item. For example, to set the user name on the Service Manager login screen, use the following DDE command (this example is in Visual Basic for Applications): `DDEPoke nChannel, "$user.id", "falcon"`

Requests and pokes take and return string type data.

Structure support option

The structure support option allows a DDE advise action to use a user-defined data format. For example, DF,129, UL, I, SZ33. All values are comma delimited.

Sample values:

Value	Description
DF	Identifies the string as a data format
129	Integer value for the clipboard data format value required for the advise action.
UL	Unsigned long integers
I	Integers
SZ33	Null terminated string 33 characters long

SystemEvents file

You define system events in the SystemEvents file. This file contains records that have an Event Name and a RAD Application name. When the system receives an event, the corresponding RAD application invokes a new RAD thread. The SystemEvents file contains all the events that invoke a RAD application. The events used to invoke a RTE function register themselves upon start-up of the client. If you edit a system event record, you must re-login before the system recognizes the changes.

Note: You can have multiple records for one event; each application invokes a separate RAD thread.

Usage notes

To use the DDE Server functionality, the Service Manager Windows client must be started and a user should be logged in. DDE does not automatically start the server (as OLE does). The user must be logged in so that the environment is set up for the Service Manager user.

The DDE server can also handle DDE client transactions that perform:

- Requests: Get the value of a named item and return it as a string
- Pokes: Set the value of a named item
- Executes: Ask the GUI to execute a transaction or set the focus to a named item

Use this functionality to script user interaction for common operations such as closing a record, which may require several fields to be filled in and several transactions to be made.

DDE example

This example uses Visual Basic for Applications.

Note: The Service Manager server must be running in order for the following example to work.

The format of the Service Manager execute command string for system events is:

```
SystemEvent( event name, parameter name, parameter value, ...)
```

Where *event name* corresponds to the event name in the Service Manager SystemEvents table and *parameter name / value pairs* are known to the RAD program.

```
Sub ReceiveInteraction()
       channel = DDEInitiate("Service Manager", "Actions")
       DDEExecute channel, "[SystemEvent(""ReceiveInteraction"", ""Caller Name"",
""KENTNER"" )]"
       DDETerminate channel
       End Sub
```

The example above:

- Initiates a conversation with the Service Manager system.
- Executes a DDE command starting the system event ReceiveInteraction, passing the parameter name Caller Name with the parameter value of Kentner.
- Terminates the conversation.

DDE script example

The following example, written in VBA, illustrates a DDE script that takes a user directly to the Database Manager from the login screen. Before executing this script, you must be on a Service Manager login screen.

```
Sub SC()
       Dim nChannel As Long
       Dim strReturned As String
       nChannel = DDEInitiate("Service Manager", "ActiveForm")
       DDEPoke nChannel, "$user.id", "falcon"
       DDEExecute nChannel, "[Transact( ""0"" )]"' login
       DDEExecute nChannel, "[Transact( ""1"" )]"' go to the command interface
       DDEPoke nChannel, "$command", "db"' go to the Database Manager
       DDEExecute nChannel, "[Transact( ""0"" )]"
       DDEExecute nChannel, "[SetFocus( ""file.name"" )]" ' set the focus in the file
name box
       DDETerminate nChannel
       End Sub
```

Edit an event using pmtapi

1. Click **Tailoring** > **Database Manager**.
2. Type `pmtapi` in the Table field.
3. Click **Search**.
4. Type a name of a `pmtapi` record. For example, type `ReceiveInteraction`.
5. Click **Search**.

   The requested record opens.

6. Add or delete field names.

   These names must match fields listed in the database dictionary record of the file that the event is used.

7. Select the data type of the field from the drop-down list.

   This data type must match the data type of the field in the database dictionary record.

8. Create the parameter for the field passed to the external application by the event.

9. Click **Save**.

Access the script panel

Applies to User Roles:

System Administrator

The DDE script panel, dde.script.g, assists in creating Service Manager DDE scripts for DDE calls inside Service Manager against an outside application such as Excel.

To access the DDE script panel:

- Click **Tailoring** > **Tailoring Tools** > **DDE Script**.

  The DDE script panel opens.

Access system events records

Applies to User Roles:

System Administrator

To access system events records:

1. Type `db` in the command line, and click the Execute Command button. The Database Manager dialog box opens.

2. Type `SystemEvents` in the Form field.

3. Click **Search**. A blank system events record opens.

4. Type the name of the record you want to view, or click **Search** to display a record list of all events in the system.

Integration Manager

Integration Manager refers to a plug-in based platform called Service Manager Integration Suite (SMIS), which can provide centralized management and configuration of all instances of integrations that are configurable in SMIS.

Accessing Integration Manager

To access the Service Manager Integration Manager, use the Windows or Web client and open **Tailoring** > **Integration Manager** from the System Navigator.

Integration Manager (SMIS) provides the following buttons or context menu options, which enable integration delivery engineers and support engineers to manage integration instances:

- **Add**: Add a new integration instance.
- **Edit**: Edit an existing integration instance.
- **Delete**: Delete an existing integration instance.
- **Enable**: Enable an integration instance.
- **Disable**: Disable an integration instance.
- **Refresh**: Refresh the status of an integration instance.
- **Task**: Monitor failover tasks of an integration instance during a specified period of time.
- **Log**: View task execution history.

Integration types

SMIS supports two types of integrations:

- Schedule-based: A schedule-based integration runs as a schedule in the background. When a schedule-based integration instance is enabled, a corresponding scheduler is started in Service

Manager.

- UI-based: A UI-based integration can be invoked only in the UI.

Out-of-box integration templates

Out-of-box, SMIS comes with a set of predefined templates that you can use to set up integrations to the following third-party or HP products:

Product	Template name
Third-party survey tools	SMSurvey
HP Release Control (RC)	SMtoRC
HP Operations Orchestration (OO)	SMOO
HP Business Service Management (BSM)	• SMBSM_DOWNTIME (for SM-BSM downtime synchronization) • SMOMi (for integration to Operations Manager i) • SMBIR (for integration to Business Impact Report)
Another product that supports Case Exchange	CaseExchangeDefaultTemplate

Note: The out-of-box templates are not provided as sample interfaces. You need to access the Integration Manager, set up the integrations through the Integration Template Selection wizard, and configure your system to interface with the HP products listed above.

Developing custom integrations using SMIS

SMIS is also a development platform that enables you to develop new integration templates of your own. You can then register these new integration templates in SMIS so that they are configurable in SMIS. For more information, see the Service Manager Integration Suite (SMIS) Developer Guide.

Add or delete an integration instance

Applies to User Roles:

System Administrator

Before you can use an integration that is configurable in Integration Manager, you must add (and then enable) an instance of this integration.

To add an integration instance:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The Integration Template Selection wizard opens.
3. Select a template from the Integration Template list.
4. If you want to use the field mappings provided with the template, select **Import Mapping**.

   Note: A template becomes unavailable when the number of integration instances based on this template reaches a maximum value predefined in the template.

5. Click **Next**. The Integration Instance Information page opens. Verify or complete the fields as necessary. For the description of each field on this page, see the related topics.

   Note: Some fields are automatically populated with the information from the integration template. However, you can modify their values as necessary.

6. Click **Next**. The Integration Instance Parameters page opens. This page contains all predefined parameters for the integration: General Parameters and Secure Parameters. You may set confidential parameters on the **Secure Parameters** tab, and the parameter values will appear as asterisks (*) for data security.

   Note: You can modify the predefined parameter values as necessary. However, it is not recommended to add new parameters, modify parameter names or categories.

7. Click **Next**. The Integration Instance Fields page opens. This page contains all predefined fields available for the integration:
   - **SM Fields:** Contains a list of fields at the Service Manager server side that can be mapped to endpoint fields.
   - **Endpoint Fields:** Contains a list of fields at the endpoint side that can be mapped to Service Manager server fields.
8. Click **Next**. The Integration Instance Mapping page opens. This page contains all field mappings and

value mappings between Service Manager server fields and endpoint fields. Review the mappings and make modifications to suit your needs if necessary.

> **Note:** The field mappings are available if you selected **Import Mapping** in step 4. Otherwise, the **Field Mapping** tab is empty. You may need to add field mappings manually. For detailed instructions about how to configure mappings, see the related topics.

9. Click **Finish**. The new integration instance is added.

To delete an integration instance:

> **Note:** Only integration instances in Disabled status can be deleted.

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select the integration instance you want to delete.
3. Click **Delete**. This will delete the integration instance record, the corresponding Field Mapping records, and the scheduler record (for schedule-based integrations only).

Integration Instance Information fields

When you add or edit an integration instance, you must verify or complete the following fields on the Integration Instance Information page. The sample values below are given for an instance of the Service Manager to Operations Orchestration integration.

Field	Sample Value	Description
Name (required)	SM00	Name of the integration instance. This field is automatically populated with the information from the integration template and can be modified to suit your needs.
Version (required)	1.0	Version of the integration. This field is automatically populated.
Interval Time (s) (required)	300	Enter an interval (in seconds) at which the integration instance is scheduled to run. **Note:** This field is required only when **Category** is **Schedule-based**.
Max Retry Times (required)	3	Enter a maximum allowed number of retries when a scheduled run of the instance fails. **Note:** This field is required only when **Category** is **Schedule-**

Field	Sample Value	Description
		based
SM Server	localhost	Enter a display name that identifies the Service Manager server machine you are using.
Endpoint Server	OO2-SRV	Enter a display name that identifies the endpoint server machine. For example, the display name of the Operations Orchestration server machine for the SM to OO integration.
Log Level	INFO	Level of diagnostic information that the Service Manager server logs to the log file directory. The possible log levels are as follows: • DEBUG: Designates fine-grained informational events that are most useful to debug the integration instance. • INFO (default): Designates informational messages that highlight the progress of the integration instance at coarse-grained level. • WARNING: Designates potentially harmful situations. • ERROR: Designates error events that might still allow the integration instance to continue running. • OFF: Turns off logging of the integration instance. The log hierarchy is DEBUG < INFO < WARNING < ERROR. Selecting a log of a higher level can render logs of lower levels invalid.
Log File Directory	C:\ Service Manager\server\logs	Enter an absolute path that exists on the Service Manager server, where log files will be stored. **Note:** If you enter a directory that does not exist, the log files will get lost.
Category	Schedule-based	Indicates whether the integration instance is Schedule-based or UI-based.
Shared Scheduler		The scheduler that the integration instance uses to schedule background processes. Multiple integration instances can use a shared scheduler. When you create an integration template, you can define a default shared scheduler for the instances that are based on the template. All instances that are based on this template can use the same shared scheduler. However, if you create an instance that uses a different scheduler, SMIS creates a new scheduler accordingly.
Run at	selected	Indicates whether the integration instance runs at system

Field	Sample Value	Description
system startup		startup. If selected, the current integration instance automatically runs when the Service Manager server is started.
Description	OO flows linked to SM Knowledge Management.	Description of the integration instance. You can modify the pre-populated text to suit your needs.

Edit an integration instance

Applies to User Roles:

System Administrator

Note: You can only edit integration instances in the Disabled status. Enabled integration instances (in Running or Sleeping status) can be viewed only.

To edit an integration instance:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance with a Status of Disabled, and click **Edit**.
   - In the Windows client, click an integration instance to select it.
   - In the Web client, hold down the Shift key as you click an integration instance to select it.

   The Integration Instance Information wizard opens.
3. Make changes to the field values as necessary, and then click **Next**. The Integration Instance Parameters wizard opens.
4. Update the parameter values with your real data if necessary. However, it is not recommended to add a new parameter, or modify parameter names or category.
5. Click **Next**. The Integration Instance Fields page opens, displaying all the fields predefined in the integration template:
   - **SM Fields:** A list of fields in the Service Manager server side that can be mapped to endpoint fields.

- **Endpoint Fields:** A list of fields in the endpoint side that can be mapped to Service Manager server fields.

6. If necessary, on the **SM Fields** and **Endpoint Fields** tabs, add new fields and specify a field type for each of them: string, date, number, or boolean.
7. Click **Next**. The Integration Instance Mapping page opens. Make changes to the field mappings and value mappings to suit your needs.
8. Click **Finish**. Changes made to the integration instance are saved.

Integration Instance Mapping

The mapping functionality of an integration instance converts values between Service Manager and the other product automatically. It is based on the following settings:

- Value mapping - Each value mapping is based on the value mapping group table.
- Field mapping - Map the value of a source field to the value of a target field and define the direction of the mapping.
- Default value - Default value is used in the following situations:
  - No value mapping group is defined for this field and the source field value is empty.
  - A value mapping group is defined for this field but the value cannot be mapped within the value mapping group.
- Callback - SMIS provides four callbacks for complicated field mappings, which provide the flexibility to implement corresponding business logic.
- Condition - SMIS supports conditional value mappings and enables you to configure conditions.
- Pre Script - The pre script can initialize variables so that succeeding processes can use these variables.
- Post Script - If all the previous processes cannot fulfill your need, you can use the post script to perform additional process and store results into the `mapObj` object.

SMIS processes the above settings in the following sequence:

Field mapping > Pre Script > Value mapping > Default Value > Callback > Post Script

If you selected **Import Mapping** when adding an integration instance, the mapping template with out-of-box lists of predefined field mappings and value mappings become available.

The out-of-box field mappings and value mappings can be regarded as the minimum default settings for an integration instance to run. However, you can configure these default settings as necessary to suit your needs.

Add or delete field mappings

Applies to User Roles:

System Administrator

To add a new row of field mapping, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance with a status of Disabled. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. Select the **Field Mapping** tab.
5. In the **SM Field** column, click the first blank cell, and select a field from the list.
6. In the **Direction** column, select a direction from the list.
7. In the **Endpoint Field** column, click the first blank cell, and select a field from the list.
8. In the **SM Default** or **EP Default** column, enter a default value or use a place holder expression.

   For more information about place holder, see "Use placeholders" on page 86.
9. In the **SM Callback** or **EP Callback** column, enter a callback function.
10. In the **Value Mapping Group** column, specify a value mapping group if necessary.
11. Click **Finish**.

To delete a row of field mapping, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance with a status of Disabled. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. Select the **Field Mapping** tab.
5. Clear all the fields in the row you want to delete.
6. Click **Finish**.

Edit field mappings

Applies to User Roles:

System Administrator

To edit a field mapping of an integration instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance with a status of Disabled. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. Select the **Field Mapping** tab.
5. In the **SM Field** column or **Endpoint Field** column, click an entry you wish to edit or configure, and select a field from the list.

   Note: If you want to add a new field that is not available in the list, you must first go to the Integration Instance Fields page, add this field, and specify a field type for it. There are four field types available: string, number, date, and boolean.

6. If necessary, click in the **Direction** field, and select a new direction from the list. A bidirectional direction means two mappings actually.
7. After you have finished modifying the field mappings, click **Finish**.

Configure a callback

Applies to User Roles:

System Administrator

A callback is a piece of executable code that is passed as a parameter to other code. The Service Manager Integration Suite (SMIS) provides the following four callback functions:

Callback Function	Description
lookup	Looks up a record from a Service Manager table matching the query condition. If a matching record is found, the **lookup** callback returns the value of the specified field; if not, it either returns an empty value or ignores the current mapping. **Note:** Multiple conditions should be separated with "||".
combine	Concatenates an array of values with a specified delimiter.
setValue	Sets values when the current action is among any combinations of **Insert**, **Update**, and **Close**. Otherwise, the **setValue** callback either returns an empty value or ignores the current mapping.
when	Return the value if any condition is met. In both the **condition** and **value** fields, use "${sm.field}" to get the value of SM field or use "${ep.field}" to get the value of the end point field.

Note: For more information about how to use placeholders (for example, ${sm.field} and ${ep.field}), see "Use placeholders" on page 86.

You configure callbacks for an integration instance from the Integration Instance Mapping page. You can edit or clear callbacks.

To edit a callback, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. On the **Field Mapping** tab, select a cell in the **SM Callback** or **EP Callback** column.
5. Click **Edit Callback**. The Callback Editor window opens.

6. Select a value from the **Callback Function** list. The parameters that display in the window vary with the callback function you selected: **lookup**, **combine**, **setValue**, or **when**.
7. Provide values for all the parameters. Click **OK** to save the callback.
8. Click **Finish**.

> **Note:** The changes you made to the integration instance are not saved until you click **Finish**.

To delete a callback, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. On the **Field Mapping** tab, select a cell in the **SM Callback** or **EP Callback** column.
5. Click **Clear Callback**.
6. Click **Yes** to confirm the deletion.
7. Click **Finish**.

Configure value mappings

Applies to User Roles:

System Administrator

You configure value mappings for an integration instance from the Integration Instance Mapping page.

> **Note:** JavaScript is not supported in the **SM Values** and **End Point Values** columns of the **Value Mapping** section. In case JavaScript calculations are required, you have to add the JavaScript code into the **Pre Script** or **Post Script** section.

To edit a value mapping, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.

3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. Select the **Value Mapping** tab.
5. Click the entry you want to edit, and enter a new value.
6. Click **Finish**.

To add a value mapping, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. On the **Value Mapping** tab, click the fields in the first blank row, and enter values for the fields.
5. Click **Finish**.

To delete a value mapping, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. On the **Value Mapping** tab, clear all the fields in the row you want to delete.
5. Click **Finish**.

For more information about how to configure conditions for value mappings, see "Configure a condition" below.

Configure a condition

Applies to User Roles:

System Administrator

SMIS enables you to configure conditions for value mappings. You can set the **Condition** field of a value mapping entry to one of the following strings:

- `true`: The value mapping defined in this entry is always effective.
- `false`: The value mapping defined in this entry is always ineffective.
- A string that uses place holder: The value mapping defined in this entry is effective only when the condition is met.

  For more information about how to use place holder, see "Use placeholders" on page 86.

Note:

- If the value for a mapping condition is blank, the value is set as `true` by default.
- JavaScript is not supported in the **Condition** field of the value mapping. In case JavaScript calculations are required, you have to add the JavaScript code into the **Pre Script** or **Post Script** section.

When you configure value mappings and set conditions, make sure logic conflicts do not occur. If several conditions of a value mapping are met but a logic conflict occurs, only the last value mapping is effective. As in the following example, the value mapping result for the `Status` field in Service Manager is `Pending` rather than `Open`.

Value Mapping Group	SM Values	End Point Values	Description	Condition
Status	Open	Pending		${context.inbound} && ${context.newSMIncident}
Status	Pending	Pending		${context.inbound} && ${context.newSMIncident}

To add or edit a condition, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. On the **Value Mapping** tab, select a cell in the **Condition** column.
5. Provide or edit the value for the condition.
6. Click **Finish** to save your changes.

To delete a condition, follow these steps:

1. Click **Tailoring** > **Integration Manage**r. Integration Instance Manager opens.
2. Select an integration instance. The Integration Instance Information wizard opens.
3. Click **Next** to get to the Integration Instance Mapping page in the wizard.
4. On the **Value Mapping** tab, select a cell in the **Condition** column.
5. Remove the condition value.
6. Click **Finish** to save your changes.

Pre script

Service Manager Integration Suite (SMIS) executes the pre script after field mapping and before value mapping. You can use the pre script to initialize variables so that SMIS can use these variables in value mapping, or execute additional calculations to influence the value mapping. You can follow normal Javascript syntax to compose the pre script. For the objects that the pre script can use, see "Placeholder objects" on the next page.

For example, the following pre script first verifies if the `properties.Description` field in the endpoint is not empty. If the field is not empty, the script calls a function and assigns the result of the function back to the `properties.Description` field.

```
if(ep['properties.Description']) ep['properties.Description'] = lib.CaseExchange_
SAWUtil.processHtmlText(param, context, 'description', ep
['properties.Description']);
```

It is not supported to update the affected record by using JavaScript statements in the **Pre Script** section. Only the update of the record itself via the running SMIS instance is supported.

Post script

If all previous processes cannot fulfill your need, you can write the post script to perform additional process and store results into the `mapObj` object. You can follow normal Javascript syntax to compose the post script. For the object that the post script can use, see "Placeholder objects" on the next page.

It is not supported to update the affected record by using JavaScript statements in the **Post Script** section. Only the update of the record itself via the running SMIS instance is supported.

Use placeholders

You can use placeholders in the following fields when you configure an integration instance:

- In field mapping: **Callback**, **SM Default**, and **EP Default**
- In value mapping: **Condition**

You can use the following placeholder syntax:

- `${(sm|ep|param|context|vars).fieldName}` if `fieldName` does not contain a "."
- `${(sm|ep|param|context|vars)["fieldName"]}` if `fieldName` contains a "."

You can use the `sm`, `ep`, `param`, `context`, and `vars` objects in a placeholder, see "Placeholder objects" below for details.

Placeholder allows you to use any Javascript syntax, or to call a function from the ScriptLibrary, for example, `lib.scriptlib.function`.

The following examples are some common use of placeholder:

- `${(sm.AssignmentGroup)}` represents the value of the **AssignmentGroup** field in Service Manager.
- `${(ep["AssignedGroup.Name"])}` represents the **AssignedGroup.Name** field in the end point.
- If you use `${context.inbound==true} && (!${context.newSMIncident})` in a condition, the condition is "The value of the **context.inbound** field is `true` and the value of the **context.newSMIncident** field is `false`."
- `${vars.$L_file.assignment}` refers to the field assignment of variable `vars.$L_file`.
- Use `${lib.<scriptlib>.<func>()}` to call a Java script.

Placeholder objects

You can use the following objects in a placeholder:

- `sm`: Refers to the value of a field in HP Service Manager. You can use either `fieldName` or `alias` to refer to the value of a Service Manager field.
- `ep`: Refers to the value of a field in the end point. You can use either `fieldName` or `alias` to refer to the value of an end point field.

- `param`: Refers to the value of a parameter that is defined in SMIS configuration.
- `context`: Refers to the task information as in the following table. `context` can store shared variable that you can use in other places, for example, callback, condition in value mappings, and post script.

Task information	Description
internalId	The ID of the record in Service Manager.
externalId	The ID of the record in the end point.
object	The table name of the object in Service Manager.
action	The action of an inbound or outbound request.
direction	The direction of the action: inbound or outbound.

internalObject	Refers to a specific record in Service Manager. You can perform the following operations with `internalObject`:
	◦ Directly modify `internalObject` to update the record. This operation is usually used for inbound tasks. For example, the following code in Additional Script can directly specify the value of a field:
	`context.internalObject["resolution.code"]="Request Rejected"`
	It is not recommended that you directly modify the value of a field by manipulating `internalObject`, because this action causes an inconsistency between the activity log and the actual result. Therefore, `internalObject` is usually used to perform operations that does not change the record itself, for example, creating activity log, or building relationship with another record.
	◦ Retrieve certain record information through `internalObject` in the pre script or post script. For example, the following code retrieves the value of the **Resolution Code** field through `internalObject`:
	`if(context.action=="Cancel" && context.internalObject ['resolution.code']=="Withdrawn by User") context.cancelledBySM = true;`

- `vars`: Refers to a global variable.
- `mapObj`: Refers to the last map object, which contains the final result of field mapping, pre script, and value mapping. You can only use `mapObj` in the post script. If you modify `mapObj` in the post script, your modification will overwrite the result of field mapping and value mapping. That is, the value of the corresponding field in the record will be what you specified in the post script.

The following example scenario helps you understand the use of the `sm`, `ep`, and `mapObj` objects:

- Assume that you configure the field mapping between the following SM and endpoint fields:
  - SM field: `resolution.code`
  - Endpoint field: `properties.CompletionCode`
- Some of the value mapping configurations for these two fields are as follows:

SM field (`resolution.code`)	**Endpoint field (`properties.CompletionCode`)**
Automatically Closed	NoUserResponse
Not Reproducible	NotReproducible

- In an inbound task, the value of the `properties.CompletionCode` field is `NoUserResponse` in the endpoint.

In this scenario, after the field mapping (and before the execution of the pre script), the `sm` and `ep` objects are initialized as follows:

- ep["properties.CompletionCode"]="NoUserResponse"
- sm["resolution.code"]="NoUserResponse"

You can manipulate these objects in the pre script.

After the value mapping, the `mapObj` object is initialized as follows (if you do not change these objects in the pre script):

mapObj["resolution.code"]="Automatically Closed"

This is the result of the field mapping and value mapping. If you do not modify this result in the post script, the **Resolution Code** field of the record will be **Automatically Closed**.

However, if you modify the result by adding the following code in the post script:

mapObj["resolution.code"]="Not Reproducible"

The previous field mapping and value mapping result will be overwritten, and the **Resolution Code** field of the record will be **Not Reproducible**.

Enable or disable an integration instance

Applies to User Roles:

System Administrator

To enable an integration instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance with a Status of Disabled, and click **Enable**.
3. In the prompt window, click **Yes**. The integration instance is enabled.
   If the integration instance is successfully enabled, its status changes to Running. However, if the integration instance is schedule-based, its status switches between Running and Sleeping:
   - **Running** indicates that the integration instance is processing data at a scheduled time interval.
   - **Sleeping** indicates that the integration instance has finished the data processing at a scheduled time interval. When a subsequent scheduled time interval is triggered, the integration instance status changes from Sleeping to Running.

To disable an integration instance, follow these steps:

Note: A schedule-based integration instance can be disabled only when it is in the Sleeping status.

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance with a Status of Running (UI-based) or Sleeping (schedule-based), and then click **Disable**.
3. In the prompt window, click **Yes**. The integration instance is disabled.

   Note: Disabling a schedule-based integration instance terminates the corresponding scheduler of the integration instance. If the scheduler is not terminated immediately, wait for a while and click **Refresh** (Refresh Integration instance) to check the status. If the integration instance is still not disabled, repeat the Disable operation or go to **System Status** to manually terminate the corresponding process named after the integration instance and its ID.

Monitor integration instance status

Applies to User Roles:

System Administrator

To monitor integration instance status:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance.
3. Click **Refresh**. The status of the selected integration instance refreshes.

Monitor failover tasks

Applies to User Roles:

System Administrator

The Task Manager window lists all failed tasks of an integration instance. You can check to see whether a task failed or has expired, as well as its retry times. A task expires if the scheduler has performed the maximum number of retries for it. If a task has expired, HP Service Manager no longer processes it until you reset it or manually rerun it.

To monitor a failover task, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance.
3. Click **Task**. The Task Manager window opens.
4. To filter tasks by time range, select a date range in the **From** and **To** fields, and click **Filter**.
5. Double-click a record in the task list. The task details are shown.
6. (Optional) If the task is unexpired, click **Reset** to set **Retry Times** to **0** and **Expired** to **false**.

   or

   If the task is expired, click **Run Now** to rerun it.

Note: When a failed task is successfully done, it is removed from the task queue.

Monitor SMIS task log

When an integration instance is active, HP Service Manager logs all system messages of the integration in the Service Manager Integration Suite (SMIS) task log. A log entry in the SMIS task log always links to

a task in the SMIS task queue. The SMIS task log allows an administrator to view the task history of an integration instance, and restart unsuccessful tasks when needed. For more information about how to enable an integration instance, see "Enable or disable an integration instance" on page 88.

To monitor the SMIS task log, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select an integration instance.
3. Click **Log**. The **Task Log** page opens.
4. To filter log entries by time range, select a date range in the **From** and **To** fields, and click **Filter**.
5. Double-click a record in the log list. The **Task Log Detail** page opens.

If the task is unsuccessful, you can continue the following steps to restart the task:

6. click the **View** button on the **Task Log Detail** page. The **Task Detail** page opens.
7. Click **Run Now**.

Purge the SMIS task log records

By default, the Service Manager Integration Suite (SMIS) task log keeps all task records even if these tasks are successfully processed and removed. Service Manager provides an out-of-box scheduler record to purge the SMIS task log. To use this scheduler record, follow these steps:

1. Click **Tailoring** > **Database Manager**.
2. Type `schedule` in the **Form** field and then click **Search**.
3. Open **schedule** from the record list. A blank Schedule File record is displayed.
4. Type `background purge/archive SMISTaskLog` in the **Name** field and then click **Search**.
5. Specify the **Expiration** field to define the start time of the purge task.
6. Click **Save**.

Using LW-SSO with integrations

Lightweight Single Sign-On (LW-SSO) is optional but highly recommended for some integrations. For example, the Release Control integration. Enabling LW-SSO for integrations will bypass the login

prompts when connecting two HP products.

Incoming UI LW-SSO

If LW-SSO is enabled in both the Service Manager Web tier and another HP product, users who have logged on to Service Manager are allowed to sign on to the other HP product through the web tier without a login prompt; however, you must enable LW-SSO in the Service Manager server additionally if you want users who have logged on to another product to directly sign on to Service Manager through LW-SSO. This is because the Service Manager server needs to trust the Web tier.

Incoming Web Services LW-SSO

If LW-SSO is enabled in the Service Manager server, other HP products can use a dedicated user account to access Service Manager Web Services without re-authentication.

Integration user accounts

For each integration, there might be two types of integration user accounts:

- Dedicated user account: a dedicated user account that one product uses to call Web Services of the end-point product through LW-SSO.
- End-user account: a user account that an end-user uses to log in to one product and then sign on to another product through LW-SSO.

These two types of integration user accounts must be created on both product sides. In addition, an integration user account must have the same user name (but can have different passwords) on the two sides.

You can use LW-SSO with the following integrations:

- Release Control (RC)
- Operations Orchestration (OO)
- Business Service Management (BSM) Operations Manager i
- Business Service Management (BSM) Business Impact Report

For details, see the specific information about how to configure LW-SSO in each of these products.

Configure LW-SSO in the Service Manager server

Applies to User Roles:

System Administrator

Service Manager servers, version 9.30 and later, support Lightweight Single Sign-On (LW-SSO). A Service Manager integration can pass an authentication token to Service Manager and does not require re-authentication. This simplifies the configuration of Single Sign-On for HP solutions by removing the need to use Symphony Adapter (which proxies LW-SSO-based authentication with the Service Manager Trusted Sign-On solution).

Enabling LW-SSO in the Service Manager server enables web service integrations from other HP products (for example, Release Control) to bypass Service Manager authentication if the product user is already authenticated and a proper token is used; enabling LW-SSO in both the Service Manager server and web tier enables users to bypass the login prompts when launching the Service Manager web client from other HP applications.

Note: Existing integrations that use the Symphony Adapter and Trusted Sign-On rather than this new LW-SSO mechanism can continue to work.

To configure LW-SSO in the Service Manager server:

1. Go to the <Service Manager server installation path>/RUN folder, and open `lwssofmconf.xml` in a text editor.
2. Make sure that the `enableLWSSOFramework` attribute is set to `true` (default).
3. Change the domain value `example.com` to the domain name of your Service Manager server host.

   Note: To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application to the web tier can log in but may be forcibly logged out after a while.
4. Set the `initString` value. This value MUST be the same with the LW-SSO setting of the other HP product you want to integrate with Service Manager.

Note:

Example

```
<?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" />
    <web-service>
       <inbound>
         <restURLs>
               <url>.*7/ws.*</url>
               <url>.*sc62server/ws.*</url>
               <url>.*/ui.*</url>
         </restURLs>
         <service service-type="rest" >
           <in-lwsso>
               <lwssoValidation>
                 <domain>example.com</domain>
                <crypto cipherType="symmetricBlockCipher" engineName="AES"
                 paddingModeName="CBC" keySize="256" encodingMode="Base64Url"
                 initString="This is a shared secret passphrase"</crypto>
               </lwssoValidation>
           </in-lwsso>
         </service>
        </inbound>
        <outbound/>
   </web-service>
</lwsso-config>
```

Configure LW-SSO in the Service Manager Web tier

Applies to User Roles:

System Administrator

If Lightweight Single Sign-On (LW-SSO) is enabled in the Service Manager Web tier, integrations from other HP products will bypass Service Manager authentication when launching the Service Manager Web client, provided that the HP product user is already authenticated and a proper token is used.

Note:

- To enable users to launch the Web client from another HP product using LW-SSO, you must also enable LW-SSO in the Service Manager server.

- Once you have enabled LW-SSO in the web tier, web client users should use the web tier server's fully-qualified domain name (FQDN) in the login URL:
  `http://<myWebtierHostName>.<myDomain>:<port>/webtier-x.xx/index.do`

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

To configure LW-SSO in the Service Manager Web tier:

1. Open the `<Tomcat>\webapps\< Service Manager Web tier>\WEB-INF\web.xml` file in a text editor.
2. Modify the `web.xml` file as follows:
   a. Set the `<serverHost>` parameter to the fully-qualified domain name of the Service Manager server.

      Note: This is required to enable LW-SSO from the web tier to the server.

   b. Set the `<serverPort>` parameter to the communications port of the Service Manager server.
   c. Set the `secureLogin` and `sslPort` parameters. See Web parameter: secureLogin and Web parameter: sslPort.

      - If you do not want to configure SSL between Tomcat and the browser, set `secureLogin` to `false`.
      - We recommend that you enable secure login in a production environment. Once `secureLogin` is enabled, you must configure SSL for Tomcat. For details, see the Apache Tomcat documentation.

   d. Change the value of context parameter **isCustomAuthenticationUsed** to false.
   e. Remove the comment tags (<!-- and -->) enclosing the following elements to enable LW-SSO authentication.

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

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

f. Save the `web.xml` file.

3. Open the `<Tomcat>\webapps\<Service Manager Web tier>\WEB-INF\classes\lwssofmconf.xml` file in a text editor.

4. Modify the `lwssofmconf.xml` file as follows:

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

   b. Set the `<domain>` parameter to the domain name of the server where you deploy your Service Manager Web tier. For example, if your Web tier's fully qualified domain name is `mywebtier.domain.hp.com`, then the domain portion is `domain.hp.com`.

   > **Note:** To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application (for example, HP Enterprise Collaboration) to the web tier can log in but may be forcibly logged out after a while.

   c. Set the `<initString>` value to the password used to connect HP applications through LW-SSO (minimum length: 12 characters). For example, **smintegrationlwsso**. Make sure that other HP applications (for example, Release Control) connecting to Service Manager through LW-SSO share the same password in their LW-SSO configurations.

   d. In the `<multiDomain>` element, set the trusted hosts connecting through LW-SSO. If the Service Manager web tier server and other application servers connecting through LW-SSO are in the same domain, you can ignore the `<multiDomain>` element ; If the servers are in multiple domains, for each server, you must set the correct `DNSDomain` (domain name), `NetBiosName` (server name), `IP` (IP address), and `FQDN` (fully-qualified domain name) values. The following is an example.

<DNSDomain>**example.com**</DNSDomain>

<NetBiosName>**myserver**</NetBiosName>

<IP>1.23.456.789</IP>

<FQDN>**myserver.example.com**</FQDN>

Note: As of version 9.30, Service Manager uses <multiDomain> instead of <protectedDomains>, which is used in earlier versions. The multi-domain functionality is relevant only for UI LW-SSO (not for web services LW-SSO). This functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL in a browser window, except when both applications are in the same domain.

e. 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 either `true` or `false`. In a production environment, you are recommended to set both parameters to `true`.
- If you do not want to use SSL, set both `secureHTTPCookie` and `secureLogin` to `false`.

Here is an example of `lwssofmconf.xml`:

```
<?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="This is a shared secret passphrase"/>
                </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>
```

f. Save the `lwssofmconf.xml` file.

5. Open the `<Tomcat>\webapps\<Service Manager Web tier>\WEB-INF\classes\application-context.xml` in a text editor.

6. Modify the `application-context.xml` as follows:

   a. Add `lwSsoFilter` to filterChainProxy:

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

   Note: If you need to enable web tier LW-SSO for integrations and also enable trusted sign-on for your web client users, add lwSsoFilter followed by preAuthenticationFilter, as shown in the following:
   `/**=httpSessionContextIntegrationFilter,`
   `lwSsoFilter,preAuthenticationFilter,``anonymousProcessingFilter`.

   For information about how to enable trusted sign-on in Service Manager, see Example: Enabling trusted sign-on.

   b. Uncomment bean lwSsoFilter:

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

   c. Save the `application-context.xml` file.

7. Repack the updated Service Manager web tier files and replace the old `web tier .war` file deployed in the `<Tomcat>\webapps` folder.

8. Restart Tomcat so that the configuration takes effect.

Configure LW-SSO in Business Service Management (BSM)

If LW-SSO is enabled in both Service Manager and HP Business Service Management (BSM), users who have logged on to Service Manager are allowed to sign on to BSM through the web tier without providing a user name and password.

To configure LW-SSO in BSM:

1. Log on to BSM as a system administrator.
2. Click **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**.
3. Check to see if the following two fields are correctly configured:
   - Token Creation Key (initString): Must be the same as the **initString** value specified in the Service Manager LW-SSO configuration (minimum length: 12 characters). For example, **smintegrationlwsso**.
   - Trusted Hosts/Domains: Must contain the domain name of the Service Manager Web tier server. For example, if your Service Manager Web tier's fully qualified domain name is mywebtier.domain.hp.com, then the domain name is **domain.hp.com**.

   If these two fields are correctly configured, LW-SSO is already enabled in your BSM environment, and you can ignore the steps below. If not, proceed to the steps below.
4. Click **Configure**. The Authentication Management Wizard opens.
5. Click **Next**. The Single Sign-On Configuration page opens.
6. Do the following:
   - In the **Token Creation Key (initString)** field, enter a string of characters. For example, **smintegrationlwsso**.

     Note: This value must be the same as the initString value in your Service Manager LW-SSO configuration.
   - In the **Trusted Hosts/Domains** column, add the domain name of the Service Manager Web tier

server.

- In the **Type** column, select **DNS** for the Service Manager Web tier server.

7. Click **Next** twice, and then click **Finish**.

   LW-SSO is now enabled in your BSM environment.

   Note: For other 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 LW-SSO in Operations Orchestration (OO)

Applies to User Roles:

System Administrator

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

Note:
- In the following procedure, <OO_HOME> represents the Operations Orchestration home directory.
- LW-SSO requires that the accounts used to log on to Operations Orchestration and Service Manager have the same account name (but can have different passwords).

To configure LW-SSO in Operations Orchestration 9.x and earlier versions:

1. Stop the RSCentral service.
2. In `<OO_HOME>\Central\WEB-INF\applicationContext.xml`, enable the import between `LWSSO_SECTION_BEGIN` and `LWSSO_SECTION_END` as shown below.

   ```
   <!--  LWSSO_SECTION_BEGIN-->
            <import resource="CentralLWSSOBeans.xml"/>
   <!--  LWSSO_SECTION_END -->
   ```

3. In `<OO_HOME>\Central\WEB-INF\web.xml`, enable all the filters and mappings between `LWSSO_SECTION_BEGIN` and `LWSSO_SECTION_END` as shown below.

```
<!-- LWSSO_SECTION_BEGIN  -->

 <filter>
    <filter-name>LWSSO</filter-name>
    <filter-
class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProxy
    </filter-class>
    <init-param>
       <param-name>targetBean</param-name>
       <param-value>dharma.LWSSOFilter</param-value>
    </init-param>
    ......
</filter>
<!-- LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
        <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
  <filter-mapping>
     <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
     </filter-mapping>
     <filter-mapping>
       <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-pattern>/*</url-
pattern>
  </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4. In `<OO_HOME>\Central\conf\lwssofmconf.xml`, edit the two parameters:

   - **domain:** Domain name of the Service Manager Web tier server.
   - **initString:** Must be same as the **initString** value in the Service Manager LW-SSO configuration (minimum length: 12 characters). For example, **smintegrationlwsso**.

   For example:

```
<webui>
 <validation>
   <in-ui-lwsso>
     <lwssoValidation id="ID000001">
```

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

5. Restart the RSCentral service so that the configuration takes effect.

To configure LW-SSO in Operations Orchestration 10:

Refer to *HP Operations Orchestration Central User Guide > Setting Up Security – LWSSO* available from HP Software Support Online.

Configure LW-SSO in Release Control

Applies to User Roles:

System Administrator

> **Note:** You must have administrative access to Release Control (RC) to use this procedure. This procedure is optional but highly recommended for using the RC integration.

To configure LW-SSO in Release Control:

1. Create an RC user that has the same account name and password used to log on to Service Manager.
   a. Log on to RC as a system administrator, and click **Module** > **Administrator**.
   b. Click **Users**.
   c. Click the **New User** icon.

d. Provide information of the user account, for example, **falcon**.

e. Click **OK**.

2. Log on to RC as a system administrator, and click **Module** > **Adminstrator** > **Configuration** > **Server**.
3. In the **Server name** field, enter the FQDN of the Release Control Server host. For example, **myrchost.domain.hp.net**.
4. In the **Server address** field, enter the server address of Release Control. For example, **http://myrchost.domain.hp.net:8080/ccm**.
5. Provide values for other fields if necessary.
6. Click the **Save** button in the left pane to save the draft.
7. Click **Security** > **HP LightweightSSO(LWSSO)**.
8. Provide values for the following fields:
   - **Domain:** Domain name of the Release Control server host.
   - **Initialization string:** Should be the same with the **initString** value specified in the Service Manager LW-SSO configuration (minimum length: 12 characters). For example: **smintegrationlwsso**.
   - **Protected domains:** Enter the domain name of the Service Manager Web tier server. For example, if your Web tier's fully qualified domain name is mywebtier.domain.hp.com, then the domain portion is domain.hp.com.
9. Click the **Save** button in the left pane and then click **Activate draft**.
10. Restart the Release Control service so that your configurations take effect.

BDM Mapping Management

Applies to User Roles:

System Administrator

The BTO Data Model (BDM) is intended to be used as a standard data model for integrations between HP BTO products, for example, HP Service Manager and HP Business Service Management (BSM) . In Service Manager, a BDM mapping is a mapping between a Service Manager object (associated to a file in Service

Manager) and a BDM object (predefined in BDM). A BDM mapping consists of the following parts: field mapping, value mapping, atom mapping, and configuration.

Note: Service Manager supports data mappings of the `incident` entity, which are compliant with three versions of BDM: 1.0, 1.1, and 1.2, respectively.

System administrators can create new BDM mapping configurations or customize existing BDM mapping configurations in Service Manager.

To configure a BDM mapping in Service Manager:

1. Go to **System Administration** > **Ongoing Maintenance** > **BDM Mapping Management**. The BDM mapping configuration search page opens.
2. Do one of the following:
   - Search for an existing BDM mapping configuration.

     For example, enter **incident** in the BDM Name field, select **1.2** in the Version field, and then click **Search**. The mapping configuration of BDM object **incident** is displayed.
   - Add a new BDM mapping configuration.
     i. In the BDM Name field, enter the name of a BDM object.
     ii. In the Version field, select a version of BDM from the list.
     iii. In the File field, click the Fill icon and then select the name of a file from the resulting list. This is the Service Manager file that you want to map to BDM.
     iv. Click **Add**. The new BDM mapping record is added.
3. Configure the mapping information on the following tabs:
   - Field Mapping

     Note: If you add a new field to the file associated to the Service Manager object, you must click the Fill icon for the File field to refresh the field list in the SM Object Field column.
   - Value Mapping

- Atom Mapping
- Configuration

For detailed description of the information on each tab, see the related topics.

4. (Optional) Click **Publish** to publish the BDM mapping.

   Note: Once published, a BDM mapping record becomes read-only.

Field Mapping

The **Field Mapping** tab of a BDM mapping defines the field mappings between a Service Manager object and a BDM object. This section describes how to configure the columns on this tab, and provides detailed information about the inner objects, functions, and variables that can be used to configure callbacks in the SM Callback and BDM Callback columns.

Field Mapping columns

The following table describes the columns on the **Field Mapping** tab.

Column Name	Description
SM Object Field	The name of a field in the Service Manager file, and can be selected from the list. **Note:** Do not select the first item such as **[probsummary]** in the list, which references the name of the file that you want to map to BDM. The BDM mapping utility does not support complex structures at this time (for example, an array of arrays or an array within an array of structures).
Direction	Indicates the mapping direction of a field mapping, and has only three values to select from. • **->:** from SM Object Field to BDM Object Field/Attribute. • **<-:** from BDM Object Field/Attribute to SM Object Field. • **<->:** in both directions.
BDM Object Field/Attribute	The name of a field in the BDM object, and should be in a format like XPath of XML. For example, the following XML segment: `<is_registered_for target_role='xxx'>`

Column Name	Description
	<target_global_id>xxx</target_global_id> <target_type>xxx</target_type> <configuration_item> <id>xxx</id> <type>xxx</type> <description>xxx</description> </configuration_item> </is_registered_for> should be formatted as: is_registered_for/@target_role (@ means it is an attribute) is_registered_for/ target_global_id is_registered_for/ target_type is_registered_for/ configuration_item/ id is_registered_for/ configuration_item/ type is_registered_for/ configuration_item/ description • You can use an array to represent repetitive elements. For example: <users> <user> <name>xxx</name> <email>xxx</email> </user> <user> <name>xxx</name> <email>xxx</email> </user> ... </users> Can be described as: users/user[0]/name users/user[0]/email users/user[1]/name users/user[1]/email • The namespace of a BDM field should be formatted as: ns:property1/ns:subproperty2 **ns** is the alias of a namespace, and should be included in the **BDM Callback** of the **@xmlns** mapping entry: $xmlns({..., "ns":"http://www.xxx.com/xxx/xxx", ...}) If the alias is omitted, then a default namespace configured in @xmlns will be used:

Column Name	Description
	`'\$':"http://www.xxx.com/xxx/xxx"`
SM Default Value	Defines the default value of the SM Object Field if there is no value in the corresponding BDM Object Field/Attribute when mapping the BDM object to the Service Manager object.
SM Callback	Enter custom JavaScript code, which will be invoked when mapping BDM Object Field/Attribute to SM Object Field. For information about how to configure callbacks, see the **Callbacks** section below. **Note:** If no callback is configured, the BDM Object Field/Attribute will be directly mapped to the SM Object Field.
BDM Default Value	Defines the default value of the BDM Object Field/Attribute if there is no value in the corresponding SM Object Field when mapping the Service Manager object to the BDM object.
BDM Callback	Enter custom JavaScript code for mapping between the BDM Object Field/Attribute and the SM Object Field. When mapping the Service Manager object to the BDM object, the custom JavaScript code will be invoked. For more information about how to configure callbacks, see the **Callbacks** section below.
BDM Type	Select one from the list: String (default), Number, and DateTime. If no BDM Type is selected, the default type (String) will be used.
Value Mapping Group	The name of a value mapping group to which the BDM Object Field/Attribute and SM Object Field belong. A value mapping group contains a collection of enumerated BDM/SM value pairs. The Service Manager value and BDM value will be mapped according to the configuration on the **Value Mapping** tab.
Description	Enter a text description for this BDM mapping.

Callbacks

In the **SM Callback** and **BDM Callback** columns, you can enter custom JavaScript code for mapping between the Service Manager object and BDM object. Some inner objects, variables, and functions can be used in the custom JavaScript code. The key word **$** is reserved to identify these inner objects, variables, and functions.

Reserved key word ($)

The following rules apply when you use the reserved key word: **$**.

- If you want to use your own variable prefixed with '$', you must escape it with character '\'. For example:

  ```
  var \$test = 'abc';
  ```

- You can also use inner variables and objects in a string. For example:

  ```
  var strTemp = "Incident Number: $sm.number";
  ```

  If you want to use a '$' in a string, you must escape it. For example:

  ```
  cost: 100 \$ ...
  ```

- In a regular expression, you do not need to escape '$' with '\':

  ```
  var regExpr = /^[Jj]ava[Ss]cript$/
  ```

  However, if you define with the RegExp object, you must escape '$', because '$' is in a string:

  ```
  var regExpr = new RegExp( "^[Jj]ava[Ss]cript\$" );
  ```

Inner objects, functions, and variables

The following tables list the inner objects, functions, and variables.

- Inner Objects

Object Name	Member Method Signature / Method Description

$sm
 	
The current Service Manager object.
	value(field)
	
	field: The name of a field of the Service Manager object. If you do not include the <field> parameter, the currently configured field is used. Subfields should be separated with a forward slash ('/').
	
	This function is used to extract the value of a field of the Service Manager object. If you do not include the <field> parameter, it will return the current field value. For example:
	
	`$sm.value( "id" )`
	
	`$sm.value( "resolution[0]" )`
	
	`$sm.value()`

	setValue(value, field) **value:** The value of the <field> to be set. **field:** The name of a field of the Service Manager object. If you do not include the <field> parameter, the currently configured field will be used. This function is used to set the value of a field of the Service Manager object. If you do not include the <field> parameter, it will return the current field value.

$bdm
 	
The current BDM object.
	value(field)
	
	field: The name of a field of the BDM object. If you do not include the <field> parameter, the currently configured field will be used. Subfields should be separated with a forward slash ("/").
	
	This function is used to extract the value of a field of the BDM object. If you do not include the <field> parameter, it will return the current field value. For example:
	
	`$bdm.value( "is_registered_for/configuration_item" )`
	
	`$bdm.value( "ns:users/ns:user[0]/name" )`
	
	`$bdm.value()`

Object Name	Member Method Signature / Method Description
	setValue(value, field) **value:** The value to be set for the <field>. **field:** The name of a field of the BDM object. If you do not include the <field> parameter, the currently configured field will be used. **Note:** The field value must be the value in the BDM Object Field/Attribute column. This function is used to set the value of a field of the BDM object.
$ctx The current mapping context object, which is used to hold some variables to be used in the whole mapping process.	set(key, value) **key:** The key to be set for the <value>. **value:** The value to be kept in the mapping context object for the key. This function is used to set a key-value pair in a mapping context object. For example: `$ctx.set("affected_ci", affected_ci)`
	get(key) **key:** The key in a key-value pair. This function is used to get the value of a key in a mapping context object. For example: `var affected_ci = $ctx.get("affected_ci")`

- Inner functions

Function Signature	Description
$xmlns()	Used to define an xml namespace. Example:

Function Signature	Description

	`$xmlns({"\$":"http://www.hp.com/2009/software/data_model",`
	`"bdm":" http://www.hp.com/2009/software/data_model"}).`
	In this example, **"\$":"http://www.hp.com/2009/software/data_model"** is a default namespace, where reserved key word **$** is escaped with a backslash ("\"); **"bdm":" http://www.hp.com/2009/software/data_model"** is another namespace, where **bdm** is the alias of the namespace. You can add more namespaces, but there is only one default namespace.

$afterString (str) **str:** A portion of the current mapping field value.	Used to return the portion of the current mapping field value that is after the string specified by the <str> parameter. Example: `$afterString("urn:x-hp:software:servicemanager:incident:id:")` If the current mapping field is 'global_id' of the BDM object, and its value is **urn:x-hp:software:servicemanager:incident:id:7B21A623-158B-45D4-9C7C-3D2821096A44**, the $afterString will return: **7B21A623-158B-45D4-9C7C-3D2821096A44**.
$prefix(str) **str:** The string value to be prefixed before the current mapping field value.	Used to prefix a string before the current mapping field value. Example: If the current mapping field is 'id' of the Service Manager object and its value is "5A8EABC6-CA1B-499B-A230-4D6DE07487D8", `$prefix("urn:x-hp:software:servicemanager:incident:id:")` will return **urn:x-hp:software:servicemanager:incident:id: 5A8EABC6-CA1B-499B-A230-4D6DE07487D8**.
$select (fileName, query) ◦ **filename:** The name of a valid Service Manager file. ◦ **query:** The	Used to do select the SM object from the SM DB. Example: `var requestedBy = $select("contacts",'operator.id="falcon"');`

Function Signature	Description
Service Manager query language.	
$combine (delimiter) **delimiter:** A symbol or character used to separate the combined values.	Used to combine the current field values of the Service Manager/BDM object into one string.
combine(arr, delimiter) ◦ **arr:** An array of values to be combined. ◦ **delimiter:** A symbol or character used to separate the combined values.	Used to combine the specified array of values into one string. Example: `combine( ['a','b','c'], ',')`
$isCreate()	Used to verify if the current operation has created an SM object in Service Manager (true) or not (false).
$isUpdate()	Used to verify if the current operation has updated an SM object in Service Manager (true) or not (false).

- Inner variables

Variable Name	Description
$result	This variable is used to hold the returned result that will be assigned to the current target field of the Service Manager/BDM object if the custom JavaScript code cannot

Variable Name	Description

	generate a value (for example, the 'if' statement cannot generate a value, and thus needs to use the $result variable to hold the result):
	`var affected_ci = $ctx.get("affected_ci");`
	`if( affected_ci ) {`
	`  $result = affected_ci['type'];`
	`}`

Value Mapping

The **Value Mapping** tab of a BDM mapping defines the value mappings between a Service Manager object and a BDM object.

The following describes the columns on this tab.

Column Name	Description
Value Mapping Group	The name of a value mapping group. A value mapping group contains a collection of enumerated BDM/SM value pairs.
BDM Values	The values of the BDM fields.
SM Values	The values of the Service Manager fields.
Description	Description of the value mapping.

For example, below is a value mapping named **impact**, and there are four mapping entries for this value mapping group:

Value Mapping Group	BDM Values	SM Values
impact	enterprise	1
impact	site-dept	2
impact	multiple-users	3
impact	users	4

The name **impact** can be filled in the **Value Mapping Group** column on the **Field Mapping** tab:

SM Object Field	Direction	BDM Object Field/Attribute	SM Default Value	SM Callback	BDM Default Value	BDM Callback	BDM Type	Value Mapping Group
initial.impact	<->	impact_scope						impact

This means when mapping the Service Manager object to the BDM object, if the value of field `initial.impact` of the Service Manager object is 2, the value `2` will be mapped to `site-dept` for the field `impact_scope` of the BDM object, and vice versa.

Atom Mapping

The **Atom Mapping** tab of a BDM mapping defines the required mappings between certain fields in a BDM object and Atom (an XML-based document format for web feeds). The Service Manager RESTful web service supports the standard Atom representation, which conforms to the Atom Publishing Protocol. According to the Atom Publishing Protocol, the following elements are required in an Atom 1.0 feed: **title**, **id**, and **updated**.

The following table describes the columns on the **Atom Mapping** tab.

Column Name	Description
BDM Object Field	The name of a valid field in the BDM object
Atom Object Field	The name of a valid Atom field.
Atom Object Field Type	The type of a valid Atom field.

Below is an example of an Atom mapping:

BDM Object Field	Atom Object Field	Atom Object Field Type
reference_number	title	String
last_modified_time	updated	DateTime
description	summary	String
global_id	id	String

In the resulting Atom xml representation below, the **id**, **updated**, **title** and **summary** elements will take the values of the BDM object fields **global_id**, **last_modified_time**, **reference_number** and **description**, respectively.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<entry xmlns="http://www.w3.org/2005/Atom" xmlns:ns2="http://a9.com/-
```

```
/spec/opensearch/1.1/" xmlns:ns3="http://www.w3.org/1999/xhtml">
<id>urn:x-hp:software:servicemanager:incident:id:7B21A623-158B-45D4-9C7C-
3D2821096A44</id>
<updated>2010-01-27T11:41:25.000+08:00</updated>
<title type="text">IM10008</title>
<summary type="text">Desktop DVD-drive makes strange noices</summary>
```

Customizing BDM mapping configuration

System Administrators can define key-value pairs that can be shared by SM callbacks and BDM callbacks in BDM mapping records. With this functionality, administrators only need to update these key values in one place instead of in individual callbacks.

To customize BDM mapping configuration:

1. Log in to the Windows client as a System Administrator.
2. Click **System Administration** > **Ongoing Maintenance** > **BDM Mapping Management**.
3. In the Version field, select a value. For example, **1.2**.
4. Click **Search**. The mapping record `incident` is displayed.
5. Select the **Configuration** tab. A two-column table is displayed. This table defines key-value pairs that can be used in BDM mapping callbacks.
   - **Name**: Defines the name of a key to be used in callbacks.
   - **Value**: Defines the value of the key.

   Out-of-box, there are three keys: Host, Port, and AppName.
6. Type key-value pairs in the table. For example, you can type values for the following out-of-box keys:
   - Host: **abc.domain.com**
   - Port: **8080**
   - AppName: **webtier-9.30**
7. To view an out-of-box example of using these keys:

a. Select the **Field Mapping** tab, and locate the SM Object Field named **affected.item**.

b. In this field section, locate the row in which the BDM Object Field/Attribute value is: **affects/configuration_item/smns:drilldown_url**

c. Click the BDM Callback in the same row, right-click it and then select **Magnify**.

The callback code displays in a pop-up text window.

d. Find the following strings, which contain the three out-of-box key names.

- `$ctx.getMappingConfiguration()['Host']`
- `$ctx.getMappingConfiguration()['Port']`
- `$ctx.getMappingConfiguration()['AppName'])`

8. To use a defined key in a callback:

a. Select the **Field Mapping** tab, click a callback in the SM Callback or BDM Callback column. Right-click the callback and select **Magnify**.

The callback code displays in a pop-up text window.

b. Edit the callback code using the following syntax:

`$ctx.getMappingConfiguration()['Host']`, where Host should be replaced with your key name.

c. Click **Save and Close**.

9. To test the values you have defined for the out-of-box keys:

a. Send a REST request by launching this URL in a web browser: `http://<SM_serverHost>:<Port>/SM/7/rest/1.2/incident_list/reference_number/IM10002`.

A login window is displayed.

b. Type a valid Service Manager username/password (for example, System.Admin/blank password), and click **OK**.

The REST request response is displayed.

c. Locate this string: `<smns:drilldown_url>http://<hostname>:<port>/<AppName>/index.do`, where `<hostname>`, `<port>`, and `<AppName>` should be replaced with the values of Host, Port, and AppName, respectively.

Integrations and extacess records

Integrations such as SRC, Mobility, RC should call existing processes from the processes they define instead of modifying an existing process.

In the situation where you need to define extaccess records that call display actions in the record's State there is a good chance that the process will need additional logic to properly function. The best practice for dealing with this situation is to create and call a new process rather than modifying an existing process with integration-specific logic.

For example, an integration wants to perform display action x, which calls Process (p), but needs to put integration specific logic into Process (p) in order to make it perform correctly. The best practice in this case is to:

- Create a new process record which performs the integration specific logic.
- Call the original Process (p) in the "Next Process" tab.
- Add a new action to the State record.
- Call that action from the extaccess record.

This will make the integration easier to maintain and debug.

When you add a new display action to the State record, the $L.action variable will most likely have to be updated. Usually the integration specific process record will need to update $L.action to match the display action being wrapped.

For example, an integration wants to call the "save" display action. A new process record called "integration.record.save" is created, which finishes by calling "record.save" in the next process tab. A new display action called "integration.save" is added to the State record and the extaccess record calls that in its Allowed Actions tab. The "integration.record.save" process record ensures that the $L.action variable is set to "save."

In some cases, other local variables may need to be set as well. Incident Management, for example, has a $L.mode variable that needs to be managed. Be sure to check both the existing State and Process record when developing a new process for references to variables that may need to be managed.

HP Change Configuration and Release Management (CCRM)

HP Service Manager is part of the HP Change Configuration and Release Management (CCRM) solution. CCRM enables the enterprise IT organization to do the following:

- Provide the structure and formal workflow necessary to implement changes
- Reduce the risk of making changes by providing an accurate picture of IT infrastructure, as well as the impact any change may have on IT services
- Enable early detection of unplanned changes
- Maintain an accurate record of IT infrastructure

To minimize incidents that result from unplanned or improperly planned changes to the organization, an IT organization must be able to respond in the following ways to change drivers:

- Proactively: to provide benefits to the organization, either through lower total cost of ownership (TCO), or by providing options that enable business to develop
- Reactively: to resolve errors that impact the level of services that are provided

CCRM offers a solution comprised of three integrated HP products:

- Service Manager automates and standardizes the change process in accordance with ITIL best practices—from request through release and review.
- Release Control plays a role at a specific point in the process as a decision-support tool; it includes risk analysis, impact assessment, collision detection, and forward schedule of changes.
- Universal CMDB consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

CCRM also offers an automation extension to automate change requests (via HP Operations Orchestration (OO)) and another extension to provide dashboard views of assigned request status as well as comparisons between current projects and staffing profiles (via HP PPM Center).

For more information about CCRM, see the CCRM documentation available with the Service Manager documentation from HP Software Support Online.

SAP Solution Manager

The integration of SAP Solution Manager Service Desk with HP Service Manager provides a cohesive Incident and Service Request Management solution for the entire enterprise, resulting in higher enterprise availability, improved service quality and reduced IT costs.

HP Incident Exchange builds a dynamic link between HP Service Manager Software and SAP Solution Manager Service Desk and improves the Incident and Service Request Management Process throughout the entire enterprise. HP Incident Exchange offers dynamic integration between HP Service Manager and SAP Solution Manager Service Desk for improved incident workflow.

The interface to exchange support messages between HP Service Manager and SAP Solution Manager Service Desk was designed and developed jointly by HP and SAP and is certified by SAP.

For details, see the *HP Service Manager Exchange with SAP Solution Manager Installation and Administration Guide* and the *HP Service Manager Exchange with SAP Solution Manager User Guide*.

HP Project and Portfolio Management Center (PPM)

The HP SM Service Catalog-PPM Center Project Proposal Integration Solution aims to submit project proposals from Service Manager to PPM Center, and feed back the proposal's status (rejection/approval) from PPM Center to Service Manager.

For details, see the *HP SM Service Catalog-PPM Center Project Proposal Integration Solution Configuration Guide*.

HP Application Lifecycle Management/Quality Center (ALM/QC)

This integration provides 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). The overall intent of this integration are:

- Leverages SM/SC's position as the service provider and application with the most intimate contact with the customer.
- Efficiently reconciles and resolves the demands placed within SM/SC.
- Tightly couples the demands placed within SM/SC with the ALM/QC requirement management and defect management capabilities within SM/SC.

This integration synchronizes SM/SC Change or Problem with ALM/QC Defect or Requirement for record creation and update. The following scenarios are included:

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

For details, see the *HP Defects and Requirements Exchange with HP Service Manager/ServiceCenter and HP Quality Center/Application Lifecycle Management Installation and Administration Guide*.

HP Release Control (RC)

HP Release Control (RC) ties the change planning and analysis process with automated change execution and validation to help reduce the risk of service downtime. It provides the means for more accurate planning and approval decisions during the review process, as well as real-time visibility and cross-team communication to prevent service disruptions that occur due to unplanned changes, schedule delays, collisions, or failures during change execution. Teams can coordinate hand-offs and sharing of information between the Change Advisory Board (CAB) and the implementation team. Refer to the HP Release Control (RC) documentation for more information.

The RC integration provides extended Change Management support. Change records are synchronized from HP Service Manager to RC and then back to Service Manager; Service Manager Change Management users can access the RC Calendar from within Service Manager. RC Calendar performs calculations, such as risk and collision analysis, and stores the information on the RC database server. The change planning and analysis process is expanded with automatic impact, collision, and risk detection; comprehensive change scheduling; and enhanced CAB collaboration. When RC is integrated with Service Manager, change records are converted into generic requests and RC sends the generic requests to HP Universal CMDB (UCMDB) for analysis to determine the relationships between configuration items (CIs). Email notifications are sent when changes are approved or rejected.

Note: Only one instance of this integration is allowed.

Prerequisites:

- A System Administrator must add, configure, and enable an instance of this integration in Integration Manager (SMIS).
- It is strongly recommended to use Lightweight Single Sign-On (LW-SSO) to bypass the log-in prompts.
- To view RC Calendar and Change Assessment, make sure the following requirements are met:
  - **Browser** - Microsoft Internet Explorer 6.0 or above
  - **Flash Player Browser Plugin** - 9.0 or above

Upgrade the Release Control integration

Applies to User Roles:

System Administrator

If you are upgrading from an earlier version of HP Service Manager (for example, 9.20), after you have upgraded the Service Manager applications, you need to upgrade the Release Control (RC) integration in Integration Manager (SMIS). This upgrade includes deleting the old RC integration instance, adding a new one and re-configuring the integration parameters (including those new parameters introduced after the Service Manager 9.20 release).

Note: If you are also upgrading your UCMDB and RC environments when upgrading the integration, you are recommended to do the upgrades in the following order (otherwise the integration may not work properly after the upgrades):

1. Upgrade UCMDB (for example, from version 9.01 to 9.03). For details, refer to the UCMDB documentation.
2. Upgrade RC (for example, from version 9.12 to 9.13). For details, refer to the Release Control documentation.
3. Upgrade Service Manager (for example, from version 9.20 to 9.41). For details, see the following steps.

To upgrade the RC integration in Service Manager, follow these steps:

1. Log on to Service Manager as a System Administrator.
2. Upgrade the Service Manager applications. For details, see the *HP Service Manager Upgrade Guide*.
3. Click **Tailoring** > **Integration Manager**.
4. Delete the old RC integration instance.
5. Add a new RC integration instance. For detailed steps, see "Add a Release Control integration" on page 129.

   Note: The following RC integration parameters were introduced or renamed after the Service Manager 9.20 release.

Parameter	Description
rc.username	(New) The user name of the RC user account that manages multitenancy in RC.

Parameter	Description
rc.password	(New) The password of the RC user account that manages multitenancy in RC.
rcStandalone	(New) Set to true to enable the RC integration to work without UCMDB; when set to false, both Service Manager and RC must integrate with UCMDB for the integration to work.
rc.adapter.name	(Renamed from the `specified.service.desk` parameter in version 9.20) This is the name you specified when configuring the RC adapter for the Service Manager server.
rcSimplified	Specify this value to true, a simplified and Section 508 compliant RC widget is embedded in SM.

6. Enable the RC integration instance.

Release Control integration setup

Applies to User Roles:

System Administrator

To set up an Release Control (RC) integration, follow these steps:

1. "Configure the RC adapter" on the next page

   This task creates an adapter in RC to enable RC to access the HP Service Manager server.

2. "Add a Release Control integration" on page 129

   This task adds an RC integration and enables it in Integration Manager. This will enable users to launch the RC Calendar and Change Assessment from within Service Manager.

   Note: The RC integration can work either without or with UCMDB. This is controlled by the rcStandalone parameter you specify when adding the RC integration.

3. "Enable LW-SSO for the Release Control integration" on page 131

   This task is highly recommended. Enabling LW-SSO for the integration will enable RC to call a Service Manager web service through LW-SSO, and will bypass the login prompts when users launch the RC Calendar from within Service Manager.

4. "Configure language and time zone for the RC integration" on page 131

   This task is required only when your Service Manager needs to provide login languages other than the 14 out-of-box languages (through open localization) and when you want to enable time zones other than the 51 out-of-box time zones.

5. "Show custom Service Manager fields in Release Control Analysis" on page 132

   This task is required only when you want to expose custom fields to the RC Analysis module. This includes adding custom fields to an extaccess record (ChangeRC) in Service Manager and configuring RC to show the custom fields you exposed.

6. "Verify the RC integration setup" on page 135

   Perform this task to check if you have successfully set up your RC integration.

Configure the RC adapter

Applies to User Roles:

System Administrator

Note: Before using the Release Control integration, you must configure an RC adapter for the HP Service Manager server.

To configure the RC adapter, follow these steps:

1. Run the following command on the RC server:

   <HP Release Control installation directory>\bin\SdiConfigurer.bat

2. Enter required information at each screen prompt, and press **Enter**.

   Note: If you press **ENTER** without typing a selection, the default entry is automatically selected.

Screen prompt	Description
Select service	Select **ServiceCenter/Service Manager service desks**.

Screen prompt	Description
desk type	
Enter adapter name	Enter a name for the adapter. For example, `sm`. **Note:** You will need this adapter name when setting up the RC integration in the SMIS interface in Service Manager. See "Add a Release Control integration" on page 129.
Select Service Manager/Center version	Select **9.41 and above**.
Enter Service Manager user name	Enter an existing Service Manager user account that the RC server uses to access the Service Manager server. For example, `smrcintegration`. **Note**: You are recommended to create a dedicated Service Manager user account for the RC integration. This user account must have the SOAP API execute capability in Service Manager.
Enter password	Enter the password of the Service Manager user account that the RC server uses to access the Service Manager server. For example: `!qaz2wsx`.
Enter Service Manager timezone	Enter the time zone specified in Service Manager for the Service Manager user account that the RC server uses to access the Service Manager server. For example: `US/Pacific`.
Enter Service Manager host name	Enter the fully-qualified domain name (FQDN) of the Service Manager server host.
Is https required in order to access wsdl?	Type `n`.
Enter Service Manger port	Enter the port number of the Service Manager server host used for communication with the RC server. For example: `13080` (default).
Insert the url suffix for the wsdl file	Enter `sc62server/PWS/` (default). **Note:** `SM/7/` is not supported in the current version.

When the above procedure is complete, an <adapter_name>-adapter.zip file (for example, sm-adapter.zip) is automatically generated in Release Control's bin\result folder.

3. Log on to RC as a system administrator, and click **Module** > **Administrator**.
4. Go to **Configuration** > **Integrations** > **Service Desk Adapters**.
5. Click the arrow button and select **Service Desk Adapter**.

   Note: For RC 9.20, go to **Configuration** and click the **Import configuration set** button.

6. In the **Select file to upload** dialog box, browse to <HP Release Control installation directory>\bin\result\<adapter_name>-adapter.zip and open the file.

   A new node with the name of the adapter is added under the **Integrations** > **Service Desk Adapters** node.

7. Save a draft of your configuration.

   a. In the left pane, click the **Save current editable configuration set** button.

   b. In the **Draft name** box, enter the name of the draft and click **Save**.

   Note:
   - A new configuration set is initially saved as a draft. A draft is a configuration set that has not yet been activated.
   - For RC 9.20, the aforementioned step 6 and step 7 should be:

     In the **Select file to upload** dialog box, browse to <HP Release Control installation directory>\bin\result\<adapter_name>-adapter.zip and open the file. In the **Draft name** box, enter the name of the draft and click **Import**.

     A new node with the name of the adapter is added under the **Integrations** > **Service Desk Adapters** node.

8. Activate the draft.

   a. Select the required draft.

   b. Click the **Activate current configuration set** button to activate the selected draft and apply the new configuration properties to RC.

Add a Release Control integration

Applies to User Roles:

System Administrator

To use the HP Service Manager to RC integration, you must first configure the RC adapter and then add and enable an instance of this integration in Integration Manager. It is highly recommended that you enable Lightweight Single Sign-On (LW-SSO) in RC and in Service Manager to bypass the log-in prompts.

The RC integration can work either without UCMDB (that is, in standalone mode) or with UCMDB. This is controlled by the value of the rcStandalone parameter you will specify below.

Note: Before you add and enable the Service Manager to RC integration, be sure to configure the RC adaptor.

To add and enable a Service Manager to RC integration instance, follow these steps:

1. Log on to Service Manager as a System Administrator.
2. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
3. Click **Add**. The Integration Template Selection wizard opens.
4. Select **SMtoRC** from the Integration Template list.
5. Click **Next**. The Integration Instance Information page opens.
6. Verify or complete the fields as necessary.

   Note: Some fields are automatically populated with the information from the integration template. However, you can modify the values for these fields as necessary.

7. Click **Next**. The Integration Instance Parameters page opens.
8. Click the **General Parameters** and **Secure Parameters** tabs, and modify the parameter values as shown in the table below:

Parameter	Value	Example
rc.server.url	`http://<servername>:<port>/ccm`. Replace *<servername>* and *<port>* with the hostname and port number of your RC Server. **Note:** The LW-SSO configuration requires <*servername*> to be the fully qualified domain name (FQDN) of the RC server host.	`http://rc.hp.com:8080/ccm`
rc.adapter.name	Enter your RC adapter name. This is the name you specified when configuring the RC adapter for the Service Manager server. **Note:** When you configured the adapter in RC, RC automatically suffixed the adapter name with "-adapter". Do NOT include the suffix in this field value.	sm
rc.username	Enter the user name of the RC user account that manages multitenancy in RC.	admin
rc.password	Enter the password of the RC user account that manages multitenancy in RC.	admin
rcStandalone	Set to true to enable the RC integration to work without UCMDB; when set to false, both Service Manager and RC must integrate with UCMDB for the integration to work.	true (default)
rcSimplified	Specify this value to true, a simplified and Section 508 compliant RC widget is embedded in SM.	False(default)

Note: It is not recommended to add new parameters, modify parameter names or categories.

9. Click **Next** twice and then click **Finish**. Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

   Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

10. Enable the integration instance.

Enable LW-SSO for the Release Control integration

Applies to User Roles:

System Administrator

LW-SSO is highly recommended for the Release Control (RC) integration for the following purposes:

- To enable RC to synchronize change records from and to Service Manager by calling a HP Service Manager web service using LW-SSO
- To enable users to launch the RC Calendar from within Service Manager using LW-SSO

To enable LW-SSO for the RC integration, complete the following tasks:

- "Configure LW-SSO in the Service Manager server" on page 93
- "Configure LW-SSO in the Service Manager Web tier" on page 94
- "Configure LW-SSO in Release Control" on page 103

Configure language and time zone for the RC integration

Applies to User Roles:

System Administrator

HP Service Manager provides 14 out-of-box (OOB) languages. By default, the Calendar is displayed in the same language as your Service Manager login language. However, Service Manager and Release Control (RC) can be localized into some other languages (for example, Vietnamese) through open localization. In this case, you may need to specify a mapped language ID in Release Control for each new language.

To add a RC ID for Service Manager Calendar, follow these steps:

1. Log on to Service Manager as the System Administrator.
2. Type `db` in the command line and press **Enter**. The Database Manager window opens.
3. Type `language` in the Form field, and click **Search**.
4. Select **language** of the Format Name column and double click it.
5. Click **Search**. A list of records opens.

6. Select a new language (for example, Vietnamese).
7. In the **RC Identifier** field, enter the corresponding language ID in RC (for example, vi).
8. Click **OK**.

HP Service Manager provides 51 out-of-box (OOB) time zones for the RC integration. Service Manager and RC automatically share the same time zone. If you want to use time zones other than OOB ones, you must specify a mapped time zone in Service Manager.

To synchronize the time zone between Service Manager and RC, follow these steps:

1. Log on to Service Manager as the System Administrator.
2. Type `db` in the command line and press **Enter**. The Database Manager window opens.
3. Type `tzfile` in the **Form** field, and click **Search**. The System Parameter Maintenance window opens.
4. Select a value from the **Time Zone Java ID** list.
5. Click **Add**.

Show custom Service Manager fields in Release Control Analysis

Applies to User Roles:

System Administrator

The RC integration uses the ChangeRC record for Change and the ChangeTaskRC record for Task to expose HP Service Manager fields to RC. If you want to create custom exposed fields in the Web Service, you need to perform the following tasks in Service Manager and RC, respectively. The following example shows how to show custom Service Manager **Change** fields in RC analysis.

Task 1. Set which fields to expose to RC in Service Manager

1. Log on to Service Manager as the System Administrator.
2. Go to **Tailoring** > **Web Services** > **WSDL configuration**.

3. In the Object Name field, type `ChangeRC`, and click **Search**.

   The ChangeRC extaccess record opens.

4. Select the **Fields** tab to view exposed fields or add one or more new fields. For details about how to create custom exposed fields in Service Manager Web Services, see the HP Service Manager Web Services Guide.

5. Click **Save**.

Task 2. Configure RC to show the new custom field values

Note:

- The already exposed field of Location (`middle,location`) is used in this example.
- When the WSDL configuration in HP Service Manager is changed, the RC adapter has to be re-generated by running the `SdiConfigurer.bat` utility. Refer to "Configure the RC adapter" on page 126 for more information.

1. Log on to RC as a System Administrator.
2. Go to **Module** > **Administrator** > **Configuration** > **Integrations** > **Fields**.
3. Open the **Miscellaneous** section of the fields, and select the **site-location** field.
4. On the **Field Definition** tab, change the Category to **Analysis Data**.
5. On the **Details Layout** tab, select the **Show in Details tab** checkbox.
6. Click the **Save** button and select a new name for the saved version, such as **new field site location**.
7. Go to **Module** > **Administrator** > **Configuration** > **Integrations** > **Service Desk Adapters**, and choose your Service Manager adapter (for example, **sm-adapter**).
8. Select **convertChange.js** from the adapter's drop-down list. Content of this Java script file is displayed in the right pane..
9. Edit the file by adding a line for the Location field as follows:

```
function convert(sm_rfc, generic_rfc) {
     generic_rfc.setField("request-id", sm_rfc.get("header.changeNumber"));
     generic_rfc.setField("company", sm_rfc.get("header.company"));
     generic_rfc.setField("creation-time",

convertDate(sm_rfc.get("header.origDateEntered")));
     generic_rfc.setField("last-update-time",

convertDate(sm_rfc.get("sysmodtime")));
     generic_rfc.setField("contact-person",

sm_rfc.get("header.coordinator"));
     generic_rfc.setField("initiated-by",

sm_rfc.get("header.requestedBy"));
     generic_rfc.setField("opened-by",

sm_rfc.get("header.openedBy"));
     generic_rfc.setField("implementors",

sm_rfc.get("header.coordinator"));
     generic_rfc.setField("contact-phone",

sm_rfc.get("header.coordinatorPhone"));
     generic_rfc.setField("category", sm_rfc.get("header.category"));
     generic_rfc.setField("subcategory",sm_rfc.get("header.subcategory"));
     generic_rfc.setField("emergency",sm_rfc.get("emergency"));
     generic_rfc.setField("site-location", sm_rfc.get("middle.location"));
// Requested End Date
    setDateField(sm_rfc.get("requestedDate"), "requested-end-date", generic_
rfc);
// Change Priority
var sm_rfc_priority = sm_rfc.get("header.priority");
var rc_priority = "Unknown priority";
if (sm_rfc_priority == 1)
    rc_priority = PRIORITY_IMMEDIATE;
else if (sm_rfc_priority == 2)
    rc_priority = PRIORITY_HIGH;
else if (sm_rfc_priority == 3)
    rc_priority = PRIORITY_NORMAL;
else if (sm_rfc_priority == 4)
    rc_priority = PRIORITY_LOW;
[. . .]
```

10. Add a line to the file for each field you entered in the ChangeRC extaccess record, as shown above.

Note: Remember to use the dbdict-based field name rather than the WSDL Caption for the

> `sm_rfc`, as shown above. The `generic_rfc` uses the field name as defined in **Integrations** > **Fields**.

11. Click the **Save** button to save the modified JavaScript record, and if prompted, enter a new name.
12. Click the **Activate** button.
13. Log out and then log back in.
14. Re-update the change records for the change to take effect.
15. Click a change, and then click **Details** in the lower portion of the screen.

    The Site Location field displays in **Analysis** > **Changes**.

Verify the RC integration setup

Applies to User Roles:

System Administrator

When you have set up an RC integration and enabled LW-SSO for the integration, you can perform the following tasks to see if you have successfully set up your RC integration.

> **Note:** All users that access HP Service Manager from RC must have the SOAP API execute capability in Service Manager.

Task 1. Create test user accounts

1. Create a new operator in Service Manager with the same username as a user account in RC (for example, `admin`), and grant enough rights to this account so that this account can create RFCs.
2. Create a new user (for example, `approver`) in Service Manager with the necessary rights to approve change requests.
3. Add the user (for example, `approver`) to the Approvals list.

a. Go to **Change Management** > **Maintenance** > **Approvals**.

b. Type `Approval` in the Name field, and add the new operator with approval rights to the list, or replace the existing one.

4. Create a new user in RC with the same username (for example, `approver`) and grant it the rights to approve change requests.

Task 2. Test LW-SSO from Service Manager to RC

1. Log on to the Service Manager Web client with user account `admin`.
2. Create a change request, and change its phase to Change Approval.
3. Click **Miscellaneous** > **Calendar**.

If the RC Calendar displays with the RC log-in prompt bypassed, LW-SSO is successfully enabled for integration from Service Manager to RC.

Task 3. Test LW-SSO from RC to Service Manager

1. Log on to RC as `approver`.
2. Approve the new change request synchronized from Service Manager.

If the change request can be approved with the Service Manager log-in prompt bypassed, LW-SSO is successfully enabled for integration from RC to Service Manager.

Change Assessment

The Analysis module displays a detailed analysis of each change request that has entered the system. Change Advisory Board (CAB) members can view information such as the potential impact of the change and the possible risk involved in implementation. The CAB uses this information to make more informed and accurate decisions regarding the approval of planned changes.

- **Assess** > **Impact** Describes how to view the impact analysis calculation results for a change request. See how the business and system configuration items (CIs) are affected by the change request.
- **Assess** > **Collisions** Displays details about all the change requests that collide with the change request selected in the Change Requests pane.

- **Assess** > **Risk** Enables you to view the risk analysis for a change request. See an overall summary of the risk analysis for the selected change request, including distribution charts of the risk factors contributing to the Potential Damage and Probability of Failure calculations. These distribution charts enable you to pinpoint the most significant factors contributing towards the risk level of the selected change request.
- **Assess** > **Similar Changes** Displays a list of changes that are similar to the change request selected in the Change Requests or Action Items pane.
- **Assess** > **Time Period Conflicts** Displays the time period conflicts in which the selected change request is scheduled to take place either outside of a Change Window (periods in which change requests are allowed to take place) or within a Blackout period (periods in which change requests are not allowed to take place).

View Change Assessment in Change Management

Applies to User Roles:

Change Analyst

Change Approver

Change Coordinator

Change Manager

To view Change Assessment for existing changes, follow these steps:

1. Log on to HP Service Manager web client.
2. Click **Change Management** > **Changes** > **Search Changes**.
3. Click **Search**. A list of change records opens.
4. Select a record to view its details.
5. Locate and click **Change Assessment**. You can view the assessment details.

   Note: To view the contents in the Change Assessment section:

- The change should be recorded in the Release Control Calendar.
- You may need to wait for a while until Service Manager and Release Control finish synchronizing the data.

Using RC calculated risk for Change Approval

Applies to User Roles:

System Administrator

Change Manager

Change Approver

HP Service Manager provides the out-of-box (OOB) approval type `Approval Depending on RC Risk Value` for the Change Approval phase. When Service Manager and RC finish synchronizing the data of a change, RC calculates the risk of this change and populates its risk value to Service Manager. If the RC calculated risk value is high, then the approval is triggered by default so that both Change Manager and Change Approver are required to approve or deny the change. If the risk value is low or medium, only Change Approver is required to advance the change to the next phase.

RC calculated risk has three levels: high, medium, and low. System Administrator can change the approval condition of `Approval Depending on RC Risk Value` to trigger the approval upon different risk levels.

Note: RC calculated risk values are not available for the following change categories:

- Subscription
- Knowledge Management
- CI Group
- Unplanned Change

Trigger approvals based on the risk value

To trigger the approval upon certain risk values, follow these steps:

Applies to User Roles:

System Administrator

1. Log on to HP Service Manager as System Administrator.
2. Click **Tailoring** > **Document Engine** > **Approvals**.
3. Click **Search**. A list of approvals opens.
4. Select **Approval Depending on RC Risk Value**.
5. Change the default approval condition `toupper (risk.severity in $L.file="HIGH")` accordingly.

   For example, if you set the condition as `toupper (risk.severity in $L.file="MEDIUM")`, the approval is triggered when the risk value of a change is medium.

   > **Note:** You can also add approval conditions for risk values if necessary.

6. Click **Save**.

To view the risk value populated by RC, follow these steps:

Applies to User Roles:

Change Approver

Change Manager

1. Log on to the Service Manager web client.
2. Click **Miscellaneous** > **Calendar**.
3. Select the change record you want to view from the Summary list.
4. In the **Preview** tab, select **Overview**. You can view the Risk value in the **Analysis Info** section.

Release Control Calendar

When a Release Control (RC) integration is set up in HP Service Manager, you can access the RC Calendar from the System Navigator, from related records of changes (interactions, incidents, and problems), and from Change Management.

The Change Requests — Calendar View pane in RC displays change requests that have been processed by HP Release Control for each calendar day in calendar format. The change requests that appear are those that are included in the currently active filter.

This pane displays the change requests in calendar and/or list format depending on which viewing mode you selected:

- Day and Week mode. Displays the change requests processed by HP Release Control in both table and calendar format.
- Month mode. Displays the number of change requests for each calendar day as a link.

For more information, refer to *HP Release Control User Guide*.

Note: If you disable the RC Calendar, RC time period management, impact analysis, risk analysis and other integrated functions are disabled simultaneously.

View the Calendar from the System Navigator

Applies to User Roles:

Change Analyst

Change Approver

Change Coordinator

Change Manager

To view the Calendar from the System Navigator, click **Miscellaneous**> **Calendar**.

If you are the Change Manager, you can click the **Plan Selected Change** button and update changes in the Calendar.

Note: The Calendar option in the System Navigator is available in the web client only, and can be viewed only after you enable the SMtoRC instance.

View the Calendar from interactions, incidents, or problems

Applies to User Roles:

Service Desk Agent

Service Desk Manager

Incident Analyst

Incident Coordinator

Incident Manager

Problem Analyst

Problem Coordinator

Problem Manager

When the RC integration is added, the rcStandalone parameter controls whether the RC integration works in standalone mode (which does not require UCMDB) or non-standalone mode (which requires UCMDB). In non-standalone mode (that is, when rcStandalone is set to false), you can view the Calendar of a record only when the Affected CI, Service, and Primary CI of the record are captured in UCMDB. In standalone mode, you can view the Calendar as long as these fields are filled in.

To view the Calendar from a new interaction, incident, or problem, follow these steps:

1. Log on to the HP Service Manager web client.
2. Open a new record, as follows:
   - Click **Service Desk** > **Create New Interaction**.
   - Click **Incident Management** > **Create New Incident**.
   - Click **Problem Management** > **Problem Control** > **Create New Problem**.
3. Fill in the required fields.
4. Click **Fill** and select values for the Affected CI, Service, and Primary CI fields, rather than entering the values.
5. For the new interaction, do the following:
   - Click **Escalate**.
   - Fill in the required escalation details.
   - Click **Next**.
   - Scroll down and locate **Calendar**.
6. For the new incident or problem, do the following:

- Click **Save**.
- Scroll down and locate **Calendar**.

The Calendar displays the changes for the CI from the Affected CI, Service, or Primary CI fields for the record.

To view the Calendar from an existing record, follow these steps:

1. Log on to the Service Manager web client.
2. Open the existing record, as follows:
   - Click **Service Desk** > **Search Interaction Records**.
   - Click **Incident Management** > **Search Incidents**.
   - Click **Problem Management** > **Problems Control** > **Search Problems**.
3. Click **Search**. A list of records opens.
4. Select a record to view its details.
5. Scroll down and locate **Calendar**. The Calendar displays the changes for the CI from the applicable Affected CI, Service, and Primary CI fields of the open record.

View the Calendar in Change Management

When the RC integration is added, the rcStandalone parameter controls whether the RC integration works in standalone mode (which does not require UCMDB) or non-standalone mode (which requires UCMDB). In non-standalone mode (that is, when rcStandalone is set to false), you can view the Calendar of a record only when the Affected CI, Service, and Primary CI of the record are captured in UCMDB. In standalone mode, you can view the Calendar as long as any or all of these fields are filled in.

- "View the Calendar for new or existing changes" below
- "View the Calendar for new or existing change tasks" on page 144

View the Calendar for new or existing changes

Applies to User Roles:

Change Analyst

Change Approver

Change Coordinator

Change Manager

To view the Calendar for new changes, follow these steps:

1. Log on to HP Service Manager web client.
2. Do one of the following:
   - Click **Change Management** > **Changes** > **Create New Change** if you are not working with Service Manager Process Designer (PD).
   - Click **Change Management** > **New Change** if you are working with Service Manager Process Designer (PD).
3. Select a change category.

   Note: The Calendar section is not available for the following change categories:

   KM Document, Release Management, and Subscription

4. Fill in the fields as required.

   Note: To view the Calendar for the new change:

   - Make sure the Affected CI, the Service or both are filled in.
   - Click **Fill** and select values for the Affected CI field rather than entering the values.

5. Click **Save**.
6. Locate and click **Calendar**. The Calendar displays the changes for the CI from the Affected CI and the Service fields of this change.

To view the Calendar for existing changes, follow these steps:

1. Log on to Service Manager web client.
2. Do one of the following:

- Click **Change Management** > **Changes** > **Search Changes** if you are not working with Service Manager Process Designer (PD).
- Click **Change Management** > **Search Changes** if you are working with Service Manager Process Designer (PD).

3. Click **Search**. A list of change records opens.
4. Select a record to view its details.
5. Locate and click **Calendar**. The Calendar displays the changes for the CI from the Affected CI and the Service fields of this change.

> **Note:** The Calendar section can be viewed only when the Affected CI, or the Service, or both are filled in.

View the Calendar for new or existing change tasks

Applies to User Roles:

Change Analyst

Change Approver

Change Coordinator

Change Manager

To view the Calendar for new change tasks, follow these steps:

1. Log on to HP Service Manager web client.
2. Do one of the following:
   - Click **Change Management** > **Tasks** > **Create New Task** if you are not working with Service Manager Process Designer (PD).
   - Click **Change Management** > **Create New Task** if you are working with Service Manager Process Designer (PD) Content Pack 9.30.3.
3. Select a change task category.

Note:

- In non-PD environment, the Calendar section is not available for the following change task categories:

  Create Group, Create Release, Delete Group, Identify Affected Systems, Update Affected Systems, and Update Group

- In PD environment, the Calendar section is not available for the following change task categories:

  Create Group, Delete Group, and Update Group

4. Fill in the fields as required.

Note: To view the Calendar for the new change task:

- Make sure the Affected CI, the Service or both are filled in. Both the start date and the end date are filled in. The start date and end date are configured in calendar mappings with change task. See Configure calendar mappings for more information.
- click **Fill** and select values for the Affected CI field rather than entering the values.

5. Click **Save**.
6. Locate and click **Calendar**. The Calendar displays the changes for the CI from the Affected CI and the Service fields of this change task.

To view the Calendar for existing change tasks, follow these steps:

1. Log on to Service Manager web client.
2. Do one of the following:
   - Click **Change Management** > **Tasks** > **Search Tasks** if you are not working with Service Manager Process Designer (PD).
   - Click **Change Management** > **Search Tasks** if you are working with Service Manager Process Designer (PD).

3. Click **Search**. A list of change records opens.
4. Select a record to view its details.
5. Locate and click **Calendar**. The Calendar displays the changes for the CI from the Affected CI and the Service fields of this change task.

   Note: The Calendar section can be viewed only when the Affected CI, or the Service, or both are filled in, and both the start date and the end date are configured in calendar mappings.

Multitenancy (multicompany) support

The HP Release Control (RC) integration supports multitenancy, which allows users to see change records in RC for their authorized tenants only. For example, when a user from Company A logs on to HP Service Manager, the user can only view (from changes, interactions, incidents, problems, or the System Navigator) the data of Company A's account in RC through Calendar.

Note:

- In Service Manager, some users may be able to view data of more than one company, but in Calendar they can view the data of only one company at one time, which is determined by the user's Default Company defined in Service Manager.
- To support multitenancy, both Service Manager and RC must integrate with UCMDB. If you have deployed your RC integration without UCMDB, the multitenancy feature is not available.

Enable multitenancy for Service Manager and UCMDB

Applies to User Roles:

System Administrator

Note: To support multitenancy, both HP Service Manager and RC must integrate with UCMDB. If you have deployed your RC integration without UCMDB, the multitenancy feature is not available.

To enable multitenancy for Service Manager and UCMDB, follow these steps:

1. Log on to Service Manager as a System Administrator.
2. Go to **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
3. Select the **Run in Multi-Company Mode** check box under the **General** tab.
4. Select the **HP Universal CMDB** check box on the **Active Integrations** tab.
5. Provide values for the following fields:

Field	Description
UCMDB webservice URL	Type the URL to the UCMDB Web Service API. The URL has the following format: *<UCMDB server name>*:*<port>*/axis2/services/ucmdbSMService Replace *<UCMDB server name>* with the host name of your UCMDB server, and replace *<port>* with the communications port your UCMDB server uses. Example: *<UCMDB.hp.com>*:8080/axis2/services/ucmdbSMService
UserId	The user ID of the user account that has permission to access the UCMDB Web Service API.
Password	The password of the user account that has permission to access the UCMDB Web Service API.
Multi-tenant UCMDB webservice URL	Type the URL to the UCMDB Web Service API. The URL has the following format: *<UCMDB server name>*:*<port>*/axis2/services/UcmdbManagementService Replace *<UCMDB server name>* with the host name of your UCMDB server, and replace *<port>* with the communications port your UCMDB server uses. Example: *<UCMDB.hp.com>*:8080/axis2/services/UcmdbManagementService
UserId	The user ID of the user account that has permission to access the multitenant UCMDB Web Service API.

Field	Description
	Example: sysadmin
Password	The password of the user account that has permission the access the multitenant UCMDB Web Service API. Example: sysadmin

Note: In the **UCMDB webservice URL** and **Multi-tenant UCMDB webservice URL** fields, you do not need to enter http:// or any trailing slashes. You only need to provide the host name, port, and the Web Services API to the HP Universal CMDB server.

6. Click **Save**.

Add or update a company record and deactivate tenancy

Applies to User Roles:

System Administrator

Note: To support multitenancy, both HP Service Manager and RC must integrate with UCMDB. If you have deployed your RC integration without UCMDB, the multitenancy feature is not available.

To add or update a company record and deactivate tenancy, follow these steps:

1. Log out, and then log on to Service Manager again as a System Administrator after you "Enable multitenancy for Service Manager and UCMDB" on page 146.
2. To add a company record into tenant, follow these steps:
   a. Go to **System Administration** > **Base System Configuration** > **Companies**.
   b. Provide values for the fields as necessary.
   c. Select **Yes** in the Show Company in Multi-Company Lists field.
   d. Provide a value for the UCMDB Customer ID field.

Note: The UCMDB Customer ID must be a positive integer, not including 1.

e. Click **Add**. A dialog box opens, asking "Do you want to synchronize with UCMDB and Release Control?"

- If you select **Yes**, a company record synchronized with UCMDB and RC is added. On the Company Information page, you can see the read-only checkboxes of **Synched with UCMDB** and **Synched with RC** are selected.
- If you select **No**, a company record is added but without being synchronized with UCMDB and RC. You can synchronize the record later.

Note:

- Each added company record has a unique Customer ID. A new company record given an existing Customer ID cannot be successfully added.
- The company information synchronized with RC includes Customer ID and Company Code. Once synchronized, the Company Code of the record becomes read-only.
- If you selected **Yes** and RC failed to synchronize the record due to some reasons, you can see the **Synched with RC** check box is unselected on the Company Information page. To synchronize the record to RC, you need to update and save the record.

3. To update a company record, follow these steps:

a. Search the company record list and select a record you want to update.

b. Update the company information as necessary.

c. If you want to enable multitenancy for this company record, make sure to select **Yes** in the **Show Company in Multi-Company Lists** field.

d. Click **Save**. The result could be one of the following:

- If both **Synched with UCMDB** and **Synched with RC** are unselected, a dialog box opens, asking "Do you want to synchronize with UCMDB and Release Control?" Click **Yes**. The record is then automatically synchronized with UCMDB and RC.

- If **Synched with UCMDB** is selected while **Synched with RC** is unselected, no dialog box opens. The record is automatically synchronized with RC if it is not successfully synchronized with RC yet.
- If both **Synched with UCMDB** and **Synched with RC** are selected, the record is repeatedly synchronized to RC and no dialog box opens. You can see the modification you made to the record in Service Manager. In this case, since the Company Code is read-only, the record is not updated in RC.

Note:

- To synchronize a record with RC, it is mandatory to click **Yes** in the Question dialog box.
- You can view the synchronizing results of company data in a log file. For the location of the file, go to **Tailoring** > **Integration Manager** and select the SMtoRC integration. The Log File Directory field on the **Integration Instance Information** page indicates the location of the log file.
- It may take some time before you can see the check boxes selected, as it takes time to implement a schedule.

4. To deactivate a company's tenancy, follow these steps:
   a. Search the company record list and select a company record you want to deactivate.
   b. Select **No** in the **Show Company in Multi-Company Lists** field.
   c. Click **Save**.
   d. Click **Yes** in the question dialog box.

Re-synchronize a company record with RC

Applies to User Roles:

System Administrator

In some cases, you need to re-synchronize a company record with RC. For example, if a company record was synchronized to RC and was deleted later in RC, you can re-synchronize the record to generate a new record in RC; if the tenants information in Service Manager and RC does not match, you can re-synchronize the information to RC.

Note: To support multitenancy, both Service Manager and RC must integrate with UCMDB. If you have deployed your RC integration without UCMDB, the multitenancy feature is not available.

1. Open a company record that was synchronized with RC.
2. Click **Re-Synch** next to the **Synched with RC** check box. The company record is re-synchronized.

Note: The **Re-Synch** button for the **Synched with RC** check box is disabled unless you selected **Yes** in the **Show Company in Multi-Company Lists** field and the record was successfully synchronized with RC.

HP Universal CMDB

HP Universal CMDB is a Configuration Management database for enterprise IT organizations to capture, document, and store information about configuration items (CIs), service dependencies, and relationships that support business services. When integrated with a Service Manager system, HP Universal CMDB stores the actual state of CIs and CI relationships, while the Service Manager system stores the expected or managed state of the CIs. Service Manager tracks any change requests, baselines, and historical updates CIs in the HP Universal CMDB.

Service Manager can integrate with UCMDB, as well as with UCMDB Configuration Manager (a UCMDB component) and UCMDB Browser (a UCMDB add-on).

HP Universal CMDB Integration Guide

The *HP Universal CMDB Integration Guide* aids Service Manager implementers who are responsible for integrating a HP Universal CMDB system with a HP Service Manager system. The guide also has instructions on the following topics:

- Integration requirements
- Integration setup steps
- Service Manager reconciliation rules
- Service Manager Discovery Event Manager rules
- Integration tailoring options

You can view and search this guide using Adobe® Reader, which you can download from the Adobe Web site.

The *HP Universal CMDB Integration Guide* is available from the help.

Enable an integration to HP Universal CMDB

Applies to User Roles:

System Administrator

You must have the **SysAdmin** capability word to use this procedure.

You can configure Service Manager to display the actual state of CIs in the HP Universal CMDB server by defining an active integration in the System Information Record. After you define this active integration, Service Manager displays the Actual State tab in Configuration Management forms, and displays the **View in UCMDB** or **View in UCMDB Browser** button in CI records synchronized from UCMDB.

Note: The UCMDB Browser is an optional add-on to UCMDB. For more information, see "HP Universal CMDB Browser" on page 157.

To enable an integration to UCMDB in Service Manager:

1. Click **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
2. Click the **Active Integrations** tab.
3. Select the **HP Universal CMDB** option.
4. Complete the following fields.

Field	Description
UCMDB webservice URL	This is the URL to the HP Universal CMDB web service API. The URL has the following format: `http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService` Replace <*UCMDB server name*> with the host name of your UCMDB server, and replace <*port*> with the communications port your UCMDB server uses.
UserId Password	This is the UCMDB account (user name/password) used to synchronize CI information with Service Manager. For example, admin/admin.
Multi-tenant UCMDB webservice URL	This is the URL that Service Manager uses to synchronize company records with UCMDB when running in multi-company mode. This URL should use the following format: `http://<ucmdb server name>:<port>/axis2/services/UcmdbManagementService`.
UserId Password	This is the UCMDB account (user name/password) that has the privilege to add/delete company records.
UCMDB Browser	This is the UCMDB Browser URL. It is in the following format:

Field	Description
URL	`http://<UCMDB browser server name>:<port>/ucmdb-browser` For example: **http://myucmdbbrowserserver:8081/ucmdb-browser** **Note:** The **UCMDB Browser URL** field is required to enable an integration to the UCMDB Browser. If you specify a value for this field, the **View in UCMDB Browser** button will replace the **View in UCMDB** button in CI records synchronized from UCMDB; only when you leave this field empty, the **View in UCMDB** button is displayed.

5. Click **Save**.

   Service Manager displays the message:

   Information record updated.

Note: To enable the integration, you still need to set up an integration point in UCMDB. For details, see HP Universal CMDB Integration Guide.

Configuration item actual states

By default, HP Service Manager only stores and displays the expected or managed state of CIs. The information Service Manager displays in the Configuration Management form is essentially the definitive list of attributes that the CI should have. However, the actual state of the CI may differ from the expected state.

To view the actual state of the CI, you must first create an integration to an HP Universal CMDB server. The HP Universal CMDB server periodically discovers the actual state of CIs and records the actual state in the Configuration Management database. Service Manager accesses the actual state information by using a Web services connection. Service Manager sends the CI ID to the HP Universal CMDB server and receives a full list of the attributes for that CI. Service Manager displays the CI attributes in the Actual State section of the Configuration Management form.

If a Service Manager CI does not have a matching CI in the HP Universal CMDB server, then Service Manager does not display the Actual State section. For example, you may track office furnishing CIs in Service Manager that cannot be discovered and tracked in the HP Universal CMDB.

View the actual state of a configuration item

Applies to User Roles:

Configuration Manager

Configuration Administrator

Configuration Auditor

This procedure requires that your HP Service Manager system has an active integration to an HP Universal CMDB server.

To view the actual state of a configuration item, follow these steps:

1. Click **Configuration Management** > **Resources** > **Search CIs**.
2. Use search or advanced search to find one or more records.
3. Select the CI with the actual state you want to see.
4. From the CI detail form, open the **Actual State** section. Service Manager displays the actual state of the CI, as well as its UCMDB Id value.

   Note: The **Actual State** section is only visible if your system has an active integration to an HP Universal CMDB server and the CI has a matching entry in the Configuration Management database. Service Manager does not display the **Actual State** section if there is no matching CI in the HP Universal CMDB server.

Multi-tenant (multi-company) support

The HP Universal CMDB (UCMDB) to HP Service Manager Integration supports a multitenancy configuration in which both the Service Manager and UCMDB systems track Configuration Items (CIs) and Configuration Item Relationships (CIRs) by company ID. In a multi-tenancy configuration, you can tailor the integration so that each tenant only sees and works with the CIs and CIRs that match their company ID. Multi-tenancy is intended for managed service providers (MSPs) who wish to offer Configuration Management as a service to multiple tenants.

What multi-tenant information is stored in UCMDB?

Your UCMDB system stores a company ID attribute for each CI and CIR. The company ID determines what adapter and synchronization schedule your UCMDB system uses to update CI data. Each CI and relationship record can only have one company ID. The UCMDB system obtains a company ID from the Service Manager system.

If more than one tenant (company) shares the same CI, each tenant has their own unique CI record describing the CI. In effect, the UCMDB system creates multiple CI records to track one managed asset. Each tenant's CI record is unique to that tenant and lists the company's unique company ID.

What multi-tenant information is stored in Service Manager?

Your Service Manager stores the company records that describe each tenant in the multi-tenant configuration. The Service Manager system is the definitive source of company IDs and pushes new and updated information to your UCMDB system.

Service Manager tracks the company ID of each CI and relationship in a multi-tenant configuration. CI records inherit the company ID of the UCMDB feeder that discovered them. Relationship records inherit the company ID of the parent CI in the relationship.

In a best practices implementation, Service Manager uses Mandanten to ensure that operators only see CI and relationship records where the CI's company ID matches the operator's company ID. If you restrict the view with Mandanten, then Service Manager also restricts the view to all other related records such as change requests and incidents.

For more information, refer to the *HP Universal CMDB to HP Service Manager Integration Guide* available from the HP Software Product Manuals site.

HP Universal CMDB Configuration Manager

HP Universal CMDB Configuration Manager (Configuration Manager) provides the tools to help the system manager better control the CMS (Configuration Management System) data. It focuses primarily on analyzing and controlling the data in the CMS, as the ITIL directs. Configuration Manager provides an environment for controlling the CMS infrastructure, which encompasses many data sources and serves a variety of products and applications.

The Configuration Manager to Service Manager (CM-SM) integration provides a policy-based change control solution that can handle configuration changes effectively. This solution is different from the UCMDB to Service Manager (UCMDB-SM) integration solution, which provides attribute modeling change control. The UCMDB-SM integration solution provides the most control but requires manual attribute data entry and can generate a large amount of unplanned changes to be reviewed and accepted or backed out. For customers that do not need change planning at this level of detail, the CM-SM integration solution is recommended.

Using Configuration Manager, the UCMDB authorized state is pushed to Service Manager, and Service Manager benefits from working with the same data that resides in the CMS and can be easily consumed by other parties. The data provided to Service Manager is already controlled and of high quality, and Service Manager therefore no longer holds a distinct state of its CIs. As the state of a configuration item is fully managed by the CMS (including actual, authorized, and historical states), the configuration controls implemented in the UCMDB-SM integration in which Service Manager must analyze which CI changes require an RFC are not used. Service Manager now consumes both actual and authorized CI states from UCMDB.

For more information about the CM-SM integration solution, refer to the following Universal CMDB Configuration Manager documents:

- *HP Universal CMDB Configuration Manager User Guide*, which is available from the HP Software Manuals Site
- *Technical white paper: Handle configuration changes effectively* (**http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA0-7486ENW.pdf**)

HP Universal CMDB Browser

The UCMDB Browser is a lightweight web-based client to access UCMDB data. The UCMDB Browser provides a simple and intuitive search for Configuration Items (CIs) in UCMDB and displays important data in the context of the selected CI. It is an ideal tool for providing quick access to specific CI information. For each CI, relevant data is presented and gathered into information widgets (for example, Properties, Environment, and Impact Simulation widgets). Data is presented by default in a Preview mode, with the option to view more comprehensive data in an Expanded mode.

How to integrate Service Manager with the UCMDB Browser

You enable an integration to the UCMDB Browser when enabling an integration to UCMDB. For details, see "Enable an integration to HP Universal CMDB" on page 152.

Supported use cases

When integrated with UCMDB Browser, Service Manager provides the following out-of-box features.

Viewing CI information in the UCMDB Browser

A **View in UCMDB Browser** button is available in the Configuration Item form. This button is displayed in each CI record that is synchronized from UCMDB. When a user clicks this button a CI, a UCMDB Browser login screen is displayed; after the user logs in with a UCMDB Browser account (username/password), the UCMDB Browser opens in the context of this CI.

Retrieving primary CI change history from the UCMDB Browser

The Change History widget from the UCMDB Browser is displayed in a problem record whose primary CI is synchronized from UCMDB. This widget is provided in the **Primary CI History in UCMDB** tab on the Problem form. Users can view the CI changes on that primary CI for root cause investigation.

Note: For accessibility support of the embedded UCMDB widget, refer to the UCMDB Browser documentation.

Support of Automated Service Modeling (ASM)

Note: Automated Service Modeling requires the UCMDB ASM Enhanced package to be deployed in UCMDB.

As version of 9.41, Service Manager supports the ASM functionality in the UCMDB Browser. Service CIs and consumer-provider relationships that are discovered by ASM can be pushed to Service Manager; additionally, you can tailor Service Manager such that Service Manager users can access ASM in the context of a business service, and access Impact Simulation in the context of an affected CI.

Support of ASM enables Service Manager users to view the accurate service trees that are discovered by ASM and facilitates service modeling in Service Manager.

For details, see the UCMDB Integration Guides.

Discovery Event Manager

The Discovery Event Manager tool provides you with information about configuration items (CIs) in use by your organization. Discovery Event Manager collects data from associated Web services, such as the HP Universal Configuration Management Database (UCMDB) for enterprise IT organizations. UCMDB captures, documents, and stores information about CIs, service dependencies, and relationships that support business services. The Discovery Event Manager tool takes the information captured by UCMDB and compares the actual state of each incoming CI record (both existing and new) to the managed field state of the CI record in HP Service Manager.

If the actual state of an incoming UCMDB CI record differs from the managed field state of the CI record in Service Manager, the Discovery Event Manager tool works with Configuration Management and Change Management to perform any required changes to the incoming CI record according to the rules you have set in the Discovery Event Manager tool.

Discovery Event Manager change open process

You can use the Discovery Event Manager tool to automate the change open process. When a change is needed to address issues for review or tasks to be performed, the change open process begins. The change goes through phases that drive the unplanned change through the necessary tasks to update the managed fields of a CI or to determine if the change is necessary or desired. To see an Unplanned Change flow diagram, see the related topics.

The change phases are as follows:

Discovery Assessment phase: Assess whether or not an unplanned change is allowed. Comments can be added and updated in this phase, as needed. The CCB Approver must confirm that the change is desired.

- If the change is approved, update the managed field and close the change.
- If the change is denied, move it to the Discovery Backout phase to undo the change.

Discovery Backout phase: Back out a change after determining that the change is not necessary or desired. Comments can be added and updated in this phase, as needed, including updates to modified data. If the backout of the change is complete, move it to the Discovery Verification phase.

- If the denied change is verified, close the change.
- If the denied change is not verified, return to the Discovery Backout phase.

Discovery Implementation phase: The change requires further consideration before it is closed.

- If the backout of the change fails verification, return to the Discovery Implementation phase for further consideration.
- If verification of the change succeeds, close the change.

Discovery Verification phase: Verify that the change is successfully implemented.

- If verification of the change fails, return to the Discovery Implementation phase.
- If verification of the change succeeds, close the change.

Discovery Event Manager managed fields

Managed fields are key fields in the HP Service Manager configuration item (CI) record types that the Discovery Event Manager tool uses to validate the incoming CI records from Web services. By default, the fields of the incoming CI records should match the key fields in the Service Manager CI records.

If Discovery Event Manager discovers any discrepancies between the actual state of the incoming CI record fields and the Service Manager managed fields, these discrepancies are handled by Change Management by default. Rules define what to do with a CI record to make it compliant with the CI record types in Service Manager.

Add a managed field in Discovery Event Manager

Applies to User Roles:

System Administrator

Managed fields are key fields in HP Service Manager configuration item (CI) record types. They are important to helping the Discovery Event Manager tool to discover differences between the data in the incoming CI records from Web services versus what Service Manager is expecting to receive in those records. If the incoming records do not match the managed key fields in Service Manager, the rules set in the Discovery Event Manager tool determine what will happen to those incoming CI records.

For example: If the joinbizservice table has three fields in the Managed Fields tab in Discovery Event Manager and some of the expected information is different or missing from any of those fields, the Discovery Event Manager tool will deal with that incoming CI record that is not compliant with the Service Manager managed fields for that CI record type.

If you determine that a necessary field is not included in the existing discovery process, you can add a managed field to the applicable table using the settings on the **Managed Fields** tab.

Note: If a managed field does not exist in an incoming CI record, the Discovery Event Manager tool is not able to find discrepancies based on that field.

Tips: The following steps describe how to manually add a managed field. If you want to automatically add multiple or all fields from a table as managed fields, you can click the **Load Fields** button on the **Managed Fields** tab.

To add a managed field:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager rules form is displayed.
2. Click **Search** to retrieve a list of CI ID types.
3. Select the ID type for the fields you want to view, and then select the **Managed Fields** tab. You can see which fields are being managed for this CI type.
4. To select a new field you want managed, do the following:
   a. Select the drop-down arrow in the next blank **Field Name** field. You will see the list of fields related to this CI type.
   b. Select the field you want to add to the **Managed Fields** tab for this CI type.
   c. For a field that is part of an array of structures, choose a **Structure** and specify the field's **Index** value. For example, the CI type computer contains array elements, such as ports, printers, and scanners. Choose an array element within the structure, and then choose the corresponding index number.
   d. Click **Save**.
5. Repeat this process to add a managed field for another ID type.
6. Click **OK**.

View, modify, or delete a managed field in Discovery Event Manager

Applies to User Roles:

System Administrator

Managed fields are important to ensuring that the Discovery Event Manager tool can process incoming configuration item (CI) data from Web services. When the inventory of your organization changes, you can add or update the CI types based on your new inventory requirements. You can also review the managed fields for existing CI types to determine if the necessary fields exist and add, modify, or delete managed fields.

Warning: If you are deleting a field, make sure you select the field you want to delete. If you delete the wrong field, you must add the field back into the Managed Fields tab.

To view, modify, or delete a managed field:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form is displayed.
2. Click **Search** to retrieve a list of CI ID types.
3. Select the ID type for the fields you want to view, and then select the **Managed Fields** tab. A list of managed fields for the selected CI type is displayed.
4. Select the field you want to edit or delete.
   - Make any necessary changes.
   - Click **Delete** to delete a field that is no longer valid.
   - Click **Save**.
5. Click **OK**.

Discovery Event Manager rules

Discovery Event Manager processing is governed by rules that define what actions Discovery Event Manager will perform when the actual state of an incoming configuration item (CI) record differs from the managed state of a CI record in HP Service Manager.

During initial configuration of Discovery Event Manager, you start with a basic set of rules for Change Management. You can refine those rules as necessary. Each rule identifies a series of checks that Discovery Event Manager processes whenever a CI record is received from Web services. Depending on the rule, Discovery Event Manager may add or delete the record, open a change, log the information, or update the record's status.

Service Manager opens a change or incident based on the settings defined in the `populateChange` or `populateIncident` function in the `discoveryEvent` ScriptLibrary record. You can override the default settings by writing a custom JavaScript on the **Change Customization** or **Incident Customization** tab.

Discovery Event Manager rule options

Rules help to automate the process of managing incoming configuration item (CI) records. When you have rules set up, you can manage whether a record is added, updated, or deleted to the CI records in HP Service Manager. The Discovery Event Manager tool checks the incoming CI records and determines

what to do when the actual state of the CI records does not match the managed state of the CI records in HP Service Manager. When Discovery Event Manager finds the rule that applies to an incoming CI record type, the server checks the rule, and then updates the record according to the rules you have set up.

Example: If a user's machine has 4 GB of RAM added and the Discovery Event Manager tool discovers that the actual state of the CI record does not match the HP Service Manager managed state for that CI record type, the Discovery Event Manager tool opens an unplanned change. This then gives the Change Manager the opportunity to review the CI record and determine what tasks to complete.

Actions are required in the following cases:

- Records that do not exist.
- Records that contain unexpected data.
- Records are marked for deletion.

The following options are available when configuring rules to meet your business needs:

- **Action if matching record does not exist:** If a CI record does not exist in Service Manager.
  - **Add the record:** (Default) When the information received from Web services through Discovery Event Manager does not bring up a matching record in Service Manager, add the record.
  - **Add the record, and set dependency as true**: This option is available only for synchronization of CI relationship data. Service Manager will add the CI relationship record and enable outage dependency for the record by checking its **Outage Dependency** check box and setting its number of dependent downstream CIs to 1.
  - **Open an Incident:** Open an incident to investigate a new CI record that currently does not exist in Service Manager to determine if it is compliant with Service Manager.
  - **Open a Change:** Open an unplanned change to review the new CI record, because it currently does not exist in Service Manager. This change gives the Service Manager Administrator an opportunity to deny the Change Management request and back it out by using the change management process or to accept the actual state of the new CI record and assign tasks accordingly.
- **Action if record exists but unexpected data discovered:** Changes to the information in an existing CI record raise a flag for the Discovery Event Manager tool. Some of the information is not part of the managed state in Service Manager. The unexpected data in the CI record must be logged or reviewed.

- **Open a Change:** (Default) Open an unplanned change to review the actual state of the CI record. This change gives the Service Manager Administrator an opportunity to deny the Change Management request and back it out by using the change management process, or to accept the actual state of the existing CI record and assign tasks accordingly.
- **Log Results and update record:** Log the results of the actual state of the CI record, and then update the record.
- **Open an Incident:** Open an Incident to investigate the actual state of a CI record and determine what actions must be performed or initiated to bring the record into compliance with Service Manager.

- **Action if record is to be deleted:** If an external event specifies that the record needs to be deleted.
  - **Delete record:** (Default for CI relationship records) This option is available for synchronization of both CI and CI relationship records. Service Managerautomatically deletes the record.
  - **Open an Incident**: This option is available only for synchronization of CI relationship records. Service Manager opens an incident to investigate the deleted record and determines which actions must be performed or initiated to bring the record into compliance with Service Manager.
  - **Open a Change**: This option is available only for synchronization of CI relationship records. Service Manager opens an unplanned change to review the deleted record. The change allows someone to investigate whether the deleted record is compliant with your business practices. If the record is compliant, the change can be approved. If the record is not compliant, then the change can be denied and the record added back to the system.
  - **Update record to the selected status:** (Default) This option is available only for synchronization of CI records. Service Manager updates the status of the CI record to a value selected from the drop-down list (for example, **Retired/Consumed**), instead of deleting the record permanently.
  - **Open an Incident to update record to the selected status:** This option is available only for synchronization of CI records. Service Manager opens an incident to update the record's status to a value selected from the drop-down list (for example,**Retired/Consumed**). Once the incident has been closed, Service Manager automatically updates the CI record to the selected status.
  - **Open a Change to update record to the selected status:** This option is available only for synchronization of CI records. Service Manager opens an unplanned change to update the CI record's status to a value selected from the drop-down list (for example, **Retired/Consumed**). The change allows someone to investigate whether the requested status change is compliant with your business practices. Once the change has been approved and closed, Service Manager

automatically changes the CI record to the selected status. If the change has been denied, Service Manager makes no changes to the CI record.

Add a rule in Discovery Event Manager

Applies to User Roles:

System Administrator

Rules are the core of Discovery Event Manager processing. Based on your organization's requirements, you can refine the basic set of rules that are configured with the Discovery Event Manager tool by adding rules.

To add a rule:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **New**. The new rule form opens.
3. Enter the new rule name.
4. Select a table to be associated with the rule from the **Table Name** list, and then click **Next**.
5. Enter the condition for the rule. The rule is added to the records table.
6. Click **Save**.
7. Click **OK**.

View or modify rules in Discovery Event Manager

Applies to User Roles:

System Administrator

Rules help you to automate the change control process, so that incoming configuration item (CI) records can be updated to comply with the CI record fields in HP Service Manager. As you reevaluate your organization's requirements, you may view the rules that are set up and make changes as you see fit.

To view or modify existing rules:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **Search** to retrieve a list of CI ID types.
3. Select the ID type for the rules you want to view.
4. Select the **Rules** tab. The existing rules settings for the selected CI type are displayed.
5. If you want to edit the rule, do the following:
   - Make the necessary changes. For example, if you choose to select a different action step for records that do not exist, make your change.
   - Click **Save**.
6. Click **OK**.

Delete a set of rules in Discovery Event Manager

Applies to User Roles:

System Administrator

Rules help to automate the change control process, so that incoming configuration item (CI) records can be updated to comply with the CI record fields in HP Service Manager. As you reevaluate your organization's requirements, you may realize that the existing rules settings for a CI type are no longer valid. You can delete the existing rules settings to replace them with a new set of rules.

Warning: Make sure you are deleting the rules for the CI ID type you want deleted. If you delete the wrong set of rules by mistake, you will have to add the CI ID type and set up the rules for each action that needs to be taken.

To delete a set of rules:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **Search** to retrieve a list of CI ID types.
3. Select the CI ID type, and then select the **Rules** tab. Existing rules settings for the selected CI type are displayed.

4. After you determine that you want to delete the rules for this CI type, click **Delete**.
5. Click **OK**.

Create a DEM reconciliation rule

Applies to User Roles:

System Administrator

It is possible that your Service Manager system already contains CI records that match CIs in your UCMDB system. Rather than add duplicate CI records to your Service Manager system, you can configure Service Manager to reconcile CI records between the two systems based on specified Discovery Event Manager (DEM) reconciliation rules.

A DEM reconciliation rule record allows you to specify what Service Manager queries you want to use to determine whether an existing CI record matches a CI in an UCMDB system. An administrator typically specifies reconciliation rules prior to starting the integration to the HP Universal CMDB system so that Service Manager will not create duplicate CI records.

When performing CI reconciliation between Service Manager and UCMDB, Service Manager uses the **ucmdb.id** field to query the device table or a join table to determine whether an Update or Create operation is needed. The reconciliation process is as follows:

1. The UCMDB system sends a web service message containing the latest CI attribute data to Service Manager.
2. Service Manager scans the web service message for the CI ucmdb.id value.

   Note: The ucmdb.id field is displayed in the Actual State Section of the CI form, with a label of **Ucmdb ID**.
3. Service Manager searches for an existing CI record that has the same ucmdb.id value.
4. If Service Manager finds a CI that has the ucmdb.id value, no reconciliation is needed. Service Manager compares the UCMDB CI attributes to the Service Manager managed fields and runs the appropriate Discovery Event Manager (DEM) rules as needed to update the CI record in Service Manager.
5. If Service Manager cannot find a CI that has the ucmdb.id value, it searches for a DEM reconciliation rule record that is defined for the CI type.

6. If no DEM reconciliation rule record is found, Service Manager creates the CI record according to the appropriate DEM rules.

7. If a DEM reconciliation rule record is found, Service Manager evaluates the rules and appends (ucmdb.id=NULL or ucmdb.id~=NULL and istatus="XXXXXX") to the reconciliation rules in the backend, where the istatus value is retrieved from the DEM rule for deletion (for example, **Retired/Consumed**). If no istatus value is found in the DEM rule, Service Manager only appends ucmdb.id=NULL to the reconciliation rules in the backend.

8. If no matching CI record is found by the reconciliation rules, Service Manager creates the CI record according to the appropriate DEM rules.

9. If a matching CI record is found by the reconciliation rules, Service Manager updates the CI record according to the appropriate DEM rules

Using join tables for reconciliation

When setting reconciliation rules, if the CI type you are reconciling has a joindef definition (as defined in the devtype table), use the join table name instead of the device table. For example, if you want to reconcile computer CIs, use the joinnode table instead of the device table.

Sequence of reconciliation

By default, Service Manager executes the reconciliation rules in their listed order. To change the order in which Service Manager reconciles CIs, you can add a numeric value to the **Sequence** field.

Multi-company mode

By default, Service Manager uses only the ucmdb.id field for CI reconciliation, and the company.id field is not used. You can manually add DEM reconciliation rules.

Steps to create a DEM reconciliation record

To create a DEM reconciliation rule record, follow these steps:

1. Click **Tailoring** > **Web Services** > **DEM Reconciliation Rules**.

   Service Manager displays the DEM Reconcile Record form.

2. In the **Table** field, select a Service Manager table against which you want to run reconciliation queries.

Note: Only tables that are specified in CI type records are displayed in the drop-down list. You can create only one DEM reconciliation record for one table.

3. Click **New**.
4. Enter expressions in the **Expression** column, and enter a sequence number for each expression in the **Sequence** column. For example, you can add the following expressions for the **device** table. In this example, Service Manager looks for a matching record first based on the logical.name field, and then based on the sm.device.display.name field.

Expression	Sequence
logical.name=logical.name in $L.file	1
sm.device.display.name=sm.device.display.name in $L.file	2

5. Click **Add**.

   Service Manager creates the reconciliation rule record.

Add a configuration item in Discovery Event Manager

Applies to User Roles:

System Administrator

As inventory changes within your organization, you will need to add new configuration item (CI) types, or possibly update or delete others, to keep your inventory records up-to-date for the Discovery Event Manager tool. You can manage the CI types in the CI record type table.

To add a configuration item in Discovery Event Manager:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **New**.
3. Enter the name of the new CI record type.
4. Select a table from the table list, and then click **Next**.

5. Enter the Condition for the CI record type. The CI record type is added to the records table.

   - The condition must ensure that only one rule is applied when the web service request is processed.
   - An empty condition evaluates to true by default.

6. Click **Save**.
7. Click **OK**.

View, modify, or delete a configuration item in Discovery Event Manager

Applies to User Roles:

System Administrator

As inventory changes within your organization, you will need to add, update, or delete configuration item (CI) types to keep your inventory records up-to-date for the Discovery Event Manager tool. You can manage the CI types in the CI record type table.

To view, modify, or delete a configuration item in Discovery Event Manager:

Warning: If you are deleting a CI record type, make sure you select the CI record type you want to delete. If you delete the wrong record type, you must add the record back into the CI Record ID table.

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **Search** to retrieve a list of CI ID types.
3. Select the ID type you want to view, and then click **Previous** or **Next** to scroll through the list of records.
4. Select the **Rules** tab to view the rules that are set for the selected CI type.
5. Select the record you want to change and make any necessary changes.
6. Select the ID type you want to delete, and then click **Delete**.

7. Click **Save**.
8. Click **OK**.

Customize changes in Discovery Event Manager

Applies to User Roles:

System Administrator

If your best practice is to have an incoming configuration item (CI) record that is not compliant with the managed state of that CI record in HP Service Manager go through the change management process, you can customize how you want the Discovery Event Manager tool to process those incoming CI records.

To customize the way changes are handled within Discovery Event Manager:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **Search** to retrieve a list of Configuration Item (CI) ID types.
3. Select the ID type for the customization you want to make, and then select the **Change Customization** tab.
4. Enter the customized script you want to override the default values set by the `discoveryEvent` ScriptLibrary record (the change record may be referenced as "change").
5. Click **Save**.
6. Click **OK**.

Customize incidents in Discovery Event Manager

Applies to User Roles:

System Administrator

If your best practice is to have an incident logged against an incoming configuration item (CI) record that is not compliant with the managed state of a CI record in HP Service Manager, you can customize the rules you set for automatically opening an incident record.

To customize the JavaScript for opening an incident record:

1. Click **Tailoring** > **Web Services** > **Discovered Event Manager Rules**. The Discovery Event Manager form opens.
2. Click **Search** to retrieve a list of Configuration Item (CI) ID types.
3. Select the ID type for the customization you want to make to incidents, and then select the **Incident Customization** tab.
4. Enter the customized script you have created to override the default values set by the discoveryEventScriptLibrary record (the incident record may be referenced as "incident").
5. Click **Save**.
6. Click **OK**.

HP Operations Orchestration (OO)

HP Operations Orchestration (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 OO flows communicate and document procedures, decreasing dependencies on individuals or groups. Refer to the HP Operations Orchestration (OO) documentation for more information.

When integrated with Service Manager, OO shares information between monitoring and automation systems and the help desk. Web client users have access to OO flows from Knowledge Management, where they can view, add, update, or delete OO flows. Incident Management processes are enhanced by linking Knowledge documents with OO flows, and automated deployment of changes can be implemented by linking OO flows to change records.

Note: Only one instance of this integration is allowed.

Prerequisites:

- System Administrators must add, configure, and enable an instance of this integration in Integration Manager (SMIS).
- Secure Sockets Layer (SSL) is required for communication between the servers.
- Optionally, you can use Lightweight Single Sign-On (LW-SSO) to bypass the log-in prompts.

Operations Orchestration integration setup

To set up the OO integration in your environment, you need to complete the following tasks:

- "Add an Operations Orchestration integration" on the next page

  This task adds and enables an OO integration in the Integration Manager (SMIS). It specifies all parameter values required to set up the integration.

- "Enable SSL connection from Service Manager to Operations Orchestration" on page 177

This task enables SSL connection between the Service Manager and OO servers. The Service Manager server acts as a trusted client connecting to the OO server. This task creates a root CA and self-signed certificate in the OO server and then imports them into Service Manager.

- "Enable LW-SSO for the Operations Orchestration integration" on page 185

  This task is optional but strongly recommended. Enabling LW-SSO for the integration allows Service Manager users to bypass the log-in prompts when viewing OO flow execution results from within Service Manager.

Add an Operations Orchestration integration

Applies to User Roles:

System Administrator

To use the Service Manager to OO integration, you must add and enable an instance of this integration in Integration Manager. Optionally, you can enable Lightweight Single Sign-On (LW-SSO) in OO and in Service Manager to bypass the log-in prompts.

To add and enable a Service Manager to OO integration instance:

1. Log on to the Service Manager Windows or Web client.
2. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
3. Click **Add**. The Integration Template Selection wizard opens.
4. Select **SMOO** from the Integration Template list. Ignore the **Import Mapping** check box, which has no effect on this integration.

   Note: Only one instance of this integration is allowed. If an instance of this integration already exists in Integration Manager, the **SMOO** template is unavailable. You have to delete the existing integration instance before you can add a new one.

5. Click **Next**. The Integration Instance Information page opens.

6. Complete the following fields as necessary.

Field	Value	Description
Name (required)	User-defined. Default: SMOO.	Name of the integration instance.
Version (required)	1.1	Version number of the integration.
Interval Time (s) (required)	User-defined. For example: 600.	Polling interval (in seconds) for Operations Orchestration flow synchronization.
Max Retry Times (required)	Enter 0 (zero) for this field.	Maximum allowed number of retries if the background scheduler fails to run. SMOO does not use this value.
SM Server	Enter a name that identifies your Service Manager server host. For example, sm_host1.	Display name for your Service Manager server host.
Endpoint Server	Enter a name that identifies your Operations Orchestration server host. For example, oo_host1.	Display name for your Operations Orchestration server host.
Log Level (required)	Select a level from the drop-down list. Default: INFO.	Level of diagnostic information that the Service Manager server logs to the log file directory. The possible log levels are: DEBUG, INFO (default), WARNING, ERROR, and OFF.
Log File Directory (required)	Specify a directory. For example: c: \smoologs.	This is a directory that exists on the Service Manager server host where log files of the Service Manager to OO integration are stored. The log files are generated in the following format: SMOO-<yyyy><mm><dd>.log (for example, SMOO-20100328.log) **Note:** If you specify a directory that does not exist, the log files will get lost; if you do not specify a directory, the Service Manager to OO integration will not work.
Run at	Selected/not	Automatically enable/disable the integration instance

Field	Value	Description
system startup	selected	when the Service Manager server is started.
Description	HP Operations Orchestration flows linked to Service Manager.	Description of the integration instance.

7. Click **Next**. The Integration Instance Parameters page opens.

8. Click the **General Parameters** and **Secure Parameters** tabs, and modify the parameter values as shown in the table below:

Parameter	Value	Example
oo.server.url	Server address of Operations Orchestration Central: `https://[servername]:[port]`. Note that [servername] should be the fully qualified domain name (FQDN) of the Operations Orchestration server host.	`https://oo.hp.com:8443` **Note:** If you are using OO 10.x, mark the **Enable Authentication** check box to ensure the integration API can pass the authentication.
oo.user.name	User name of the Operations Orchestration user account that the Service Manager server uses to access Operations Orchestration Central to synchronize and launch OO flows.	`admin`
oo.password	Password of oo.user.name.	`admin`
basepath.delimiter	Delimiter between multiple basepaths. The default delimiter is a semicolon (;).	;
basepath	basepath1;bathpath2;... The paths are separated by the basepath delimiter. Only the OO flows under the basepath and its sub-folders will be synchronized from OO.	/Library/ITIL/Change Management;/Library/ITIL/Incident Management
Accept-Language	REST Request Language Setting	en

Parameter	Value	Example
http.conn.timeout	Http Connection Timeout setting (seconds)	30
http.rec.timeout	Http Receive Timeout setting (seconds)	30
OOKM	Set to true/false to enable/disable the visibility of this integration instance in Knowledge Management (default: true).	`true` or `false`
OOCM	Set to true/false to enable/disable the visibility of the OO integration instance in Change Management (default: true).	`true` or `false`

9. Click **Next** twice and then click **Finish**. Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

   Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

10. Enable the integration instance.

11. Optionally:
    - Configure LW-SSO in Operations Orchestration.
    - Configure LW-SSO in Service Manager

Enable SSL connection from Service Manager to Operations Orchestration

Applies to User Roles:

System Administrator

The Service Manager to OO integration requires that Secure Sockets Layer (SSL) be enabled in the Operations Orchestration and Service Manager servers to ensure data security. Before using this integration, you must complete the following procedures:

1. Configure SSL in Operations Orchestration.
2. Configure SSL in Service Manager.

Note:

- The following procedures are provided as examples, assuming that you have not changed the security configurations of Operations Orchestration and Service Manager since they were installed. You may need to adjust the procedures depending on your specific security configurations in Operations Orchestration and Service Manager.
- To perform the following procedures, you must have OpenSSL installed on your Operations Orchestration Central host. In addition, you must have a Java platform installed on the Operations Orchestration and Service Manager hosts.
- In the following procedures, <OO_HOME> represents the Operations Orchestration home directory, and <SM_HOME> represents the Service Manager home directory.

Configure SSL in Operations Orchestration

To configure SSL in Operations Orchestration 9.x, perform the following tasks.

Task 1: Back up keystores in Operations Orchestration

Before you start configuring SSL in Operations Orchestration, make a backup copy of existing keystores (if any) in the following directories:

- <OO_HOME>\Central\conf
- <OO_HOME>\RAS\Java\Default\webapp\conf
- <OO_HOME>\Scheduler\conf
- <OO_HOME>\Studio\conf

Note: If your Operations Orchestration system does not contain any keystores in these folders, skip this task.

Task 2: Configure SSL in Operations Orchestration Central

You can use any pair of public/private certificates based on your specific certificate requirements, security policies, and so on. This section provides an example of using OpenSSL and the standard Java keytool to generate a self-signed certificate.

To configure SSL in Operations Orchestration Central:

1. Stop the RSCentral, RSScheduler and RSJRAS services.
2. Generate a private/public key pair for Root Certificate Authority.
   a. Change to the following directory: `<OO_HOME>\Central\conf`.
   b. Run the following command to create the private key:

      ```
      openssl genrsa -des3 -out <RSA_private_key_file> 2048
      ```

      For example: `openssl genrsa -des3 -out cakey.pem 2048`
   c. When prompted, enter a password phrase you want to use to protect your authority's private key file (`cakey.pem`). For example, **CAKeyPassword**.

      Note: Remember this password phrase. You will be asked to enter it again later when you use the Java keytool to generate a request (see step 3).
   d. Run the following command to create the public key:

      ```
      openssl req -new -key <RSA_private_key_file> -x509 -days 1095 -out
      mycacert.pem
      ```

      For example, `openssl req -new -key cakey.pem -x509 -days 1095 -out mycacert.pem`.
   e. Enter other required information that will be incorporated into your certificate request.

      Note: To create a unique `.pem` file, provide a unique Organization Name (for example, `org1`). When asked for a Common Name, enter the fully qualified domain name (FQDN) of the Operations Orchestration host.
3. Use the Java keytool to generate a request.
   a. Run the following command:

      ```
      keytool -genkey -alias sm -keyalg RSA -keystore rc_keystore -storepass
      <store password for rc_keystore> -keypass <key password for rc_keystore> -
      dname "CN=<OO_server_FQDN>, OU=<Organization Unit>, O=<Organization>,
      L=<Location>, ST=<State or Province>,C=<Country>"
      ```

For example: `keytool -genkey -alias sm -keyalg RSA -keystore rc_keystore -storepass bran507025 -keypass bran507025 -dname "CN=<hostname.domainname>, OU=MyOrganizationUnit, O=MyCompany, L=MyCity, ST=MyState,C=MyCountry"`

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

b. Run the following command:

```
keytool -certreq -keystore rc_keystore -alias sm -storepass <store password for rc_keystore> -file <CRS file>
```

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

c. Run the following command:

```
openssl x509 -req -days 1095 -in <CRS file> -CA mycacert.pem -CAkey <RSA_private_key_file> -CAcreateserial -out smcert.pem
```

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

d. When prompted, type the password phrase you entered in step 2 to protect your authority's private key file (`cakey.pem`). For example, **CAKeyPassword**.

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

a. Run the following command:

```
keytool -import -v -alias rootca -keystore rc_keystore -storepass <store password for rc_keystore> -file mycacert.pem
```

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

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

b. When you are prompted to confirm that this certificate should be trusted, type: `y`.

The command window prompts: "Certificate was added to keystore".

c. Run the following command:

```
keytool -import -v -alias sm -keystore rc_keystore -storepass <store
password for rc_keystore> -file smcert.pem
```

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

The command window prompts: "Certificate reply was installed in keystore".

Task 3: Configure SSL in Operations Orchestration RAS

1. Change to the following directory: `<OO_HOME>\RAS\Java\Default\webapp\conf\`.
2. Copy the generated root CA `mycacert.pem` and self-signed certificate `smcert.pem` from `<OO_HOME>\Central\conf` to the current directory.
3. Import the root CA `mycacert.pem` and self-signed certificate `smcert.pem` to `ras_keystore.jks`. See step 4 in *Configure SSL in Operations Orchestration Central*.

Task 4: Configure SSL in Operations Orchestration Scheduler

1. Change to the following directory: `<OO_HOME>\Scheduler\conf\`.
2. Copy the generated root CA `mycacert.pem` and self-signed certificate `smcert.pem` from `<OO_HOME>\Central\conf` to the current directory.
3. Import the root CA `mycacert.pem` and self-signed certificate `smcert.pem` to `rc_keystore`. See step 4 in *Configure SSL in Operations Orchestration Central*.

Task 5: Start the Operations Orchestration services

Start the RSCentral, RSScheduler and RSJRAS services.

Task 6: Configure SSL in Operations Orchestration Studio

1. Change to the following directory: <OO_HOME>\Studio\conf\.
2. Copy the generated root CA mycacert.pem and self-signed certificate smcert.pem from <OO_HOME>\Central\conf to the current directory.
3. Import the root CA mycacert.pem and self-signed certificate smcert.pem to rc_keystore. See step 4 in *Configure SSL in Operations Orchestration Central*.

To configure SSL in Operations Orchestration 10.x, perform the following tasks.

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 path/for/new/Keystore> -storepass changeit-storetype pkcs12 -dname "CN=*<CENTRAL_FQDN>*, OU=*<ORGANIZATION_UNIT>*, O=*<ORGANIZATION>*, L=*<LOCALITY>*, *C=<COUNTRY>*"

   Note: If you do not enter a path for generating the new keystore, it is created in the folder where you entered the command, for example *<installation dir>*/central/var/security.
5. Import the self-signed certificate to the Central key.store file, using the following command:

   keytool -v -importkeystore -srckeystore new/path/created/Keystore -srcstoretype PKCS12 -srcstorepass changeit -destkeystore .key.store -deststoretype JKS -deststorepass changeit
6. 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 Operations Orchestration Central service.

Configure SSL in Service Manager

Once you have successfully configured SSL in Operations Orchestration, you are ready to configure SSL in Service Manager.

To configure SSL for Service Manager to connect to OO 9.x, perform the following steps.

1. Create a trust store for Service Manager.

   a. Change to the following directory: `<SM_HOME>/Server/RUN`.

   b. Copy the generated `mycacert.pem` and `smcert.pem` from `<OO_HOME>\Central\conf` to `<SM_HOME>/Server/RUN`.

   c. Run the following command:

      ```
      keytool -import -v -alias rootca -keystore <keystore_file> -storepass <store password for keystore_file> -file mycacert.pem
      ```

      For example: `keytool -import -v -alias rootca -keystore smtrust -storepass smoointabc123 -file mycacert.pem`

      The command window displays the certificate information.

   d. When the command window prompts: "Trust this certificate?", type `y`.

      The command window prompts: "Certificate was added to keystore".

   e. Run the following command:

      ```
      keytool -import -v -alias sm -keystore <keystore_file> -storepass <store password for keystore_file> -file smcert.pem
      ```

      For example: `keytool -import -v -alias sm -keystore smtrust -storepass smoointabc123 -file smcert.pem`

> **Note:** In this example, the trust store file name is **smtrust**, and its store password is **smoointabc123**. You will add this information to sm.ini in the next step.

2. Add the following lines to sm.ini:

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

For example:

```
#
# Certificates
#
truststoreFile:smtrust
truststorePass:smoointabc123
```

3. Restart the Service Manager server so that your configuration takes effect.

To configure SSL for Service Manager to connect to OO 10.x, perform the following steps.

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 OO.

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

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

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

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

```
# Certificates
truststoreFile:smtrust
truststorePass:smoointabc123
```

9. Start the Service Manager Server service.

Enable LW-SSO for the Operations Orchestration integration

Applies to User Roles:

System Administrator

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

To enable LW-SSO for the OO integration, complete the following tasks:

- "Configure LW-SSO in the Service Manager Web tier" on page 94
- "Configure LW-SSO in Operations Orchestration (OO)" on page 101

Manage OO flows from Knowledge Management

User roles: Users with the "SysAdmin" or "programmer" capability word

You can view, create, update, and delete Operations Orchestration (OO) flows from the **Operations Orchestration Flows** menu in Knowledge Management.

Note: To manage OO flows, you must first set up and enable an OO integration instance in Integration Manager (SMIS).

To manage Operations Orchestration flow records in Service Manager:

1. Log on to the Service Manager web client.
2. Click **Knowledge Management** > **Configuration** > **Operations Orchestration Flows**.

   The HP Operations Orchestration Flow window opens.
3. Click **Search**.

   If a Service Manager to OO integration instance is correctly configured and enabled in Integration Manager (SMIS), a list of OO flow records is displayed.

   > **Note:** The list of OO flow records is populated from the **OOFlow** table under **System Definition**. These OO flow records are either synchronized from Operations Orchestration (according to the basepath specified in the Service Manager to OO integration instance) or manually added in Service Manager (for example, an individual OO flow that is not under the basepath or its sub-folders).

   You can also type a full or partial display name in the Display Name field, and click **Search** to view one or more specific OO flow records.
4. Select a record from the list to view its details.

   The details of the selected OO flow are displayed. For the description of each field on the OO flow detail form, see "Operations Orchestration flow detail form fields" on page 188.
5. To add a new OO flow:
   a. Click **New**.
   b. Complete the fields of the OO flow record.

      > **Note:** You can only add an OO flow that has a unique UUID.

   c. Click **OK**.
6. To update an existing OO flow:
   a. Select the OO flow.
   b. Update the details.
   c. Click **Save & Exit**.

Note: If the OO flow is updated in Operations Orchestration after you update it in Service Manager, your updates will be discarded at the next synchronization.

7. To delete an OO flow:
   a. Select the OO flow.
   b. Click **Delete**.
   c. Click **Yes** to confirm the deletion.

Operations Orchestration flow synchronization rules

The SM to OO integration synchronizes flows from Operations Orchestration (OO) to Service Manager according to the basepaths that are configured in Integration Manager (Service Manager Integration Suite). The following describes the synchronization rules, using an example **basepath** value: **/Library/ITIL/Change Management; /Library/How Do I flows**.

Rule 1: Only the Operations Orchestration flows under the basepath or its sub-folders are synchronized.

Operations Orchestration Flow Path	Synchronize?
/Library/ITIL/Change Management/Network/Compare Device ACLs	Yes
/Library/ITIL/Change Management/Servers/Block NAS Task	Yes
/Library/How Do I flows/How do I: Iterate through a list	Yes
/Library/ITIL/Incident Management/Servers/Server Health Check	No

Rule 2: If an Operations Orchestration flow is removed in Operations Orchestration, it will also be removed in Service Manager when it is under the basepath or its sub-folders.

Operations Orchestration Flow Path Deleted in Operations Orchestration	Remove in Service Manager?
/Library/ITIL/Change Management/Network/Compare Device ACLs	Yes
/Library/ITIL/Change Management/Servers/Block NAS Task	Yes
/Library/How Do I flows/How do I: Iterate through a list	Yes
/Library/ITIL/Incident Management/Servers/Server Health Check	No

Rule 3: If an Operations Orchestration flow is updated in Operations Orchestration, it will also be updated in Service Manager when it is under the basepath or its sub-folders.

Operations Orchestration Flow Path Updated in Operations Orchestration	Update in Service Manager?
/Library/ITIL/Change Management/Network/Compare Device ACLs	Yes
/Library/ITIL/Change Management/Servers/Block NAS Task	Yes
/Library/How Do I flows/How do I: Iterate through a list	Yes
/Library/ITIL/Incident Management/Servers/Server Health Check	No

Note: If an Operations Orchestration flow (under the basepath or its sub-folders) is updated in Service Manager, the updates will not be discarded until the Operations Orchestration flow is updated in Operations Orchestration.

Operations Orchestration flow detail form fields

You can view the details of an Operations Orchestration (OO) flow from **Knowledge Management** > **Configuration** > **Operations Orchestration Flows**. The following table lists the fields contained in the OO flow detail form.

Note: In the table below, an OO field refers to a field from Operations Orchestration, and the integration instance synchronizes its value from Operations Orchestration; a custom field is only for Service Manager (has no corresponding field in Operations Orchestration), and will be used when launching the OO flow.

Field	Value	Comments
UUID	A universally unique identifier automatically assigned to the OO flow when it was created in OO.	An OO field.
Path	Full path of the OO flow. Consists of the path and name of the OO flow. For example: /Library/ITIL/Change Management/Network/Compare Device ACLs.	An OO field.
Display Name	User-defined name of the OO flow in Service Manager.	A custom field. When the OO flow is synchronized from OO, this field displays the name of the OO flow. However, you can change the name

Field	Value	Comments
		as you like.
Parameter Name	Name of an input for the operation(s) of the OO flow. Can be entered by the person running the flow; or set to a specific value; or obtained from information gathered by another step of the OO flow.	An OO field.
Required?	**true** or **false**	An OO field. Indicates whether the parameter is required or not.
Secure?	**true** or **false**	Indicates whether the field is a security field or not. The value of a security field will display as a string of asterisks.
Description	Full description of the OO flow, including the steps/operations, inputs, responses, and returns of the OO flow.	An OO field.

Add OO flow links to a knowledge document

User roles: Only users that have the permissions to update a knowledge document can add Operations Orchestration (OO) flow links to it.

Note: Before you perform the following steps, make sure that a Service Manager to OO integration (SMOO) instance is enabled in Integration Manager (SMIS).

To add OO flow links to a new knowledge document:

1. Log on to the Service Manager web client.
2. Click **Knowledge Management** > **Contribute Knowledge**.
3. Select a document type. The Contribute Knowledge window opens.
4. Select the **OO Flow Links** tab.
5. In the **Select Path** field, select a path, and click **Add Link**.

   The OO Flow Link Detail form is displayed.

6. In the Parameters section, complete the fields in the following table as necessary.

Note:
- In the table below, an OO field refers to a field from Operations Orchestration, and the integration instance synchronizes its value from Operations Orchestration; a custom field is only for Service Manager (has no corresponding field in Operations Orchestration), and will be used when launching the OO flow.
- In some cases, you may need to add additional parameter names and values that are required to launch the OO flow.

Field	Value	Description
Parameter Name	Name of an input for the operation(s) of the OO flow. Can be entered by the person running the flow; or set to a specific value; or obtained from information gathered by another step of the OO flow.	An OO field.
Required?	**true** or **false**	An OO field. Indicates whether the parameter is required or not.
Mapped CI Field	Select one from the drop-down list.	A custom field. Useful CI fields to launch the OO flow. The CI field value will be populated when launching the OO flow. The CI fields listed are defined in global list "OO Fields".
Default Value	Default value of the parameter.	A custom field. If there is no Mapped CI Field configured for the parameter, or no value in the Mapped CI Field, the default value will be populated when launching the OO flow. **Note:** This field is not the same field in OO.

7. Click **Add**. A message displays, stating the OO flow link is added.
8. Click **OK**. The OO flow appears in the Links table, and the OO Flow UUID displays as a link.
9. (Optional) If you want to update the OO flow, do the following:
   a. Click the UUID link.
   b. Update the parameters.

c. Click **OK**.
Note: If you do not click **OK** to save and exit, your updates to the Mapped CI Field and Default Value fields might be lost.

10. Repeat the steps above to add more OO flow links to the knowledge document.

To add OO flow links to an existing knowledge document:

Note: You can only add OO flow links to published documents and draft documents (not to retired documents).

1. Log on to the Service Manager web client.
2. Click **Knowledge Management** > **Published Documents** or **Draft Documents**.
3. Search for and open a published document, or directly select a draft document from the list.
4. Click **Edit**. The Contribute Knowledge window opens.
5. Select the **OO Flow Links** tab.
6. Add OO flow links to the knowledge document, by following steps 3 to 9 described above for a new knowledge document.

Remove OO flow links from a knowledge document

User roles: Only users that have the permissions to update a knowledge document can remove Operations Orchestration (OO) flow links from the knowledge document.

Note: Before you perform the following steps, make sure that a Service Manager to OO integration instance is enabled in Integration Manager (SMIS).

To remove OO flow links from a knowledge document:

1. Log on to the Service Manager Web client.
2. Click **Knowledge Management** > **Published Documents** or **Draft Documents**.
3. Search for and open a published document, or directly select a draft document from a list of draft documents.

4. Click **Edit**. The Contribute Knowledge window opens.
5. Select the **OO Flow Links** tab.
6. Select an OO flow link from the OO Flow Path table, and click **Remove Link**.

   The OO flow link is removed from the OO Flow Path table. At the same time, a message displays, stating that the OO flow is no longer linked to the knowledge document.
7. Repeat step 5 to remove more OO flow links from the knowledge document.

Automated resolution of incidents

When integrated with Service Manager, OO shares information between monitoring and automation systems and the help desk. Incident Management processes are enhanced by linking Knowledge documents with OO flows, allowing technicians to triage, diagnose, and resolve incidents more quickly and efficiently.

Web client users can add or remove OO flows links for a knowledge document, execute flows from related knowledge documents for an incident; and view OO flow execution results attached to an incident as historic activities.

Launch OO flows from an incident

When searching knowledge from an incident, you can launch Operations Orchestration (OO) flows linked to a knowledge document. Only users who have the permissions to edit a knowledge document can launch the OO flows linked to it.

Note: This feature is available only when a Service Manager to OO integration instance is enabled in Integration Manager (SMIS) and the Search Engine is installed.

To launch OO flows from an incident:

1. Log on to the Service Manager Web client.
2. From **Incident Management**, search for an incident record and open the record.
3. Click **More** and then select **Search Knowledge**.

4. Search for knowledge documents as follows:

   a. Click **Advanced**.

   b. Clear all the knowledgebase selections, and then select **Knowledge Library**.

   c. Click **Search**. A list of KM documents opens.

5. Select the knowledge document from which you want to launch one or more associated OO flows. The knowledge document opens.

6. Click **Execute OO Flow**.

   - If there is no OO flow linked to the document, an error message is displayed: "No related OO flows found."
     You can select to click **Edit** to add OO flow links to the document, and then click **Execute OO Flow** again. You can also select to close the document window to exit.
   - If there is only one OO flow linked to the document, the **Set Parameters** page opens.
   - If there are multiple OO flows linked to the document, the **Select an OO Flow** page opens. Select an OO flow from the list. The **Set Parameters** page opens.

   Note:
   - If the selected OO flow has a parameter with a Mapped CI Field (for example, **Ip Address**) and the Affected CI of the incident has a corresponding value (for example, an IP address) for this Mapped CI Field, this affected CI field value from the incident will be automatically populated as the value of this OO flow parameter. If the mapped CI field is an array type field, the first value of the array will be populated.
   - If the selected OO flow has a parameter without a Mapped CI Field, the value specified in the Default Value field of this parameter will be populated.

7. Provide all the required parameter values for the selected OO flow.

   Note: You may need to add additional parameter names and provide their values in some cases.

8. (Optional) If you want the OO flow to be executed asynchronously, select **Asynchronous**.

9. Click **Next**. The selected OO flow is launched, and you are returned to the Select an OO Flow page.

   Note: If you do not want to launch more OO flows, click **Finish** instead of **Next** to launch the selected OO flow and to return to the knowledge document detail page.

10. Continue to launch more OO flows from the list on the Select an OO Flow page.
11. Click **Finish**.

    Once an OO flow execution is complete, a dialog box opens, stating that the execution is done and asking if you want to view the execution result.

    - Click **Yes** to view the execution result in Operations Orchestration.

      If LW-SSO is configured in both the Service Manager web client and Operations Orchestration, you are directed to the execution result in Operations Orchestration. If LW-SSO is not configured, an Operations Orchestration login page opens; after you log on to Operations Orchestration, the execution result is displayed.

    - Click **No** to exit the dialog box.

View OO flow execution results from an incident

After launching an Operations Orchestration (OO) flow from a knowledge document through searching knowledge from an incident, you can view the OO flow execution result from the list of Historic Activities of the incident.

To view an OO flow execution result from an incident:

1. Log on to the Service Manager Web client.
2. From **Incident Management**, search for an incident record and open it.
3. In the **Activities** section, select an activity of the **OO Response** type from the activities list.

   The Activity Log - Incident Management page opens, displaying the execution details of an OO flow launched from this incident.

4. Click **Open Report**.

If Lightweight Single Sign-On (LW-SSO) is configured in both the Service Manager web client and Operations Orchestration, you are directed to the execution result in Operations Orchestration. If LW-SSO is not configured, an Operations Orchestration login page opens, and the execution result displays after you log in.

Automated deployment of changes

HP Service Manager 9.30 or later provides an enhanced integration with Operations Orchestration (OO) that allows users to link requests for change (RFCs) to OO flows. This enables users to implement automated deployment of changes by manually or automatically launching OO flows.

Before a change moves to the Change Approval phase, you can link OO flows to the change so that each of the change deployment steps is performed and the results are returned. These OO flows originated from out-of-box content in OO intended to support common Change use cases, such as Database Script Execution, Service/Server Restart, and Running Batch Files.

To run the automated flow, select the relevant OO flows and complete all required parameters of the flows. These parameters can be either fixed or references to attributes of the RFC or Configuration Items (CIs) in the RFC. You also need to select when and how the change flows will be triggered - upon change approval, based on a schedule or manually. When the change is approved and moves to the Change Implementation phase (or the Test and Build phase if the change has a category of Release Management), you can manually launch the OO flows from within Service Manager, or the OO flows are automatically executed based on the trigger conditions you set.

Note: This feature is not supported for the following change categories:

- KM document
- CI Group
- Subscription
- Unplanned Change

Add OO flow links to a new change record

User roles: Change Manager, Change Coordinator, and Release Manager

To add OO flow links to a *new* change record:

1. Log on to the Service Manager Web client.
2. Click **Change Management** > **Changes** > **Create New Change**.
3. Select a change category other than any of the following:
   - KM document
   - CI Group
   - Subscription
   - Unplanned Change

   Note: Do not select any of these categories, because the OO Flow Links feature is not available for a change record with these change categories.
4. Complete the form with all required and optional information.
5. Go to the OO Flow Links section, select a path in the Select Path field, and click **Add Link**. The OO Flow Link Detail form is displayed.
6. In the **Sequence No** field, type a number. This number defines the order in which the OO flow is automatically launched. Each OO flow link must have a unique Sequence No.
7. In the **Target CIs** field, enter the target Configuration Items that will be used when the OO flow is launched.

   Note: If you are planning to launch the flow manually, you can skip this step.
8. In the Parameters section, complete the fields listed in the following table as necessary.

Field	Value	Description
Parameter Name	Name of an input for the operation(s) of the OO flow; can be entered by the user running the flow, or set to a specific value, or obtained from information gathered by another step of the OO flow	An OO field

Field	Value	Description
Required?	`true` or `false`	An OO field that indicates whether the parameter is required or not
Mapped Change Field	Select one from the drop-down list.	A custom field This is a field from the change record used to launch the OO flow. The Change field value is populated when the OO flow is launched. The Change fields listed are defined in the "OO RFC Fields" global list.
Mapped CI Field	Select one from the drop-down list.	A custom field Useful CI field to launch the OO flow. If there is no Mapped Change Field configured for the parameter, or there is no Mapped Change Field value, the CI field value will be populated when launching the OO flow. The CI fields listed are defined in "OO Fields" global list.
Default Value	Default value of the parameter	A custom field If neither Mapped Change Field nor Mapped CI Field is configured for the parameter, or if no value is available in Mapped Change Field or Mapped CI Field, the default value is used when the OO flow is launched. **NOTE:** This field is not the same field in OO.

9. Click **Add**. The OO flow link is added.
10. Click **OK**. You are returned to the Change form.

> **Note:** If you do not click **OK** to save and exit, your updates to the Mapped CI Field and Default Value fields might be lost.

11. Repeat the steps above to add more links as necessary.
12. Click **Save** to save the change record.

Add OO flow links to an existing change record

User roles: Change Manager, Change Coordinator, and Release Manager

Note: You can add OO flow links to an existing change record that meets the following conditions:

Category	Change Phase
Release Management	One of the following: • Assess • Plan and Design
None of the following: • KM document • CI Group • Subscription • Unplanned Change • Release Management	One of the following: • Change Logging • Change Review • Change Assessment & Planning • Prepare for Change Approval

To add OO flow links to an *existing*change record:

1. Log on to the Service Manager Web client.
2. Open an existing change record that meets the conditions previously mentioned.
3. Go to the OO Flow Links section, select a path in the Select Path field, and click **Add Link**. The OO Flow Link Detail form is displayed.
4. In the **Sequence No** field, type a number. This number defines the order in which the OO flow is automatically launched. Each OO flow link must have a unique Sequence No.
5. In the **Target CIs** field, enter the target Configuration Items that will be used when the OO flow is launched.

   Note: If you are planning to launch the flow manually, you can skip this step.

6. In the Parameters section, complete the fields listed in the following table as necessary.

Field	Value	Description
Parameter	Name of an input for the	An OO field

Field	Value	Description
Name	operation(s) of the OO flow; can be entered by the user running the flow, or set to a specific value, or obtained from information gathered by another step of the OO flow	
Required?	`true` or `false`	An OO field that indicates whether the parameter is required or not
Mapped Change Field	Select one from the drop-down list.	A custom field This is a field from the change record used to launch the OO flow. The Change field value is populated when the OO flow is launched. The Change fields listed are defined in the "OO RFC Fields" global list.
Mapped CI Field	Select one from the drop-down list.	A custom field Useful CI field to launch the OO flow. If there is no Mapped Change Field configured for the parameter, or there is no Mapped Change Field value, the CI field value will be populated when launching the OO flow. The CI fields listed are defined in "OO Fields" global list.
Default Value	Default value of the parameter	A custom field If neither Mapped Change Field nor Mapped CI Field is configured for the parameter, or if no value is available in Mapped Change Field or Mapped CI Field, the default value is used when the OO flow is launched. **Note:** This field is not the same field in OO.

7. Click **Add**. The OO flow link is added.

8. Click **OK**. You are returned to the Change form.

Note: If you do not click **OK** to save and exit, your updates to the Mapped CI Field and Default

Value fields might be lost.

9. Repeat the steps above to add more links as necessary.
10. Click **Save** to save the change record.

Update OO flow links in a change record

User roles: Change Manager, Change Coordinator, and Release Manager

Note: You can update OO flow links only in a change record that meets the following conditions:

Category	Change Phase
Release Management	One of the following: • Assess • Plan and Design
None of the following: • KM document • CI Group • Subscription • Unplanned Change • Release Management	One of the following: • Change Logging • Change Review • Change Assessment & Planning • Prepare for Change Approval

To update OO flow links in a change record:

1. Log on to the Service Manager Web client.
2. Open an existing change record that meets the conditions previously mentioned.
3. In the OO Flow Links section, click the **Seq No** of an OO flow link that you want to update. The OO Flow Link Detail form opens.
4. Update the fields as necessary, and then click **Save**.

5. Click **Cancel**. You are returned to the Change form.
6. Click **Save** to save the change record.

Remove OO flow links from a change record

User roles: Change Manager, Change Coordinator, and Release Manager

Note: You can remove OO flow links only from a change record that meets the following conditions:

Category	Change Phase
Release Management	One of the following: • Assess • Plan and Design
None of the following: • KM document • CI Group • Subscription • Unplanned Change • Release Management	One of the following: • Change Logging • Change Review • Change Assessment & Planning • Prepare for Change Approval

To remove OO flow links from a change record

1. Log on to the Service Manager Web client.
2. Open an existing change record that meets the above conditions.
3. In the OO Flow Links section, click the **Seq No** of an OO flow link that you want to remove. The OO Flow Link Detail form is displayed.
4. Click **Delete**, and then click **YES** to confirm the deletion.

   You are returned to the Change form, in which the OO flow link is removed.
5. Click **Save** to save the change record.

Manually launch change flows

User roles: Change Manager, Change Coordinator, and Release Manager

Once a change record is approved and advances to the Change Implementation (or Build and Test) phase, you can select to manually launch the OO flows linked to the change record.

Note: You can perform this task only on a change record that meets the following conditions. You can always perform this task regardless of the Automation Type of the change.

Category	Change Phase
Release Management	Build and Test
None of the following: • KM document • CI Group • Subscription • Unplanned Change • Release Management	Change Implementation

To manually launch OO flows from a change record:

1. Log on to the Service Manager Web client.
2. Open an existing change record that meets the conditions previously mentioned.
3. Click **More**, and then select **Execute OO Flow**.
    - If there is no OO flow linked to the change, an error message appears: "No related OO flows found."
    - If there is only one OO flow linked to the change, the Select Affected CI for OO Flow page opens.
    - If there are multiple OO flows linked to the change, the Select an OO Flow page opens. Select an OO flow from the table. The Select affected CI for OO flow page opens.
4. Select an affected CI from the table or click **Skip** to go to the next page if there are no CIs related

to this OO flow. The Set Parameters page opens.

- If the selected OO flow has a parameter with a Mapped Change Field (for example, Impact) and the change has a corresponding value for this Mapped Change Field, this Impact field value from the change will be automatically populated as the value of this OO flow parameter. If the Mapped Change Field is an array type field, the values of the array will be combined and separated by commas (,).
- If the selected OO flow has a parameter with a Mapped CI Field (for example, Ip Address) and the Affected CI of the change has a corresponding value (for example, an IP address) for this Mapped CI Field, this affected CI field value from the change will be automatically populated as the value of this OO flow parameter. If the mapped CI field is an array type field, the values of the array will be combined and separated by commas (,).
- If the selected OO flow has a parameter without a Mapped Change Field or Mapped CI Field, the value specified in its Default Value field will be populated.

5. Provide all the required parameter values for the selected OO flow.

   Note: In some cases, you may need to add additional parameter names and specify their values.

6. (Optional) If you want the OO flow to be executed asynchronously, select **Asynchronous**.
7. Click **Next**. The selected OO flow is launched, and you are returned to the Select an OO Flow page when the change is linked to more than one OO flow.

   Note: If you do not want to launch more OO flows, click **Finish** instead of **Next** to launch the selected OO flow and return to the change form.

8. Continue to launch more OO flows from the list on the Select an OO Flow page.
9. Click **Finish**.
10. Once an OO flow execution is complete, a dialog box opens, stating that the execution is done and asking if you want to view the execution result.

- Click **Yes** to view the execution result in Operations Orchestration.

  If LW-SSO is configured in both the Service Manager Web client and Operations Orchestration, the execution result in Operations Orchestration is displayed without any login prompt. If LW-SSO is not configured, an Operations Orchestration log-in page opens; after you log on to Operations Orchestration, the execution result is displayed.

- Click **No** to close the dialog box.

Automatically launch change flows upon approval

User roles: Change Manager, Change Coordinator, and Release Manager

You can set a change record so that the linked OO flows are executed automatically once it is approved and moved to the Change Implementation phase (or the Build and Test phase if it is a Release Management change).

1. Log on to the Service Manager Web client.
2. Open a change in the Change Assessment & Planning phase (or in the Assess or the Plan and Design phase if the change has a category of Release Management).
3. In the OO Flow Links section, select **When approved** as the Automation Type.
4. Click **Save** to save the change record.
5. Once the change has been approved, click **Close Phase** to move the change to the Change Implementation (or Build and Test) phase.

   A scheduler of OO Flow Automation is created and starts in 50 seconds, and the alert stage is **SMOO Auto-Approval**.

   The OO flows are automatically executed, and all the execution reports are saved in one activity log with an operator of **smoo-automation**.

Automatically launch change flows on a schedule (for a new change)

User roles: Change Manager, Change Coordinator, and Release Manager

You can select to trigger automatic execution of change flows at a scheduled time: either a specific date and time, or a future time based on a field value of a change, such as Planned Start, Planned End, and Requested End Date. Once the change is approved and advances to the Change Implementation phase (or Test and Build phase if it is a Release Management change), the OO flows linked to this change record will be automatically launched at the scheduled time.

To set an automatic execution time for OO flows of a new change:

1. Log on to the Service Manager Web client.
2. From Change Management, click **Create New Change**.
3. Select a change category other than any of the following:
   - KM document
   - CI Group
   - Subscription
   - Unplanned Change

   Note: The OO Flow Links feature is not available for a change record with any of these change categories.
4. Complete the form with all required and optional information.
5. In the OO Flow Links section, do either of the following:
   - Select **Use a fixed date** as the Automation Type. The **Scheduled Time** field is displayed. Select a date and specify a time, such as 06/04/10 10:00:00.

     Note: The date/time format is determined by your profile date/time format.
   - Select **Use a field in the record + interval** as the Automation Type. The **Change Field** and **Interval** fields are displayed. Select a field in the Change Field list as the base time, and then enter a value in the Interval field using the “+/-ddd hh:mm:ss” format. Note that a space is required between ddd and hh, and you can omit the plus sign (+) for positive intervals.

     For example, if you select **Requested End Date** in Change Field and enter **-1 02:30:10** in Interval, the OO flows of the change will be automatically launched one day, two hours, thirty minutes, and ten seconds before the Requested End Date.

Note:

- The automation execution time should be a future time between the Planned Start and Planned End.
- The automation execution time you selected is not validated now. Instead, the time will be validated when the change moves to the Change Implementation (or Test and Build) phase. If the validation fails, you will receive a warning and the change cannot advance to implementation. In this case, you have to reset the execution time. To do so, click **Cancel** and move the change back to a phase prior to Change Approval (or back to "Assess" or "Plan and Design"), reset the automation execution time, and then go through the change phases again.

Automatically launch change flows on a schedule (for an existing change)

User roles: Change Manager, Change Coordinator, and Release Manager

Note: You can set an automation execution time for the OO flows linked to an existing change record that meets the following conditions.

Category	**Change Phase**
Release Management	One of the following: • Assess • Plan and Design
None of the following: • KM document • CI Group • Subscription • Unplanned Change • Release Management	One of the following: • Change Logging • Change Review • Change Assessment & Planning • Prepare for Change Approval

To set an automatic execution time for OO flows of an existing change:

1. Log on to the Service Manager Web client.
2. Open an existing change record that meets the conditions previously mentioned.
3. In the OO Flow Links section, do either of the following:
   - Select **Use a fixed date** as the Automation Type. The **Scheduled Time** field is displayed. Select a date and specify a time, such as 06/04/10 10:00:00.

     Note: The date/time format is determined by your profile date/time format.

   - Select **Use a field in the record + interval** as the Automation Type. The **Change Field** and **Interval** fields are displayed. Select a field in the Change Field list as the base time, and then enter a value in the Interval field using the "+/-ddd hh:mm:ss" format. Note that a space is required between ddd and hh, and you can omit the plus sign (+) for positive intervals.

     For example, if you select **Requested End Date** in Change Field and enter **-1 02:30:10** in Interval, the OO flows of the change will be automatically launched one day, two hours, thirty minutes, and ten seconds before the Requested End Date.

Note:
- The automation execution time should be a future time between the Planned Start and Planned End.
- The automation execution time you selected is not validated now. Instead, the time will be validated when the change moves to the Change Implementation (or Test and Build) phase. If the validation fails, you will receive a warning and the change cannot advance to implementation. In this case, you have to reset the execution time. To do so, click **Cancel** and move the change back to a phase prior to Change Approval (or back to "Assess" or "Plan and Design"), reset the automation execution time, and then go through the change phases again.

View execution results of change flows

User roles: Change Manager, Change Coordinator, and Release Manager

OO flow execution results are saved in Service Manager in different ways depending on how they are executed: manually or automatically.

To view OO flow execution results from a change record:

1. Log on to the Service Manager Web client.
2. From Change Management, search for a change record and open it.
3. In the Activities section, do one of the following:
   - Select an activity of the **OO Response** type from the activities list. The Activity Log - Change Management page opens, displaying the execution details of an OO flow manually launched from this change.
   - Select an activity that has a type of **OO Response** and an operator of **smoo-automation**. The execution results of all the OO flows automatically executed are saved in this log as separate links.
4. Click **Open Report**.

   Note: For automatically executed OO flows, clicking **Open Report** opens only the report link of the first OO flow. You can view the reports of the other OO flows directly in OO.

   If Lightweight Single Sign-On (LW-SSO) is configured in both the Service Manager Web client and Operations Orchestration, the execution result in Operations Orchestration is displayed without any login prompt. If LW-SSO is not configured, an Operations Orchestration log-in page opens, and the execution result is displayed after you log in.

HP Business Service Management (BSM)

HP Business Service Management (BSM) is an end-to-end management solution portfolio that integrates network, server, application, and business transaction monitoring to help improve IT operations efficiency while delivering high-quality services. BSM Operations Manager i (OMi) optimizes event management, identifying cause/symptom relationships between events, and reduces operational expenditures. Refer to the HP Business Service Management (BSM) documentation for more information.

Incident Exchange (OMi - SM) integration

The Incident Exchange (OMi - SM) integration is a bidirectional integration between incident records in HP Service Manager and events in HP Business Service Management (BSM) Operations Management provided by the Operations Manager i (OMi) license.

This integration requires configurations on both product sides. For details, see "Incident Exchange (OMi - SM) integration setup" on the next page.

Note: As of version 9.34, Service Manager can integrate with multiple BSM OMi servers. For details, see "Add an integration instance for each Operations Manager i (OMi) server" on page 218.

Service Manager can accept RESTful-based requests from OMi to create incidents in Service Manager, based on events information in OMi. When Service Manager accepts an incident creation request from a remote OMi server, it creates an incident record and automatically assigns it to an existing group based on certain field values. Incident Management users can view the details of the related OMi event by clicking the **View OMi Event** menu option from the incident record. See "View related OMi event details from an incident" on page 230.

When an Incident Management user makes any changes to the incident record, Service Manager automatically synchronizes the changes to the corresponding event in OMi, by sending an update request to the OMi RESTful web service interface. In the event of a synchronization failure, a queuing mechanism will re-synchronize the changes. See "Synchronization of incident changes back to Operations Manager i (OMi)" on page 229.

System administrators can configure global settings that determine whether and when incident records opened from OMi events can be automatically closed. However, Incident Management users can mark individual OMi incident records as eligible or ineligible for automatic closure. See "Configure automatic closure for OMi incidents" on page 225 and "Mark an incident for automatic closure" on page 230.

Incident Exchange (OMi - SM) integration setup

The Incident Exchange (OMi - SM) integration requires the following configuration tasks be completed on the HP Service Manager and Business Service Management (BSM) systems.

1. "Create user accounts for the Incident Exchange (OMi - SM) integration" on the next page.

   This task creates a user account on each product side for the two systems to connect to each other and to synchronize data.

2. "Configure an event forwarding rule in Operations Manager i (OMi) " on page 215.

   This task configures a rule for the OMi server to forward events to the Service Manager server.

3. "Configure the Service Manager server as a connected server in Operations Manager i (OMi)" on page 212.

   Perform this task in BSM OMi. If you need to integrate Service Manager with more than one OMi server, perform this task on each of the OMi servers.

4. "Enable incident drill-down from Operations Manager i (OMi) Event Browser" on page 216.

   This task configures the Service Manager web tier in the **sm:ServiceManagerAdapter** script in OMi.

5. "Configure SSL for the Incident Exchange (OMi - SM) integration " on page 217.

   This task is needed if your OMi server requires HTTPS connections. If SSL is not configured in this case, changes on incidents that are created from OMi will not be able to be synchronized back to OMi.

6. "Configure the Instance Count in the SMOMi integration template" on page 217.

   This task is needed only when you have more than one OMi server. The Instance Count setting defines the allowed number of SMOMi integration instances in Service Manager (default: 1).

7. "Add an integration instance for each Operations Manager i (OMi) server" on page 218.

This task creates and enables an instance of this integration in Integration Manager (SMIS). A separate integration instance is required for each OMi server.

8. "Enable LW-SSO for the Incident Exchange (OMi - SM) integration" on page 224.

   Lightweight Single Sign-On (LW-SSO is) optional but recommended for the Incident Exchange (OMi - SM) integration. This task includes enabling LW-SSO in the Service Manager server and Web tier, as well as in BSM.

9. (Optional) "Configure automatic closure for OMi incidents" on page 225.

   This task is optional. By default, automatic closure is disabled for OMi incidents. System administrators can enable automatic closure and further configure under what conditions OMi incidents can be automatically closed.

10. (Optional) "Change the default assignment group for OMi incidents" on page 228.

    This task is optional. When created, OMi incidents are automatically assigned with an assignment group based on their certain field values and a predefined default assignment group. System Administrators can change the default assignment group setting (**Application**).

Create user accounts for the Incident Exchange (OMi - SM) integration

Applies to User Roles:

System Administrator

The Incident Exchange (OMi - SM) integration is bidirectional. Synchronizing events and incidents between the HP Service Manager and BSM OMi systems requires integration accounts be set up for the two systems to access each other.

1. Create an operator record with system administration privileges in Service Manager. For details, see Creating operator records.

   This is the user account that the OMi server uses to access Service Manager and to forward events to Service Manager.

   Later, when configuring the Service Manager server as a connected server in OMi, you need to specify this operator's the login name and password on the **Outgoing Connection** tab. See

"Configure the Service Manager server as a connected server in Operations Manager i (OMi)" on the next page.

2. Create a user account with system administration privileges on each BSM OMi server. For details, see the BSM online help.

   This is the user account that Service Manager uses to access the OMi server and to synchronize incident changes back to the OMi server.

   Later, when configuring the Service Manager server as a connected server in OMi, you must specify this user's login name as the **Name** of the Service Manager server on the **General** tab, and specify this user's password as the **Password** on the **Incoming Connection** tab. See "Configure the Service Manager server as a connected server in Operations Manager i (OMi)" below.

   Also, you need to specify the same user account when adding an SMOMi integration instance for each OMi server (the **username** and **Password** parameters). See "Add an integration instance for each Operations Manager i (OMi) server" on page 218.

Configure the Service Manager server as a connected server in Operations Manager i (OMi)

Synchronizing changes between HP Business Service Management (BSM) Operations Management events and HP Service Manager incidents requires configuring a Connected Server within OMi to correctly identify the target Service Manager server instance.

To configure the Service Manager server as a target connected server, perform the following steps:

1. Log on to HP Business Service Management as a system administrator.
2. Navigate to the Connected Servers manager in the Operations Management user interface:

   Admin > **Operations Management** > **Setup** > **Connected Servers**

3. Click the **New** button to open the **Create New Server Connection** dialog box.
4. In the **Display Name** field, enter a name for the Service Manager server.

   The **Name** field is filled automatically. If the auto-completed value is not the user name of the BSM user account you created for Service Manager to access the OMi server, change the value to the

correct user name. See "Create user accounts for the Incident Exchange (OMi - SM) integration" on the previous page.

Make a note of the Name of the new target server. You need to provide it later on as the **username** when configuring the Service Manager server to communicate with the OMi server. See "Add an integration instance for each Operations Manager i (OMi) server" on page 218.

Optionally, enter a description for the new target server.

Make sure that you check the **Active** check box.

Click **Next**.

5. Select **External Event Processing** to choose the server type suitable for an external incident manager like Service Manager.

   Click **Next**.

6. Enter the **Fully Qualified DNS Name** of the target Service Manager server.

   Click **Next**.

7. In the **Integration Type** dialog box, you can choose between using a Groovy script adapter, or the Event Synchronization Web Service.

   a. As an HP Service Manager Groovy script adapter is provided for integrating with Service Manager, select **Call Script Adapter**.

   b. In the **Script Name** field, select **sm:ServiceManagerAdapter**.

   c. Click **Next**.

8. In the **Outgoing Connection** dialog, enter the credentials (user name, password, and port number) to connect to the Service Manager server and to forward events to that server.

   a. In the **User Name** and **Password** fields, enter the Service Manager user credentials you created for the integration. See "Create user accounts for the Incident Exchange (OMi - SM) integration" on page 211.

   b. Repeat the password entry in the **Password (Repeat)** field.

   c. In the **Port** field, enter the communications port of the Service Manager server.

The Service Manager server configuration file (sm.ini) defines the http and http ports. Enter the http port when Service Manager is running in http mode, or enter the https port when it is running in secure http mode.

Tip: Clicking **Set default port** automatically populates the **Port** field with the default port (**13080** for http or **13443** for secure http). However, your actual Service Manager ports may differ from the default values.

d. If the Service Manager server uses secure http (SSL) mode, select the **Use Secure HTTP** check box. If it uses http mode, make sure the check box is not checked.

e. If the **Use Secure HTTP** check box is selected, download and install a copy of the Service Manager server's SSL certificate by clicking the link **Retrieve from Server**, or **Import from File** if the certificate is available in a local file.

f. Make sure that the **Enable Synchronize and Transfer Control** check box is checked.

When the **Enable 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 flag is not set, then the option **Synchronize and Transfer Control** does not appear in the list of forwarding types when configuring forwarding rules.

Also, note that if the **Enable 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 **Enable 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.

g. Click **Test Connection**. A **Success** or **ERROR** hyperlink appears.

Click the link to get a more detailed message.

h. Click **Next**.

9. If, in addition to automatically generating Service Manager incidents from OMi events, you want to also be able to drill-down into Service Manager, you need to specify the fully qualified DNS name and port of the Service Manager web application server (for example, Tomcat).

Note: To enable incident drill-down to Service Manager, you must have the Service Manager web tier deployed on a web application server.

In the **Event Drilldown** dialog box, configure the **Fully Qualified DNS Name** and **Port** of the web application server where the Service Manager web tier is deployed.

Note: If you do not specify a server in the **Event Drilldown** dialog box, it is assumed that the web tier is deployed on the same machine as the Service Manager server.

Click **Next**.

10. The next thing to do is to enable event changes to be synchronized back from Service Manager to OMi. For this you need to provide credentials for the Service Manager server to access the OMi server in the **Incoming Connection** dialog box.

    a. Select the **Accept event changes from external processing server** check box.

    Note: If **Enable Synchronize and Transfer Control** was previously selected, the **Accept event changes from external processing server** option is assumed, and cannot be disabled.

    b. Enter the password of the user account that you created for the Service Manager server to access the OMi server. See "Create user accounts for the Incident Exchange (OMi - SM) integration" on page 211.

    c. Make sure the **User Name** (auto-generated) matches the one of the user account you created. If not, click the **General** tab, and change the **Name** field to the correct value.

    d. Click **Finish**. The target Service Manager server appears in the list of Connected Servers.

Configure an event forwarding rule in Operations Manager i (OMi)

Once you have configured the HP Service Manager server as a connected server in HP Business Service Management (BSM) Operations Management i (OMi), you need to configure an event forwarding rule for the OMi server to forward events to Service Manager.

1. Log on to BSM as a system administrator.

2. Navigate to **Admin** > **Operations Management** > **Event Automation**.

3. Click the **New Item** button.
4. In the **Display Name** field, enter a name for the rule. For example, `smserver1`.
5. In the **Event Filter** field, select **Critical**.
6. In the **Target Servers** field, select the Service Manager server you configured as a connected server, and then click the **Add** button.

   The details of the target server are displayed.
7. In the **Forwarding Type** field, select **Synchronize and Transfer Control**.
8. Click **OK**.

   The forwarding rule is displayed in the **Event Forwarding Rules** section.

Enable incident drill-down from Operations Manager i (OMi) Event Browser

Once you have configured the HP Service Manager server as a connected server in HP Business Service Management (BSM) Operations Management i (OMi), if you want to be able to drill down to Service Manager incidents from the OMi Event Browser, you need to configure the Service Manager web tier in the **sm:ServiceManagerAdapter** script in OMi.

To configure the Service Manager web tier name in the **sm:ServiceManagerAdapter** script in OMi, follow these steps:

1. Log on to BSM as a system administrator.
2. Navigate to **Admin** > **Operations Management** > **Setup** > **Connected Servers**.
3. Click the **Manage Scripts** icon in the toolbar.
4. Click the **sm:ServiceManagerAdapter** field, and then click the **Edit** icon.
5. On the **Script** tab, locate the following string in the script:

   private static final String SM_WEB_TIER_NAME
6. Change the value of the parameter above to the name of your Service Manager web tier. For

example, if your web tier file name is **sm-9.xx.war**, change the parameter value to:

```
private static final String SM_WEB_TIER_NAME=sm-9.xx
```

7. Click **OK** to save the script.

Configure SSL for the Incident Exchange (OMi - SM) integration

Applies to User Roles:

System Administrator

When Business Service Management (BSM) is configured to accept https connections only, you must configure SSL for the integration. If you do not do so, changes on an incident that is created from OMi cannot be synchronized back to BSM/OMi.

Note: The following steps describe how you do so by using the built-in keytool in Service Manager, and the file paths are for Windows only. Be sure to change the file paths accordingly if your Service Manager system is running on Unix.

To configure SSL for the integration, follow these steps:

1. Import the BSM root certificate to the Service Manager server trusted keystore.

   The following is an example of the command line:

   ```
   <SM Install path>\server\RUN\jre\bin\keytool -import -alias myCA -file <.pem
   file of your BSM root certificate> -keystore <SM Install
   path>\Server\RUN\jre\lib\security\cacerts -storepass <changeit>
   ```

   Note: Where: *changeit* is the default password of the trusted keystore. Change it to your own password if you have changed it.

2. Add the following parameters to the Service Manager server configuration file (<*SM install path*>\Server\RUN\sm.ini):

   ```
   truststoreFile:<SM install path>\Server\RUN\jre\lib\security\cacerts

   truststorePass:<changeit>
   ```

3. Restart the Service Manager Server service.

Configure the Instance Count in the SMOMi integration template

Applies to User Roles:

System Administrator

As of version 9.34, HP Service Manager can integrate with more than one BSM OMi server. However, by default, only one OMi server is allowed. If you need to integrate Service Manager with more than one OMi server, you need to configure the Instance Count setting in the SMOMi integration template, as described below.

1. Log on to Service Manager as a system administrator.
2. Type `db` in the command line, and press Enter.
3. In the **Table** field, type `SMISRegistry`, and click **Search**.

   The SMIS integration template form opens.
4. Click **Search**.

   A list of SMIS integration templates opens.
5. Select **SMOMi** from the list.
6. In the **Instance Count** field, change the value of 1 to the number of OMi servers that you want to integrate with Service Manager. For example, if you need two OMi servers, change the value to `2`.
7. Click **Save**.

Add an integration instance for each Operations Manager i (OMi) server

Applies to User Roles:

System Administrator

Once you have completed your configuration in HP Business Service Management Operations Management, and have changed the Instance Count setting in the SMOMi integration template (which is needed only when you have multiple OMi servers), you are ready to add and enable a separate integration instance in Service Manager for each OMi server. For example, if you have two OMi servers, you must configure two SMOMi integration instances.

Support of multiple OMi servers

As of version 9.34, Service Manager can integrate with multiple OMi servers. This is implemented through the Instance Count setting and the **omi.mgr.id** parameter in the SMOMi integration template.

By default, the SMOMi integration template supports only one integration instance. If you have multiple OMi servers, before you proceed, make sure you have already updated the Instance Count setting in the SMOMi integration template. For details, see "Configure the Instance Count in the SMOMi integration template" on page 217.

When using the **omi.mgr.id** parameter, keep the following in mind:

- If you have only one OMi server (and hence need only one SMOMi integration instance), you must either correctly configure this parameter or clear the entire row of this parameter (both the parameter name and value) in the SMOMi integration instance, otherwise the integration will not work.
- If you have multiple OMi servers (and hence need multiple SMOMi integration instances), you must correctly configure this parameter in all SMOMi integration instances. Only those correctly configured integration instances will work. If none of the SMOMi integration instances are correctly configured, none of them will work.
- Users can view the OMi event details from an OMi incident record only when you specify the **omi.mgr.id** parameter correctly. If the value you specify in the corresponding SMOMi integration instance does not match the Universally Unique Identifier (UUID) which is automatically generated in the OMi server for the target Service Manager server and stored in the Incident record, users will not see the **View OMi Event** option from the Incident record.

To add and enable an Incident Exchange (OMi - SM) integration instance:

1. Log on to Service Manager as a system administrator.
2. Click **Tailoring** > **Integration Manager**.
3. Click **Add**.

   The Integration Template Selection wizard opens.
4. Select **SMOMi** from the Integration Template list.

Note: Ignore the **Import Mapping** check box, which has no effect on this integration.

5. Click **Next**.
6. Complete the integration instance information:
   - Modify the **Name** and **Version** fields to the exact values you need.
   - In the **Interval Time (s)** field, enter a value. For example: `600`. If an OMi opened incident fails to be synchronized back to OMi, Service Manager will retry the failed task at the specified interval (for example, 600 seconds).
   - In the **Max Retry Times** field, enter a value. For example: `10`. This is the maximum allowed number of retries for each failed task.
   - (Optional) In the **SM Server** field, specify a display name for the Service Manager server host. For example: my_Local_SM.
   - (Optional) In the **Endpoint Server** field, specify a display name for the BSM server host. For example: my_BSM_1.
   - (Optional) In the **Log File Directory** field, specify a directory where log files of the integration will be stored. This must be a directory that already exists on the Service Manager server host.
   - (Optional) In the **Log Level** field, change the log level from INFO (default) to another level. For example: **WARNING**.
   - (Optional) If you want this integration instance to be automatically enabled when the Service Manager Server service is started, select **Run at system startup**.
7. Click **Next**. The Integration Instance Parameters page opens.
8. On the **General Parameters** tab, complete the following fields as necessary:

Field	Sample Value	Description
omi.server.url	http://<servername>:opr-gateway/rest/synchronization/event	This is the URL address of the OMi server's RESTful web service. Replace <servername> with the fully qualified domain name of your OMi server.

Field	Sample Value	Description
http.conn.timeout	30	The HTTP connection timeout setting in seconds. **Note:** The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.
http.rec.timeout	30	The HTTP receive timeout setting in seconds. **Note:** The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.
http.send.timeout	30	The HTTP send timeout setting in seconds. **Note:** The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.
sm.mgr.id	55436DBE-F81E-4799-BA05-65DE9404343B	The Universally Unique Identifier (UUID) automatically generated for this instance of Service Manager. **Note:** This field is automatically completed each time when you add an SMOMi integration instance. Do not change it, otherwise the integration will not work properly.
omi.reference.prefix	urn:x-hp:2009:opr:	The prefix of the BDM External Process Reference field, which will be present in incoming synchronization requests from the OMi server.

Field	Sample Value	Description
		Note: This field is automatically completed and has a fixed value. Do not change it.
sm.reference.prefix	urn:x-hp:2009:sm:	The prefix of the BDM External Process Reference field, which will be present in outgoing synchronization requests from Service Manager. **Note:** This field is automatically completed and has a fixed value. Do not change it.
omi.eventdetail.baseurl	http://<servername>/opr-console/opr-evt-details.jsp?eventId=	The basic URL address of the event detail page in OMi. Replace <servername> with the fully qualified domain name of your OMi server.

9. On the **General Parameters** and **Secure Parameters** tabs, enter three parameter values that you specified when configuring the Service Manager server as a connected server in BSM OMi. The following table lists the parameters, whose values you can copy from your BSM OMi server.

   To copy the parameter values from BSM OMi, follow these steps:

   a. Log on to BSM as a system administrator.

   b. Navigate to **Admin** > **Operations Management** > **Setup** > **Connected Servers**.

   c. Locate your Service Manager server configuration entry and double-click anywhere on the entry pane.

   d. On the **General** tab, copy the **ID** string at the bottom into the **omi.mgr.id** field in Service Manager.

   e. On the **Incoming Connection** tab, copy the **User Name** and **Password** to the **username** and **Password** fields in Service Manager, respectively.

Field	Sample Value	Description
omi.mgr.id (on the **General Parameters** tab)	f3832ff4-a6b9-4228-9fed-b79105afa3e4	The 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. **Tip:** If you have only one OMi server, you can simply remove this parameter (remove both the parameter name and value) from the integration instance. See "Support of multiple OMi servers" on page 218.
username omi.mgr.id (on the **General Parameters** tab)	SM_Server	This is the user name that the Service Manager server uses to synchronize incident changes back to the OMi server.
Password (on the **Secure Parameters** tab)	SM_Server_Password	This is the password that the Service Manager server uses to synchronize incident changes back to the OMi server.

10. Click **Next** twice, and then click **Finish**.

    Note: Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

    Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

11. Enable the integration instance.

12. If you have multiple OMi servers, repeat the steps above for the rest of your OMi servers.

Next, you can optionally enable Lightweight Single Sign-On (LW-SSO) in both BSM and Service Manager so that users can bypass the log-in prompts. For details, see "Enable LW-SSO for the Incident Exchange (OMi - SM) integration" on the next page.

Enable LW-SSO for the Incident Exchange (OMi - SM) integration

Applies to User Roles:

System Administrator

Lightweight Single Sign-On (LW-SSO) is optional but recommended for the Incident Exchange (OMi - SM) integration. You have different LW-SSO configuration choices depending on your needs. The following describes how LW-SSO can be used in the Incident Exchange (OMi - SM) integration workflow.

When OMi creates an incident from an OMi event record

OMi creates an incident from an OMi event record by sending RESTful-based requests to Service Manager. The incident ID is then stored in the event record.

LW-SSO is NOT needed in this process. A dedicated Service Manager user account was specified when configuring the Service Manager integration in OMi. OMi uses this dedicated user account when calling the Service Manager RESTful Web Service to create the incident.

When an OMi user views the incident details

The user can log in to Service Manager and view the incident details using the incident ID stored in the event record. For more information, refer to the BSM documentation.

If the user wants to view the incident details by clicking the incident link from the event record, LW-SSO can be used; otherwise a Service Manager login prompt will appear.

LW-SSO is optional for this process. To enable LW-SSO for this process, configure LW-SSO in both the Service Manager server and Web tier (because the server needs to trust the Web tier), as well as in BSM.

- "Configure LW-SSO in the Service Manager server" on page 93
- "Configure LW-SSO in the Service Manager Web tier" on page 94
- "Configure LW-SSO in Business Service Management (BSM)" on page 100

When Service Manager synchronizes the OMi incident status back to OMi

When a user has updated the OMi incident, Service Manager calls the OMi server's RESTful Web Service to update the incident changes to the OMi event record.

LW-SSO is NOT needed in this process. A dedicated OMi user account was specified when the Incident Exchange (OMi - SM) integration was set up in SMIS, and Service Manager uses this user account when calling the OMi server's RESTful Web Service to synchronize the incident status back to the OMi event record.

When a user views the event details from the OMi incident

The user clicks the **View OMi Event** option from the incident to view the event details.

LW-SSO is optional for this process. If you enable LW-SSO in the Service Manager Web tier and in BSM, the BSM login prompt is bypassed.

- "Configure LW-SSO in the Service Manager Web tier" on page 94
- "Configure LW-SSO in Business Service Management (BSM)" on page 100

Configure automatic closure for OMi incidents

Applies to User Roles: System Administrator

OMi incidents can be automatically closed after a predefined amount of time since they were last updated (or resolved if they have not been updated after being resolved).

The workflow is as follows:

1. An incident is opened from OMi.
2. If the **Schedule Condition** is met, the system creates a schedule record for the incident. The schedule record will expire at a future time based on the **Calc Expression**.
3. A user updates the incident and saves the changes.
4. The **Reset alerts if** expression on the **Alerts** tab of the **probsummary** object definition is evaluated. If it evaluates to true, the Expiration time of the schedule record is updated based on the Calc Expression. By default, the expiration time of the schedule record is updated only when the incident has a category of **incident**.

5. When the schedule record expires, the **Alert Condition** is evaluated. If it evaluates to true, the incident is automatically closed.

To enable automatic closure for OMi incidents:

1. Configure the global settings in the Incident Management Environment record.
   a. Click **System Administration** > **Ongoing Maintenance** > **Environment Records** > **Incident Management Environment**.

   b. Change the following settings as necessary.

Field	Value
Close Incident Automatically?	This option disables or enables the automatic closure of OMi incidents at the global level. • If this option is not selected, no incidents will be automatically closed. • If this option is selected, incidents will be automatically closed under specified conditions. Default: Not selected
Closure Code	This value will be copied to the **Closure Code** field of incidents when they are automatically closed. Default: Automatically Closed
Solution	This description will be appended to the end of the **Solution** field of incidents when they are automatically closed. Default: This incident which belongs to OMi has been closed automatically.

   c. lick **Save**.

   d. Restart the Service Manager server.

   Note: If you have made any changes to any of the configuration options in the Incident Management Environment record, the Service Manager server must be restarted for the changes to take effect.

2. Configure the alert definition that determines when an incident should be closed.

   Note: The **alert** and **problem** processes must be running to enable the successful closure of OMi incidents.

a. Click **Tailoring** > **Document Engine** > **Alerts**.

b. In the Alert Name field, enter: **OMI Auto-Close**.

c. Click **Search**. The OMI Auto-Close alert definition detail form opens.

Caution: These fields in the alert definition are used to control automatic closure of OMi incidents. You can change the default values of these fields. However, you must be aware of the risk that automatic closure of OMi incidents will not work properly if the **Schedule Condition** and **Alert Condition** fields are not configured correctly.

Field	Value
Schedule Condition	This expression is used to determine if an incident should be scheduled for automatic closure. Default: `jscall("SMOMi.isAutoCloseAndResolved")`. An incident is scheduled for automatic closure when the following conditions are met. • The **Close Incident Automatically?** option in the Incident Management Environment record is selected. • In the incident record, the **Do not close this incident automatically** option is not selected. • The incident has a status of **Resolved**.
Alert Condition	This expression is evaluated when an incident is about to be automatically closed. If it evaluates to true, the incident is closed. Default: `jscall("SMOMi.isAutoCloseEnabled")`. An incident is closed when the following conditions are met. • The **Close Incident Automatically?** option in the Incident Management Environment record is selected. • In the incident record, the **Do not close this incident automatically** option is not selected.
Calc Expression	This expression is used to determine how much time will elapse before an incident is automatically closed. Default: `$L.alert.time=update.time in $L.file+'7 00:00:00'`. The default value means the amount of time elapsed is equal to seven days since the incident was last updated.

3. Configure alert information in the **probsummary** object.
   The OMi autoclose alert definition is configured to only be used by OMi incidents. The closure time is reset each time the incident is updated. If the closure time is reached without the incident being updated then Service Manager will automatically close the incident.

   a. Click **Tailoring** > **Document Engine** > **Objects**.

   b. In the **File name** field, enter **probsummary** and press ENTER. The **probsummary** object definition is displayed.

   c. Select the **Alerts** tab.

      The **Reset alerts if** expression is used to reset the automatic closure time of OMi incidents.

      Default: `category in $L.file="incident" and not null(1 in external.process.reference in $L.file)`.

Change the default assignment group for OMi incidents

Applies to User Roles:

System Administrator

HP Service Manager can accept REST based requests from BSM Operations Manager i (OMi) to create incidents based on events information in OMi. An incident opened from an OMi event is automatically assigned to an existing group based on the following field values, listed from the highest to lowest priority:

- The **Affected Service** of the incident
- The **Category** of the incident
- The **Affected CI** of the incident

However, if none of the above field values is available, the incident is assigned to a default group named **Application**. If necessary, you can change this default group setting as follows:

1. Navigate to **System Administration** > **Ongoing Maintenance** > **BDM Mapping Management**. The BDM mapping configuration search page opens.
2. Enter **incident** in the BDM Name field, select **1.1** in the **Version** field, and then click **Search**. The BDM mapping record **incident** is displayed. The Incident Exchange (OMi - SM) integration uses this BDM mapping record when creating an incident from an OMi event.

3. Select the **Field Mapping** tab, scroll down to the **assignment** field in the SM Object Field column, and click the **SM Callback** field in the same row.

4. Change **Application** in the following code to the name of another assignment group:

```
4)  A default assignment group if no other criteria is met
       if( ! $result ) {
               $result = "Application";
       }
```

5. Click **Save**. The default assignment group is now changed.

Synchronization of incident changes back to Operations Manager i (OMi)

After OMi opens an incident in HP Service Manager, Service Manager will synchronize the incident changes back to OMi.

Operations Manager i (OMi) can forward an event record to Service Manager as an incident by calling a Service Manager Web Service. The incident ID is then stored in the event record.

When a user has updated the incident opened from OMi, Service Manager calls an OMi server RESTful Web Service to update the incident changes to the OMi event record.

If Service Manager fails to synchronize the incident changes back to OMi for some reasons (for example, because of a network problem), Service Manager behaves as follows:

- Displays a warning message, indicating that the incident failed to be synchronized to OMi.
- Saves the failed task in the SMIS task queue, and retries the task to re-synchronize the changes to OMi based on an interval time and a maximum retry times configured when adding the Incident Exchange (OMi - SM) integration in SMIS. When the re-synchronization is successfully completed, the failed task is removed from the task queue.

System Administrators can monitor failed tasks, and reset their retry times or rerun expired tasks. For more information, see "Monitor failover tasks" on page 90.

Working with the Incident Exchange (OMi - SM) integration

Once the integration is set up, Service Manager Incident Management users with the right permissions can view event details from OMi incidents and mark individual OMi incidents as eligible or ineligible for automatic closure (if their system administrator has enabled automatic closure for OMi incidents).

View related OMi event details from an incident

If all of the following conditions are met, you can view the related Operations Manager i (OMi) event details from an OMi incident:

- You are accessing the incident through the HP Service Manager standard Web client (not the employee self-service (ESS) interface).
- One or more SMOMi integration instances are set up and enabled in Integration Manager.
- You are also a Business Service Management (BSM) user who has been granted the permission **Events assigned to user** including the required actions.

To view related OMi event details from an OMi incident:

1. Log on to the Service Manager Web client.
2. From **Incident Management**, search for the incident record created from OMi.
3. Click **More** and then select **View OMi Event**.

   Note: The **View OMi Event** option displays only when the **omi.mgr.id** parameter in the corresponding SMOMi integration instance is set correctly.

   If Lightweight Single Sign-On (LW-SSO) is enabled in both the Service Manager Web client and HP Business Service Management (BSM) , the OMi event detail page opens in a new browser window, displaying the details of the related event in OMi. If LW-SSO is not enabled, a BSM login page opens, and the related OMi event detail page displays after you log on to BSM.

Mark an incident for automatic closure

Applies to User Roles:

Incident Coordinator

You can mark an OMi incident as eligible or ineligible for automatic closure after a predefined amount of time since it was last updated.

To mark an incident as ineligible or eligible for automatic closure:

1. From **Incident Management**, search for an incident record opened from OMi.
2. Select or deselect the **Do not close this incident automatically** check box to mark this incident as ineligible or eligible for automatic closure.

   Note: By default, this check box is not selected.

BSM Business Impact Report (BIR)

HP Business Service Management (BSM) includes a report that you can use to help evaluate the impact of incidents on your business. A Business Impact report displays information about how a CI impacts the Business Services it belongs to. Data about the affected Business Service, Application, and Business Process CIs includes KPI data, over-time data, and SLA data. For example, if a host CI has critical status, you can use the report to display the status of the Business Service CIs to which the host CI is attached.

Incident Management users can launch an impact report from an incident in context with the incident's affected configuration item (CI). Service Desk Agents can validate the updated status of the business impact to categorize and prioritize the incident accordingly.

This integration also supports multi-tenancy. System Administrators can enable multi-tenancy for the integration.

Note:

- This integration requires that both Service Manager and BSM be integrated with HP Universal CMDB (UCMDB) so that configuration items (CIs) can be synchronized between the servers. For details about how to configure an integration from Service Manager or BSM to UCMDB, see "HP Universal CMDB" on page 152 and refer to the HP Business Service Management (BSM) documentation.
- Only one instance of this integration is allowed.

Prerequisites:

- Before end-users can use this integration, System Administrators must add and enable an instance of this integration in Integration Manager (SMIS).
- Optionally, System Administrators can use Lightweight Single Sign-On (LW-SSO) to bypass the log-in prompts.

BSM Business Impact Report integration setup

To set up the BSM Business Impact Report (BIR) integration in your environment, you need to complete the following tasks:

1. "Add a BSM Business Impact Reports integration" below

   This task creates and enables an instance of this integration in the Integration Manager (SMIS).

2. "Enable LW-SSO for the Business Impact Report (BIR) integration" on page 234

   LW-SSO is optional but highly recommended for this integration. This task includes enabling LW-SSO in both the Service Manager Web tier and BSM. Enabling LW-SSO for the integration enables Incident Management users to bypass the login prompts when launching a BSM business impact report from an incident.

3. "Enable multi-tenancy for the BSM Business Impact Report integration" on page 234

   This task is required only when your Service Manager environment is running in multi-company mode.

Add a BSM Business Impact Reports integration

Applies to User Roles:

System Administrator

To use the Service Manager to BIR integration, you must add and enable an instance of this integration in Integration Manager. Optionally, you can enable Lightweight Single Sign-On (LW-SSO) in BSM and in Service Manager to bypass the log-in prompts.

To add and enable a Service Manager to BIR integration instance:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The Integration Template Selection wizard opens.

3. Select **SMBIR** from the Integration Template list. Ignore the **Import Mapping** check box, which has no effect on this integration.

   Note: Only one instance of this integration is allowed. If an instance of this integration already exists in Integration Manager, the **SMBIR** template is unavailable. You have to delete the existing integration instance before you can add a new one.

4. Click **Next**. The Integration Instance Information page opens.

5. 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 UI-based.

Field	Value
Name	(Required) The name of the integration instance. Default: `SMBIR`
Version	(Required) The version of the integration template. Default: `1.0`
SM Server	The name of the Service Manager server machine.
Endpoint Server	The name of the BSM Server machine.
Log Level	Select one from: DEBUG, INFO (default), WARNING, ERROR, and OFF.
Log File Directory	A directory on the Service Manager Server machine in which log files will be stored.
Description	If you want, modify the default description of the instance.
Run at system startup	Select this check box only if you want this instance to be automatically enabled when the Service Manager Server is started.

6. Click **Next**. The Integration Instance Parameters page opens.

7. On the **General Parameters** tab, replace "BSM_host" in the **baseurl** parameter with the hostname of the real BSM server.

8. Click **Next** twice and then click **Finish**. Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

   Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

9. Enable the integration instance.

10. Optionally:

    - Configure LW-SSO in BSM
    - Configure LW-SSO in Service Manager

Enable LW-SSO for the Business Impact Report (BIR) integration

If LW-SSO is enabled for the BIR integration, you can launch a business impact report in BSM from a Service Manager incident.

To enable LW-SSO for the BIR integration, complete the following tasks:

- "Configure LW-SSO in the Service Manager Web tier" on page 94
- "Configure LW-SSO in Business Service Management (BSM)" on page 100

Enable multi-tenancy for the BSM Business Impact Report integration

Applies to User Roles:

System Administrator

The BSM Business Impact Report integration provides multi-tenancy support, which allows an Incident Management user to launch BSM Business Impact Report based on the UCMDB Customer ID of the user's company.

To enable multi-tenancy for this integration, you need to complete the following tasks:

1. Enable multi-tenancy in Service Manager.
2. Synchronize companies between Service Manager and UCMDB.
3. Synchronize companies between BSM and UCMDB.

If you have enabled multi-tenancy for the integration, when a user launches a Business Impact Report from an incident, the business impact report is displayed not only in the context of the incident's related Business Service or Affected CI, but also based on the Customer ID of the company record retrieved from the user's contact information.

Note: You can click the Find icon for a user's **Contact ID** field to find information about the company associated to the user.

To enable multi-tenancy in Service Manager:

1. Log on to Service Manager.
2. Go to **System Administration** >**Base System Configuration** > **Miscellaneous** > **System Information Record**.
3. In the **General** tab, select **Run in Multi-Company Mode**.
4. In the **Active Integrations** tab, do the following:
   - Select **HP Universal CMDB**.
   - In the **Multi-tenant UCMDB webservice URL** field, type the URL to the multi-tenant UCMDB Web Service API. The URL has the following format:

     <UCMDB server name>:<port>/axis2/services/ucmdbManagementService

     Replace *<UCMDB server name>* with the host name of your UCMDB server, and replace *<port>* with the communications port your UCMDB server uses.
   - In the **UserId** and **Password** fields, type the user ID and password of a UCMDB user account that has permission to access the multi-tenant UCMDB Web Service API.

   Note: The **UCMDB webservice URL**, **UserID**, and **Password** fields are not required for enabling multi-tenancy.
5. Log off and then log back on to Service Manager so that the configuration takes effect.

To synchronize a company between Service Manager and UCMDB:

1. Go to **System Administration** > **Base System Configuration** > **Companies**.
2. Open an existing company record or create a new one.

a. To open an existing company record, click **Search** and select the record from the list.

b. To create a new company record, type a `Customer ID`, `Company Code`, and `Company Name` for the new record, and then click **Add**.

3. In the **Company** tab, complete the following fields:
   - In the **Customer ID** field, type a unique ID number. For example, 2.
   - In the **Customer Code** field, type a unique code name.
   - In the **Show Company in Multi-Company Lists** field, select **Yes**.
4. Click **OK**.
5. When prompted to confirm if you want to synchronize this company with UCMDB, select **Yes**.

To synchronize a company between BSM and UCMDB:

For information about how to synchronize a company between BSM and UCMDB, refer to the BSM documentation.

Launch a Business Impact Report from an incident

Applies to User roles:

Service Desk Agent

> **Note:** Make sure that an SMBIR integration instance is enabled in **Integration Manager** before performing the steps below.

To launch a Business Impact Report from an incident:

1. Log on to the Service Manager Web client.
2. From **Incident Management**, search for an incident record and open it.
3. Click **More** and then select **Launch Business Impact Report**.
   If LW-SSO is enabled in both Service Manager and BSM, the summary information from BSM about business CIs that are affected by the affected CI of the incident is displayed. If LW-SSO is not enabled, a BSM login page displays, and the business impact summary information displays after you log on.

SM-BSM downtime synchronization

The downtime entity plays a central role in many of the IT processes that are executed during the normal operations of an IT group. Failing to correctly manage this entity across all IT disciplines can:

- Cause misunderstandings about the state of a CI and as a result the state of a business service.
- Increase false positive events.
- Increase the mean time to restoration (MTTR).
- And overall negatively influence the perception of the business users about the SLA they get from IT.

The synchronization of downtime information between Service Manager and BSM is to avoid the above situations.

HP Business Service Management (BSM) includes a module that you can use to synchronize the downtime which is generated in Service Manager. The runtime service model (RTSM) will maintain the downtime as a scheduled downtime CI with its related configuration items. If there is HP Universal CMDB (UCMDB) deployed between Service Manager and RTSM, the integration will synchronize downtime information through UCMDB between the servers.

The Service Managerand BSM integration supports two use cases of downtime management:

- Synchronize scheduled downtimes from Service Manager RFCs and tasks to BSM in order to suppress events.
  For details about Service Manager configuration and adapter setup in BSM or UCMDB for downtime management, see "SM-BSM downtime synchronization setup" on the next page.
- Event management of BSM to synchronize scheduled downtimes from BSM to Service Manager incidents for the Service Desk's attention.
  For details about how to create and close incidents in Service Manager from BSM Operations Manager i (OMi), see "Configure automatic closure for OMi incidents" on page 225 and "Change the default assignment group for OMi incidents" on page 228.

  Note: The incoming incident created from BSM downtime does impact CI Availability in Service Manager.

SM-BSM downtime synchronization setup

Prerequisite:

- To enable downtime synchronization between Service Manager and BSM, you need to apply the latest Content Package and update to UCMDB or to RTSM.
- The SLA scheduler needs to be started in the **System Status** form.
- Make sure the related CI which downtime is scheduled on has already been synchronized between Service Manager and HP Universal CMDB.

To set up the SM-BSM downtime synchronization in your environment, you need to complete the following tasks:

- "Add an instance in Service Manager Integration Suite (SMIS) " on the next page

  To set up the integration from Service Manager to RTSM, this task creates the SMBSM_DOWNTIME instance in Service Manager Integration Suite (SMIS). Note that additional setup is required on the BSM OMi side for integration from BSM to Service Manager. For details, refer to the *HP Business Service Management Operations Manager i Extensibility Guide*.

- "Tailor Service Manager to handle phase change" on page 242

  In Change Management module, authorized users can manually change the phase of a change record. This will affect the validation of related scheduled downtime. This task tailors Service Manager to keep the scheduled downtime accurate after users manually changed the phase of related change.

- "Set up integration in BSM" on page 243

  If you do not have UCMDB, perform this task to set up a new integration in RTSM to proactively pull the scheduled downtime from Service Manager.

- "Set up integration in HP Universal CMDB" on page 243

  This task sets up a new integration in HP Universal CMDB to proactively pull the scheduled downtime from Service Manager.

- "Verify the SM-BSM downtime synchronization setup" on page 244

  Perform this task to check if you have successfully set up your SM-BSM downtime synchronization.

Notes:

1. For Changes/Tasks that have final approval phases defined in Service Manager Integration Suite (SMIS), the downtimes will be synchronized after the Changes/Tasks get final approval.
2. Only downtimes that end at a future time will be synchronized.
3. Select the **Configuration Item(s) Down** checkbox when scheduling downtimes in Changes/Tasks.

Add an instance in Service Manager Integration Suite (SMIS)

Applies to User Roles:

System Administrator

To set up the integration from Service Manager to RTSM, you must add an instance of this integration in the Service Manager Integration Suite (SMIS). Note that additional setup is required on the BSM OMi side for integration from BSM to Service Manager. For details, refer to the *HP Business Service Management Operations Manager i Extensibility Guide*.

To add the SMBSM_DOWNTIME instance:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The Integration Template Selection wizard opens.
3. Select **SMBSM_DOWNTIME** from the Integration Template list. Ignore the **Import Mapping** check box, which has no effect on this integration.
4. Click **Next**. The Integration Instance Information page opens.
5. Do the following:
   - Modify the **Name** and **Version** fields to the exact values you need.
   - In the **Interval Time(s)** field, enter a value based on your business needs in regard to downtime exchange frequency. Note that a short interval time can be safe because the next scheduled task will not start until the previous task is completed and the interval time passed.
   - In the **Max Retry Times** field, enter a value. This is the maximum allowed number of retries (for example, 10) for each failed task.

- In the **Log File Directory** field, specify a directory where log files of the integration will be stored. This must be a directory that already exists on the Service Manager server. By default, logging message is output to `sm.log`.
- (Optional) In the **SM Server** field, specify a display name for the Service Manager server host. For example: my_local_SM.
- (Optional) In the **Endpoint Server** field, specify a display name for the BSM server host. For example: my_BSM_1.
- (Optional) In the **Log Level** field, change the log level from INFO (default) to another level. For example: WARNING.
- (Optional) If you want this integration instance to be automatically enabled when the Service Manager Server service is started, select **Run at system startup**.

6. Click **Next**. The Integration Instance Parameters page opens.
7. On the **General Parameters** tab, complete the following fields as necessary:

Name	Category	Value	Description
WithdrawDowntime	General	true/false	Set this value to `true`: When authorized users are manually changing the phase of a change record which has 'valid' outage, a window will open and provide choices of withdrawing the outage. Set this value to `false`: The pop-up window is disabled. This operation may cause some unapproved planned downtimes be synchronized to BSM. By default, this value is set to `true`.
Category or workflow (Process Designer) name of changes	Change	The final approval phase for changes	Set the final approval phase for downtime, which is the indication of valid downtime information.
Category or workflow (Process Designer) name of tasks	Task	The final approval phase for tasks	Set the final approval phase for downtime, which is the indication of valid downtime information.

Name	Category	Value	Description
sm.host	General	<sm server name >	Set the Service Manager server host name or DNS name to compose the External Process Reference and the Reference Number of Scheduled Downtime CI in UCMDB. **Note:** Do not include a colon in this field. Otherwise, the logic will be broken.
sm.reference.prefix	General	urn:x-hp:2009:sm	Set the prefix to compose the External Process Reference of Scheduled Downtime CI in UCMDB. **Note:** This field has a fixed value. Do not change it.

Notes:

a. Type category or workflow name of change/task in the **Name** column. This value is case-sensitive and it must match the record in Service Manager database.

b. Set the value to Change for changes in the **Category** column. Similarly, set the value to Task for tasks.

c. Type the final approval phase in the **Value** column. This value is case-sensitive and it must match the record in Service Manager database.You can separate multiple phases by semicolons, which must be the English character.

d. Detailed information will be displayed in the integration log when the following errors occur:
   - User input of categories/phases for the changes/tasks is not correct.
   - The category and phase pair does not exist in the database.

e. For Change Management categories which do not have approval phase, the downtime integration will treat its downtime information as final approved once created. You do not need to define any phases in SMIS parameters.

f. For the category or workflow name of the changes and the tasks, the integration will ignore all the final phases defined for the redundant category or workflow.

8. Click **Next** twice and then click **Finish**. Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

   Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

9. Enable the integration instance. SMIS will validate all the final phases you filled in the Integration Instance Parameters page and print warning messages if there are errors.

Tailor Service Manager to handle phase change

Applies to User Roles:

System Administrator

Implementer

In the Service Manager Change Management module, authorized users can manually change the phase of a change record. If the phase is changed to the one prior to the final approval phase in the SMBSM_DOWNTIME instance, the system will check if there are existing planned downtimes that have been set to Ready. If such downtimes exist, a window will open and provide two options for the corresponding planned downtimes:

- Click **Yes** to withdraw the corresponding planned downtimes from UCMDB. The changes or tasks need to be approved again to synchronize with UCMDB at another time.
- Click **No**. There will be no change to the planned downtimes even if the actual status of the changes or tasks are not approved.

Note: To disable the pop-up window when withdrawing the planned downtimes, you need to set the `WithdrawDowntime` parameter to `false` in the SMBSM_DOWNTIME instance. This operation may cause some unapproved planned downtimes to be synchronized to BSM.

With Process Designer (PD) Content Pack 2 applied in Service Manager, you can tailor the process to transit changes or tasks from one phase that is after the final approval phase in the SMBSM_DOWNTIME instance to another that is prior to the final approval phase.To withdraw the related planned downtime for this kind of transition, you need to add a rule set for the transition in the Closed Loop Incident Process (CLIP) solution. Refer to the following steps:

1. Go to the target workflow that needs tailoring.
2. Select the transition that moves a phase from before the final approval phase to after the final approval phase.
3. In the Rule Sets section, click **Add** and select the **clip.downtime.withdraw** rule set.
4. Click **OK** to save the workflow.

Set up integration in BSM

If you have HP Universal CMDB (UCMDB) between Service Manager and BSM, you can use UCMDB to maintain downtime CIs that are populated from Service Manager, and BSM will consume them through UCMDB. There is no need to set up an integration in BSM (RTSM).

If you do not have UCMDB between Service Manager and BSM, you need to set up a new integration in BSM (RTSM) to proactively pull the scheduled down time from Service Manager.

Being an instance of UCMDB, RTSM is embedded in BSM and performs the expected functions of a CMDB. RTSM reconciles and stores configuration items (CIs) that represent the IT environment components and helps organizations understand the relationships between these components and track their configuration.

Make sure you have applied the latest content package and update to RTSM. For instructions on how to set up a downtime integration in RTSM, refer to the *Data Flow Management Guide*.

Set up integration in HP Universal CMDB

This task sets up a new integration in HP Universal CMDB (UCMDB) to proactively pull the scheduled downtime from Service Manager. Make sure you have applied the latest Content Package and update to your UCMDB.

To set up the HP Universal CMDB adapter:

1. Log in to your UCMDB system as an administrator.
2. Create an integration point that connects to your Service Manager server. For example: SM931. Make sure this integration point uses the latest **ServiceManager Adapter 9-x**.
3. Click **Managers** > **Data Flow Management** > **Integration Studio**. UCMDB displays a list of integration points.

4. Select **sm931** in the Integration Point list. Make sure the **SM Configuration Items Population job** and the **SM Relations Population job** run first.

5. Create two integration jobs in the integration point.

   a. Create a new job including the `CLIP Down Time Population` job definition. Under **Scheduler Definition**, select the **Scheduler enabled** checkbox and set the Repeat Interval to 1 Minute. Click **OK** to save the job.

   b. Creat another new job including the `CI To Down Time CI With Connection` job definition. Under **Scheduler Definition**, select the **Scheduler enabled** checkbox and set the Repeat Interval to 1 Minute. Click **OK** to save the job.

   Pay attention to the running order. The `CLIP Down Time Population` job must be run at first. You can set the two jobs as schedule-based and set the schedule interval according to your needs.

6. After the two jobs have finished successfully, go back to the **Modeling** section and check the CIs with type **ScheduledDowntime**. Make sure their relationships are created.

Note: If no related CIs exist in UCMDB when creating relationships, the population will fail or succeed with a warning. To disable the warning, remove the downtime CI that does not have related CIs in UCMDB.

Verify the SM-BSM downtime synchronization setup

Applies to User Roles:

System Administrator

When you have set up the Downtime integration, you can perform the following tasks to see if you have successfully set up your downtime synchronization.

Task 1. Open a new change of a category that has the final approval phase defined in SMIS

1. Click **Change Management** > **Changes** > **Create New Change**.

2. Select **Hardware** for example.

3. In the Affected CI field, set the name of the CI to be synchronized. For example: `adv-afr-desk-101`.
4. Set Scheduled Downtime Start and Scheduled Downtime End to a future time.
5. Select the **Configuration Item(s) Down** checkbox.
6. Set other required fields.
7. Click **Save&Exit**.

Task 2. Approve the change at the final approval phase

1. Click **Change Management** > **Changes** > **Search Change** and search for the change opened in Task 1.
2. Move the Change to the Change Approval phase.
3. Log on to Service Manager with user account `Change.Approver`.
4. Search for the change and approve it.

Task 3. Create new format for the intClipDownTime table

1. Click **Tailoring** > **Forms Designer**.
2. Create a new format for the intClipDownTime table by using the Form Wizard.
3. Add all fields to this format.

Task 4. Check the corresponding intClipDownTime record

1. From Database Manager, open the format of the intClipDownTime table.
2. Click **Search** to see the record created for this downtime.
3. Check the External Status field:

External Status values	Description
NULL	The downtime is waiting for final approval, or the scheduler has not

External Status values	Description
	proceeded this record yet.
0 (Canceled)	The downtime is canceled before being implemented.
1 (Ready)	The downtime has been approved and is ready to be synchronized to UCMDB or BSM (RTSM).
2 (Withdrawn)	The downtime is approved firstly and then the approval is retracted (withdrawn).

Notes:

a. Only downtime records with External Status 1 can be synchronized.

b. If the External Status is not 1, wait some time for background schedulers SLA and SMBSM_DOWNTIME to process this record.

Task 5. Populate downtime from Service Manager to UCMDB

1. From UCMDB, run the CLIP Down Time Population job and the CI To Down Time CI With Connection job in a fixed order.
2. Search for the adv-afr-desk-101 CI in UCMDB. Check that a corresponding Scheduled Downtime CI is created, and a relationship between the Scheduled Downtime CI and the affected CI is created.

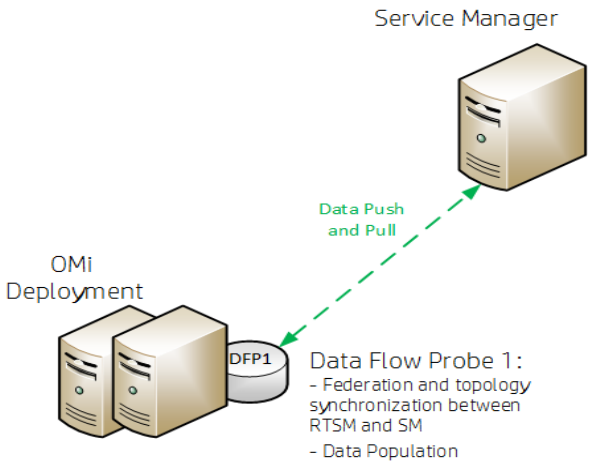
Note: If any of the aforementioned tasks fails, refer to "SM-BSM downtime synchronization setup" on page 238 and check if all the system prerequisites are met.

OMi – Service Manager integration overview

There are two variations of integrating Service Manager (SM) with OMi. One case uses the RTSM contained in OMi as the CMDB, and needs only one data flow probe (DFP1), which is installed in the OMi deployment. The other case uses a UCMDB, and needs two data flow probes (DFP1 installed on the UCMDB server and DFP2 in the OMi deployment).

Point to point integration

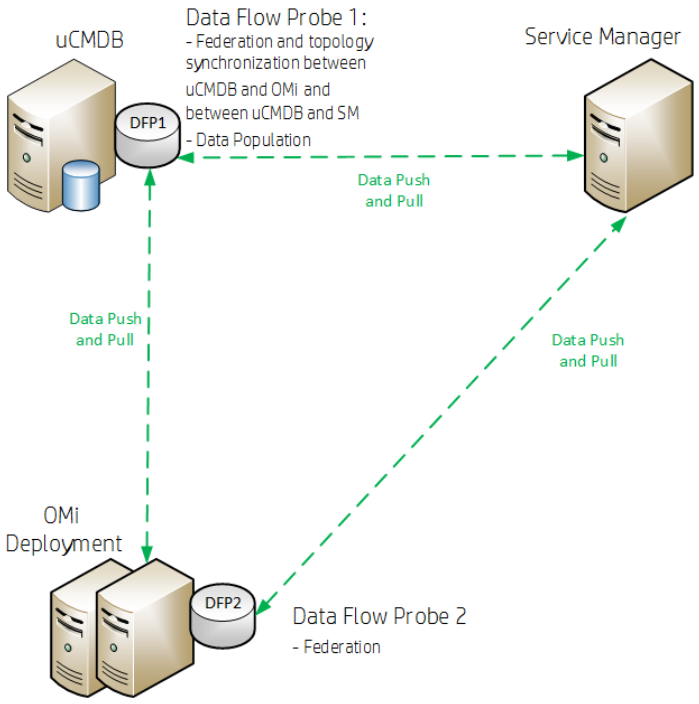
OMi is integrated with Service Manager directly, using OMi's Run Time Service Model (RTSM) as CMDB, as shown in the following figure.



HP recommends installing the Data Flow Probe 1 (DFP1) in the OMi deployment.

Integration using a Universal Configuration Management Database (UCMDB)

OMi is set up using an external UCMDB, as shown in the following figure.



HP recommends to install the Data Flow Probe 1 (DFP1) on the UCMDB server and the Data Flow Probe 2 (DFP2) in the OMi deployment.

Data flow probes

Two different data flow probes need to be installed. They have different purposes.

- DFP1 is needed for the following:
  - Populating the RTSM with CIs (Data Population)
  - Federation
  - Topology synchronization (CIs) between RTSM and SM in the case of a point to point integration

OR

- Topology synchronization (CIs) between UCMDB and OMi and between UCMDB and SM in case of using an external UCMDB

- DFP2 is needed for federation only.

Prerequisites

If you are using a standalone CMDB, you need to do the following before continuing with the OMi- SM integration:

- Set up the integration between OMi and UCMDB.
- Integrate the UCMDB with SM to synchronize CIs from the UCMDB to SM. For details, see the *Service Manager Universal CMDB Integration Guide*.

Versions

In general, the information provided in this guide is for integrating OMi with SM 9.3x. For instructions on integrating OMi with earlier versions of SM, see http://support.openview.hp.com/selfsolve/document/KM1303768/binary/BSM9.12_SM_Integration_Interactive_Docs.html. Download and extract the zip file contents, and then open the **SM_interactive_document.htm** file and follow the guidelines.

Caution: When integrating OMi with SM 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

Integration options

- **Incident exchange between SM and OMi.** OMi enables you to forward events from OMi to SM. Forwarded events and subsequent event changes are synchronized back from SM to OMi. You can also drill down from OMi events to SM incidents. For details, see .
- **Downtime exchange between OMi and SM.** OMi enables you to forward downtimes (also known as outages) from OMi to SM, and from SM to OMi. The downtime defined in OMi is directed to SM as an incident, and vice versa. For details, see "Downtime Exchange between OMi and Service Manager" on page 280.
- **View planned changes and incident details in Service Health.** This integration enables you to view planned changes and incident details in the Changes and Incidents tab in the 360° View page in Service Health. For details, see the *OMi Integration Guide*.
- The **Business Impact Report** integration is described in the *Closed Loop Incident Process (CLIP) Guide*. When deployed as part of the OMi solution, Incident Management users can launch an impact report from an incident in context with the incident's affected CI. Service desk agents can validate the updated status of the business impact to categorize and prioritize the incident accordingly. For details, see the CLIP page in the Solutions Portal at:

  https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710

Note:

- **Service Manager Query Security**: If you have set up an integration from OMi to SM, there is a CI context menu that enables you to access SM from OMi Service Health. This drill-down option is not available if you have enabled Service Manager query security.
- **Troubleshooting Multiple Domains**: If OMi and SM are in different domains, and you are using Internet Explorer as your browser, you may need to add the domains to the list of allowed domains in the Privacy tab (**Internet Options > Privacy > Sites**).

Incident Exchange (OMi - SM) integration

The Incident Exchange (OMi - SM) integration is a bidirectional integration between incident records in HP Service Manager and events in Operations Manager i (OMi).

This integration requires configurations on both product sides. For details, see "Incident Exchange (OMi - SM) integration setup" below.

Note: As of version 9.34, Service Manager can integrate with multiple OMi servers. For details, see "Add an integration instance for each OMi server" on page 262.

Service Manager can accept RESTful-based requests from OMi to create incidents in Service Manager, based on events information in OMi. When Service Manager accepts an incident creation request from a remote OMi server, it creates an incident record and automatically assigns it to an existing group based on certain field values. Incident Management users can view the details of the related OMi event by clicking the **View OMi Event** menu option from the incident record. See "Drill down to the OMi event details from an incident" on page 279.

When an Incident Management user makes any changes to the incident record, Service Manager automatically synchronizes the changes to the corresponding event in OMi, by sending an update request to the OMi RESTful web service interface. In the event of a synchronization failure, a queuing mechanism will re-synchronize the changes. See "Synchronization of incident changes back to Operations Manager i (OMi)" on page 278.

System administrators can configure global settings that determine whether and when incident records opened from OMi events can be automatically closed. However, Incident Management users can mark individual OMi incident records as eligible or ineligible for automatic closure. See "Configure automatic closure for OMi incidents" on page 269 and "Mark an incident for automatic closure" on page 280.

Incident Exchange (OMi - SM) integration setup

The Incident Exchange (OMi - SM) integration requires the following configuration tasks be completed on the HP Service Manager and Operations Manager i (OMi) systems.

1. "Create user accounts for the Incident Exchange (OMi - SM) integration" on page 253.

   This task creates a user account on each product side for the two systems to connect to each other and to synchronize data.

2. "Configure an event forwarding rule in OMi" on page 258.

   This task configures a rule for the OMi server to forward events to the Service Manager server.

3. "Configure the Service Manager server as a connected server in OMi" on page 254.

This task configures the connection settings for the target Service Manager server. If you need to integrate Service Manager with more than one OMi server, perform this task on each of the OMi servers.

4. (Optional) "Add custom attributes and map to SM fields" on page 257.

   This task adds your own custom attributes in the Groovy script selected for the SM server and maps the attributes to appropriate fields in SM.

5. "Enable event drill-down from Service Manager into OMi" on page 258

   This task sets up Service Manager operators as valid users with appropriate permissions in OMi. These permissions are required for the users to perform event drill-down from Service Manager to OMi.

6. "Enable incident drill-down from the OMi Event Browser" on page 259.

   This task configures the Service Manager web tier in the **sm:ServiceManagerAdapter** script in OMi.

7. (Optional)"Configure SSL for the Incident Exchange (OMi - SM) integration " on page 260.

   This task is needed if your OMi server requires HTTPS connections. If SSL is not configured in this case, changes on incidents that are created from OMi will not be able to be synchronized back to OMi.

8. "Configure the Instance Count in the SMOMi integration template" on page 261.

   This task is needed only when you use more than one OMi server. The Instance Count setting defines the allowed number of SM-OMi integration instances in Service Manager (default: 1).

9. "Add an integration instance for each OMi server" on page 262.

   This task creates and enables an instance of this integration in Integration Manager (SMIS). A separate integration instance is required for each OMi server.

10. (Optional) "Enable LW-SSO for the Incident Exchange (OMi - SM) integration" on page 267.

    Lightweight Single Sign-On (LW-SSO) is optional but recommended for the Incident Exchange (OMi - SM) integration. This task includes enabling LW-SSO in the Service Manager server and Web tier, as well as in OMi.

11. (Optional) "Configure automatic closure for OMi incidents" on page 269.

By default, automatic closure is disabled for OMi incidents. System administrators can enable automatic closure and further configure under what conditions OMi incidents can be automatically closed.

12. (Optional) "Change the default assignment group for OMi incidents" on page 272.

    When created, OMi incidents are automatically assigned with an assignment group based on their certain field values and a predefined default assignment group. System Administrators can change the default assignment group setting (**Application**).

13. "Test the connection" on page 273

    This task sends an event to the OMi server that matches the filter you defined (in our example filter, the severity value is Critical), and then verifies that the event is forwarded to Service Manager as expected.

14. (Optional) "Synchronize attributes" on page 274

    Not all attributes are synchronized back from SM to OMi by default. This task changes the out-of-box behavior regarding which attributes are synchronized upon change.

Create user accounts for the Incident Exchange (OMi - SM) integration

Applies to User Roles:

System Administrator

The Incident Exchange (OMi - SM) integration is bidirectional. Synchronizing events and incidents between the HP Service Manager and BSM OMi systems requires integration accounts be set up for the two systems to access each other.

1. Create an operator record with system administration privileges in Service Manager. For details, see "Creating operator records" on page 1.

   This is the user account that the OMi server uses to access Service Manager and to forward events to Service Manager.

   Later, when configuring the Service Manager server as a connected server in OMi, you need to specify this operator's login name and password on the **Outgoing Connection** tab. See "Configure the Service Manager server as a connected server in OMi" on the next page.

2. Create a user account with system administration privileges on each OMi server. For details, see the OMi online help.

   This is the user account that Service Manager uses to access the OMi server and to synchronize incident changes back.

   Later, when configuring the Service Manager server as a connected server in OMi, you must specify this user's login name as the **Name** of the Service Manager server on the **General** tab, and specify this user's password as the **Password** on the **Incoming Connection** tab. See "Configure the Service Manager server as a connected server in OMi" below.

   Also, you need to specify the same user account when adding an SM-OMi integration instance for each OMi server (the **username** and **Password** parameters). See "Add an integration instance for each OMi server" on page 262.

Configure the Service Manager server as a connected server in OMi

To synchronize changes between OMi events and Service Manager incidents, you need to configure a connected server within OMi to correctly identify the target Service Manager server instance.

To configure the Service Manager server as a target connected server, perform the following steps:

1. Log on to Operations Manager i as a system administrator.
2. Navigate to the Connected Servers user interface:

   Administration > **Setup and Maintenance** > **Connected Servers**

3. Click the **New** button, and then select **External Event Processing** to open the **Create New Server Connection** dialog box.
4. In the **Display Name** field, enter a descriptive name for the Service Manager server.

   In the **Name** field, enter the user name of the OMi user account you created for Service Manager to access the OMi server. See "Create user accounts for the Incident Exchange (OMi - SM) integration" on the previous page.

   Make a note of the Name of the new target server. You need to provide it later on as the **username** when configuring the Service Manager server to communicate with the OMi server. See "Add an integration instance for each OMi server" on page 262.

   Optionally, enter a description for the new target server.

Make sure that the **Active** check box is selected.

Click **Next**.

5. In the Server Properties pane, enter the following information:

   Fully Qualified DNS Name: The fully qualified domain name of the target Service Manager server.

   CI Type: Select **Service Manager System** from the list.

   Keep the Advanced Delivery Options as default.

   Click **Next**.

6. In the **Integration Type** dialog box, you can choose between using a Groovy script adapter, or the Event Synchronization Web Service.

   a. As an HP Service Manager Groovy script adapter is provided for integrating with Service Manager, select **Call Script Adapter**.

   b. In the **Script Name** field, select **sm:ServiceManagerAdapter**.

   c. Click **Next**.

7. In the **Outgoing Connection** dialog, enter the credentials (user name, password, and port number) to connect to the Service Manager server and to forward events to that server.

   a. In the **User Name** and **Password** fields, enter the Service Manager user credentials you created for the integration. See "Create user accounts for the Incident Exchange (OMi - SM) integration" on page 253.

   b. Repeat the password entry in the **Verify Password** field.

   c. In the **Port** field, enter the communications port of the Service Manager server.

      The Service Manager server configuration file (sm.ini) defines the http and http ports. Enter the http port when Service Manager is running in http mode, or enter the https port when it is running in secure http mode.

      Tip: If you click **Set default port**, the **Port** field is automatically populated with the default port (**13080** for http or **13443** for secure http). However, your actual Service Manager ports may differ from the default values.

d. If the Service Manager server uses secure http (SSL) mode, select the **Use Secure HTTP** check box. If it uses http mode, make sure the check box is not checked.

e. If the **Use Secure HTTP** check box is selected, download and install a copy of the Service Manager server's SSL certificate by clicking the link **Retrieve from Server**, or **Import from File** if the certificate is available in a local file.

f. Make sure that the **Enable Synchronize and Transfer Control** check box is checked.

When the **Enable 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 flag is not set, then the option **Synchronize and Transfer Control** does not appear in the list of forwarding types when configuring forwarding rules.

Also, note that if the **Enable 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 **Enable 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.

g. Click **Test Connection**. A **Success** or **ERROR** hyperlink appears.

If an error appears, click the link to get a more detailed message. Fix the problems and try again until the connection is successful.

h. Click **Next**.

8. If, in addition to automatically generating Service Manager incidents from OMi events, you want to also be able to drill-down into Service Manager, you need to specify the fully qualified DNS name and port of the Service Manager web application server (for example, Tomcat).

Note: To enable incident drill-down to Service Manager, you must have the Service Manager web tier deployed on a web application server.

In the **Event Drilldown** dialog box, configure the **Fully Qualified DNS Name** and **Port** of the web application server on which the Service Manager web tier is deployed.

> **Note:** If you do not specify a server in the **Event Drilldown** dialog box, it is assumed that the web tier is deployed on the same host as the Service Manager server.

If the web application server communicates with the browser over SSL (secure HTTP) , select the **Use Secure HTTP** check box.

Click **Next**.

9. The next thing to do is to enable event changes to be synchronized back from Service Manager to OMi. For this you need to provide credentials for the Service Manager server to access the OMi server in the **Incoming Connection** dialog box.

   a. Select the **Accept event changes from external processing server** check box.

   > **Note:** If **Enable Synchronize and Transfer Control** was previously selected, the **Accept event changes from external processing server** option is assumed, and cannot be disabled.

   b. Enter the password of the OMi user account that you created for the Service Manager server to access the OMi server. See "Create user accounts for the Incident Exchange (OMi - SM) integration" on page 253.

   c. Make sure the **User Name** (auto-generated) matches the one of the OMi user account you created. If not, click the **General** tab, and change the **Name** field to the correct value.

   d. Click **Finish**. The target Service Manager server now appears in the list of Connected Servers.

Add custom attributes and map to SM fields

You can add your own custom attributes in the Groovy script selected for the SM server in the Connected Servers pane, and then map these custom attributes to the appropriate fields in SM. For details about groovy scripting, see the *OMi Extensibility Guide*.

You can also change how attributes are mapped from OMi to SM. The mapping is done in the BDM Mapping Manager in SM:

System Administration > **Ongoing Maintenance** > **BDM Mapping Management**

For details about mapping attributes, see the Service Manager online help:

System Administration > **Integrations** > **Service Manager integration methods and tools** > **BDM Mapping Management**

Configure an event forwarding rule in OMi

Once you have configured the HP Service Manager server as a connected server in HP Business Service Management (BSM) Operations Management i (OMi), you need to configure an event forwarding rule for the OMi server to forward events to Service Manager.

1. Log on to Operations Manager i as a system administrator.
2. Navigate to **Administration** > **Event Processing** > **Automation** > **Event Forwarding**.
3. Click the **New Item** button.
4. In the **Display Name** field, enter a name for the rule. For example, `smserver1`.
5. Optionally, enter a description for the rule.
6. In the **Event Filter** field, click the **Manage Filters** button.

   Click **New**, and then select **New Simple Filter** or **New Advanced Filter**.

   Follow the screen prompts to configure the rule. For example, for Severity, select **Critical**.

   Click **OK**.
7. In the **Target Servers** field, select the Service Manager server you configured as a connected server, and then click the **Add** button.

   The details of the target server are displayed.
8. Click **OK**.

   The forwarding rule is displayed in the **Event Forwarding Rules** list.

Enable event drill-down from Service Manager into OMi

Before operators are able to perform event drill-down from SM into the OMi user interface using a URL launch of the Event Browser, the operators must be set up as valid users with appropriate permissions in OMi.

Note: Without valid user names, or if a user does not have the required viewing permissions, any

attempt to perform a URL launch of the OMi Event Browser from SM results in an empty browser window.

User account requirements

- If Single Sign-On (SSO) authentication is configured, set up each user in OMi with the *same* user name that is used by the SM operator to log on to SM and to perform the URL call. (The password of each OMi user can be any string, but not empty.) After successfully logging on to SM, the OMi users can launch the OMi Event Browser without further authentication.

  For details on setting up SSO, see **System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Using LW-SSO with integrations** in the SM online help.

- If SM is not configured to use SSO authentication, set up each user with the *same* user name that is used by the SM operator and specify a valid password. The users are required to enter their user name and password when launching the OMi Event Browser.

Required user permissions

You must grant the permission `Events assigned to user` including the required actions to each OMi user.

To do this, follow these steps:

1. Select **Administration** > **Users** > **Users, Groups, and Roles**.
2. Select a role or create a new one. In the Permissions section, go to the **Operations Console** category, select **Events** and specify the actions users can perform on **Events assigned to user**.
3. You can optionally grant the permission to view events not assigned to each user.

Enable incident drill-down from the OMi Event Browser

Once you have configured the HP Service Manager server as a connected server in Operations Management i (OMi), if you want to be able to drill down to Service Manager incidents from the OMi Event Browser, you need to perform the following tasks.

Task 1. Configure the Service Manager web tier in the sm:ServiceManagerAdapter script in OMi

To do this, follow these steps:

1. Log on to Operations Manager i as a system administrator.
2. Navigate to **Administration** > **Setup and Maintenance** > **Connected Servers**.
3. Click the **Manage Scripts** icon in the toolbar.
4. Click the **sm:ServiceManagerAdapter** script, and then click the **Edit** icon.
5. On the **Script** tab, locate the following string in the script:

   private static final String SM_WEB_TIER_NAME
6. Change the value of this parameter to the name of your Service Manager web tier. For example, if your web tier file name is **sm-9.xx.war**, change the parameter value to:

   ```
   private static final String SM_WEB_TIER_NAME = 'sm-9.xx'
   ```
7. Click **OK** to save the script.

Task 2. Set the queryhashcode parameter in the Service Manager server configuration file

To do this, follow these steps:

1. Stop the Service Manager server.
2. Add the following parameter to the server configuration file (sm.ini):

   ```
   queryhashcode:<host>:<port>
   ```

   Where: <host>:<port> must be same as the Service Manager host name and port number that are configured in the Service Manager web tier configuration file (web.xml).
3. Restart the Service Manager server.

Configure SSL for the Incident Exchange (OMi – SM) integration

Applies to User Roles:

System Administrator

When Operations Manager i (OMi) is configured to accept https connections only, you must configure SSL for the integration. If you do not do so, changes on an incident that is created from OMi cannot be synchronized back to OMi.

Note: The following steps describe how you do so by using the built-in keytool in Service Manager, and the file paths are for Windows only. Be sure to change the file paths accordingly if your Service Manager system is running on Unix.

To configure SSL for the integration, follow these steps:

1. Import the OMi root certificate to the Service Manager server trusted keystore.

   The following is an example of the command line:

   ```
   <SM Install path>\server\RUN\jre\bin\keytool -import -alias myCA -file <.pem file of your BSM root certificate> -keystore <SM Install path>\Server\RUN\jre\lib\security\cacerts -storepass <changeit>
   ```

   Where: *changeit* is the default password of the trusted keystore. Change it to your own password if you changed it previously.

2. Add the following parameters to the Service Manager server configuration file (<*SM install path*>\Server\RUN\sm.ini):

   ```
   truststoreFile:<SM install path>\Server\RUN\jre\lib\security\cacerts

   truststorePass:<changeit>
   ```

3. Restart the Service Manager Server service.

Configure the Instance Count in the SMOMi integration template

Applies to User Roles:

System Administrator

As of version 9.34, HP Service Manager can integrate with more than one Operations Manager i (OMi) server. However, by default, only one OMi server is allowed. If you need to integrate Service Manager with more than one OMi server, you need to configure the Instance Count setting in the SMOMi integration template, as described below.

1. Log on to Service Manager as a system administrator.
2. Type `db` in the command line, and press Enter.
3. In the **Table** field, type `SMISRegistry`, and click **Search**.

The SMIS integration template form opens.

4. Click **Search**.

   A list of SMIS integration templates opens.

5. Select **SMOMi** from the list.

6. In the **Instance Count** field, change the value of 1 to the number of OMi servers that you want to integrate with Service Manager. For example, if you need two OMi servers, change the value to `2`.

7. Click **Save**.

Add an integration instance for each OMi server

Applies to User Roles:

System Administrator

Once you have completed your configuration in Operations Manager i (OMi), and have changed the Instance Count setting in the SMOMi integration template (which is needed only when you have multiple OMi servers), you are ready to add and enable a separate integration instance in Service Manager for each OMi server. For example, if you have two OMi servers, you must configure two SMOMi integration instances.

Support of multiple OMi servers

As of version 9.34, Service Manager can integrate with multiple OMi servers. This is implemented through the Instance Count setting and the **omi.mgr.id** parameter in the SMOMi integration template.

By default, the SMOMi integration template supports only one integration instance. If you have multiple OMi servers, before you proceed, make sure you have already updated the Instance Count setting in the SMOMi integration template. For details, see "Configure the Instance Count in the SMOMi integration template" on the previous page.

When using the **omi.mgr.id** parameter, keep the following in mind:

- If you have only one OMi server (and hence need only one SMOMi integration instance), you must either correctly configure this parameter or clear the entire row of this parameter (both the parameter name and value) in the SMOMi integration instance, otherwise the integration will not work.

- If you have multiple OMi servers (and hence need multiple SMOMi integration instances), you must correctly configure this parameter in all SMOMi integration instances. Only those correctly configured integration instances will work. If none of the SMOMi integration instances are correctly configured, none of them will work.
- Users can view the OMi event details from an OMi incident record only when you specify the **omi.mgr.id** parameter correctly. If the value you specify in the corresponding SMOMi integration instance does not match the Universally Unique Identifier (UUID) which is automatically generated in the OMi server for the target Service Manager server and stored in the Incident record, users will not see the **View OMi Event** option from the Incident record.

To add and enable an Incident Exchange (OMi - SM) integration instance:

1. Log on to Service Manager as a system administrator.
2. Click **Tailoring** > **Integration Manager**.
3. Click **Add**.

   The Integration Template Selection wizard opens.
4. Select **SMOMi** from the Integration Template list.

   Note: Ignore the **Import Mapping** check box, which has no effect on this integration.
5. Click **Next**.
6. Complete the integration instance information:
   - Modify the **Name** and **Version** fields to the exact values you need.
   - In the **Interval Time (s)** field, enter a value. For example: `600`. If an OMi opened incident fails to be synchronized back to OMi, Service Manager will retry the failed task at the specified interval (for example, 600 seconds).
   - In the **Max Retry Times** field, enter a value. For example: `10`. This is the maximum allowed number of retries for each failed task.
   - (Optional) In the **SM Server** field, specify a display name for the Service Manager server host. For example: my_Local_SM.

- (Optional) In the **Endpoint Server** field, specify a display name for the BSM server host. For example: my_BSM_1.
- (Optional) In the **Log File Directory** field, specify a directory where log files of the integration will be stored. This must be a directory that already exists on the Service Manager server host.
- (Optional) In the **Log Level** field, change the log level from INFO (default) to another level. For example: **WARNING**.
- (Optional) If you want this integration instance to be automatically enabled when the Service Manager Server service is started, select **Run at system startup**.

7. Click **Next**. The Integration Instance Parameters page opens.
8. On the **General Parameters** tab, complete the following fields as necessary:

Field	Sample Value	Description
omi.server.url	http://<servername>:opr-gateway/rest/synchronization/event	This is the URL address of the OMi server's RESTful web service. Replace <servername> with the fully qualified domain name of your OMi server.
http.conn.timeout	30	The HTTP connection timeout setting in seconds. **Note:** The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.
http.rec.timeout	30	The HTTP receive timeout setting in seconds. **Note:** The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.
http.send.timeout	30	The HTTP send timeout setting in seconds. **Note:** The out-of-box

Field	Sample Value	Description
		value is 30 (seconds), and 15 (seconds) is used if this field is empty.
sm.mgr.id	55436DBE-F81E-4799-BA05-65DE9404343B	The Universally Unique Identifier (UUID) automatically generated for this instance of Service Manager. **Note:** This field is automatically completed each time when you add an SMOMi integration instance. Do not change it, otherwise the integration will not work properly.
omi.reference.prefix	urn:x-hp:2009:opr:	The prefix of the BDM External Process Reference field, which will be present in incoming synchronization requests from the OMi server. **Note:** This field is automatically completed and has a fixed value. Do not change it.
sm.reference.prefix	urn:x-hp:2009:sm:	The prefix of the BDM External Process Reference field, which will be present in outgoing synchronization requests from Service Manager. **Note:** This field is automatically completed and has a fixed value. Do not change it.
omi.eventdetail.baseurl	http://<servername>/opr-console/opr-evt-details.jsp?eventId=	The basic URL address of the event detail page in OMi. Replace <servername> with

Field	Sample Value	Description
		the fully qualified domain name of your OMi server.

9. On the **General Parameters** and **Secure Parameters** tabs, enter three parameter values that you specified when configuring the Service Manager server as a connected server in BSM OMi. The following table lists the parameters, whose values you can copy from your BSM OMi server.

   To copy the parameter values from BSM OMi, follow these steps:

   a. Log on to BSM as a system administrator.

   b. Navigate to **Admin** > **Operations Management** > **Setup** > **Connected Servers**.

   c. Locate your Service Manager server configuration entry and double-click anywhere on the entry pane.

   d. On the **General** tab, copy the **ID** string at the bottom into the **omi.mgr.id** field in Service Manager.

   e. On the **Incoming Connection** tab, copy the **User Name** and **Password** to the **username** and **Password** fields in Service Manager, respectively.

Field	Sample Value	Description
omi.mgr.id (on the **General Parameters** tab)	f3832ff4-a6b9-4228-9fed-b79105afa3e4	The 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. **Tip:** If you have only one OMi server, you can simply remove this parameter (remove both the parameter name and value) from the integration instance. See "Support of

Field	Sample Value	Description
		multiple OMi servers" on page 262.
username omi.mgr.id (on the **General Parameters** tab)	SM_Server	This is the user name that the Service Manager server uses to synchronize incident changes back to the OMi server.
Password (on the **Secure Parameters** tab)	SM_Server_ Password	This is the password that the Service Manager server uses to synchronize incident changes back to the OMi server.

10. Click **Verify Connection**.

    If everything is fine, the following message is displayed: `Verification succeeded`.

11. Click **Next** twice, and then click **Finish**.

    Note: Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

    Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

12. Enable the integration instance.

13. If you have multiple OMi servers, repeat the steps above for the rest of your OMi servers.

Next, you can optionally enable Lightweight Single Sign-On (LW-SSO) in both OMi and Service Manager so that users can bypass the log-in prompts. For details, see "Enable LW-SSO for the Incident Exchange (OMi - SM) integration" below.

Enable LW-SSO for the Incident Exchange (OMi - SM) integration

Applies to User Roles:

System Administrator

Lightweight Single Sign-On (LW-SSO) is optional but recommended for the Incident Exchange (OMi - SM) integration. You have different LW-SSO configuration choices depending on your needs. The following describes how LW-SSO can be used in the Incident Exchange (OMi - SM) integration workflow.

When OMi creates an incident from an OMi event record

OMi creates an incident from an OMi event record by sending RESTful-based requests to Service Manager. The incident ID is then stored in the event record.

LW-SSO is NOT needed in this process. A dedicated Service Manager user account was specified when configuring the Service Manager integration in OMi. OMi uses this dedicated user account when calling the Service Manager RESTful Web Service to create the incident.

When an OMi user views the incident details

The user can log in to Service Manager and view the incident details using the incident ID stored in the event record.

If the user wants to view the incident details by clicking the incident link from the event record, LW-SSO can be used; otherwise a Service Manager login prompt will appear.

LW-SSO is optional for this process. To enable LW-SSO for this process, configure LW-SSO in both the Service Manager server and Web tier (because the server needs to trust the Web tier), as well as in OMi.

When Service Manager synchronizes the OMi incident status back to OMi

When a user has updated the OMi incident, Service Manager calls the OMi server's RESTful Web Service to update the incident changes to the OMi event record.

LW-SSO is NOT needed in this process. A dedicated OMi user account was specified when the Incident Exchange (OMi - SM) integration was set up in SMIS, and Service Manager uses this user account when calling the OMi server's RESTful Web Service to synchronize the incident status back to the OMi event record.

When a user views the event details from the OMi incident

The user clicks the **View OMi Event** option from the incident to view the event details.

LW-SSO is optional for this process. If you enable LW-SSO in the Service Manager Web tier and in OMi, the OMi login prompt is bypassed.

Configure automatic closure for OMi incidents

Applies to User Roles: System Administrator

OMi incidents can be automatically closed after a predefined amount of time since they were last updated (or resolved if they have not been updated after being resolved).

The workflow is as follows:

1. An incident is opened from OMi.
2. If the **Schedule Condition** is met, the system creates a schedule record for the incident. The schedule record will expire at a future time based on the **Calc Expression**.
3. A user updates the incident and saves the changes.
4. The **Reset alerts if** expression on the **Alerts** tab of the **probsummary** object definition is evaluated. If it evaluates to true, the Expiration time of the schedule record is updated based on the Calc Expression. By default, the expiration time of the schedule record is updated only when the incident has a category of **incident**.
5. When the schedule record expires, the **Alert Condition** is evaluated. If it evaluates to true, the incident is automatically closed.

To enable automatic closure for OMi incidents:

1. Configure the global settings in the Incident Management Environment record.
   a. Click **System Administration** > **Ongoing Maintenance** > **Environment Records** > **Incident Management Environment**.

   b. Change the following settings as necessary.

Field	Value
Close Incident Automatically?	This option disables or enables the automatic closure of OMi incidents at the global level. • If this option is not selected, no incidents will be automatically closed. • If this option is selected, incidents will be automatically closed under specified conditions. Default: Not selected

Field	Value
Closure Code	This value will be copied to the **Closure Code** field of incidents when they are automatically closed. Default: Automatically Closed
Solution	This description will be appended to the end of the **Solution** field of incidents when they are automatically closed. Default: This incident which belongs to OMi has been closed automatically.

c. lick **Save**.

d. Restart the Service Manager server.

> **Note:** If you have made any changes to any of the configuration options in the Incident Management Environment record, the Service Manager server must be restarted for the changes to take effect.

2. Configure the alert definition that determines when an incident should be closed.

> **Note:** The **alert** and **problem** processes must be running to enable the successful closure of OMi incidents.

a. Click **Tailoring** > **Document Engine** > **Alerts**.

b. In the Alert Name field, enter: **OMI Auto-Close**.

c. Click **Search**. The OMI Auto-Close alert definition detail form opens.

> **Caution:** These fields in the alert definition are used to control automatic closure of OMi incidents. You can change the default values of these fields. However, you must be aware of the risk that automatic closure of OMi incidents will not work properly if the **Schedule Condition** and **Alert Condition** fields are not configured correctly.

Field	Value
Schedule Condition	This expression is used to determine if an incident should be scheduled for automatic closure. Default: `jscall("SMOMi.isAutoCloseAndResolved")`. An incident is scheduled for automatic closure when the following conditions

Field	Value
	are met. • The **Close Incident Automatically?** option in the Incident Management Environment record is selected. • In the incident record, the **Do not close this incident automatically** option is not selected. • The incident has a status of **Resolved**.
Alert Condition	This expression is evaluated when an incident is about to be automatically closed. If it evaluates to true, the incident is closed. Default: `jscall("SMOMi.isAutoCloseEnabled")`. An incident is closed when the following conditions are met. • The **Close Incident Automatically?** option in the Incident Management Environment record is selected. • In the incident record, the **Do not close this incident automatically** option is not selected.
Calc Expression	This expression is used to determine how much time will elapse before an incident is automatically closed. Default: `$L.alert.time=update.time in $L.file+'7 00:00:00'`. The default value means the amount of time elapsed is equal to seven days since the incident was last updated.

3. Configure alert information in the **probsummary** object.
   The OMi autoclose alert definition is configured to only be used by OMi incidents. The closure time is reset each time the incident is updated. If the closure time is reached without the incident being updated then Service Manager will automatically close the incident.

   a. Click **Tailoring** > **Document Engine** > **Objects**.

   b. In the **File name** field, enter **probsummary** and press ENTER. The **probsummary** object definition is displayed.

   c. Select the **Alerts** tab.

      The **Reset alerts if** expression is used to reset the automatic closure time of OMi incidents.

Default: `category in $L.file="incident" and not null(1 in external.process.reference in $L.file)`.

Change the default assignment group for OMi incidents

Applies to User Roles:

System Administrator

HP Service Manager can accept REST based requests from Operations Manager i (OMi) to create incidents based on events information in OMi. An incident opened from an OMi event is automatically assigned to an existing group based on the following field values, listed from the highest to lowest priority:

- The **Affected Service** of the incident
- The **Category** of the incident
- The **Affected CI** of the incident

However, if none of the above field values is available, the incident is assigned to a default group named **Application**. If necessary, you can change this default group setting as follows:

1. Navigate to **System Administration** > **Ongoing Maintenance** > **BDM Mapping Management**. The BDM mapping configuration search page opens.
2. Enter **incident** in the BDM Name field, select **1.1** in the **Version** field, and then click **Search**. The BDM mapping record **incident** is displayed. The Incident Exchange (OMi - SM) integration uses this BDM mapping record when creating an incident from an OMi event.
3. Select the **Field Mapping** tab, scroll down to the **assignment** field in the SM Object Field column, and click the **SM Callback** field in the same row.
4. Change **Application** in the following code to the name of another assignment group:

```
4)  A default assignment group if no other criteria is met
       if( ! $result ) {
              $result = "Application";
       }
```

5. Click **Save**. The default assignment group is now changed.

Test the connection

To test the connection, send an event to the server hosting OMi that matches the filter you defined (in our example filter, the severity value is `Critical`), and then verify that the event is forwarded to SM as expected.

To test the connection, do the following:

1. On the Gateway Server system running OMi, open an Event Browser.
2. On the system running OMi, open a command prompt and change to the following directory:

   `<OMi_HOME>\opr\support`

3. Send an event using the following command:

   `sendevent -s critical -t test111-1`

4. Verify that the event appears in the OMi Event Browser.
5. Select the **Forwarding** tab.
6. In the External Id field, you should see a valid SM incident ID.
7. Verify that the incident appears in the Incident Management in Service Manager:

   If the event drill-down connection is configured correctly, click the hyperlink created with the incident ID. A browser window opens, which takes you directly to the incident in HP Service Manager.

   If the event drill-down connection is not configured, do the following:

   a. In the Forwarding tab in the OMi Event Browser, copy or note the incident ID from the External Id field.

   b. In the HP Service Manager user interface, navigate to:

      Incident Management > Search Incidents

   c. Paste or enter the incident ID in the Incident Id field.

   d. Click the **Search** button. This takes you to the incident in the Incident Details.

8. Close the incident in HP Service Manager.
9. Verify that the change in the state of the incident (it is now `closed`) is synchronized back to OMi. You should not be able to see the event that was closed in SM in the active Event Browser, but it should now be in the History Browser.

Synchronize attributes

Not all attributes are synchronized back from SM to OMi by default. When the SM incident is initially created from an OMi event, event attributes are mapped to the corresponding SM incident attribute. Out of the box, after the initial incident creation, whenever the incident or event subsequently changes, only a subset of the changed event and incident attributes are synchronized. The following describes how to customize the list of attributes to synchronize upon change.

Unidirectional synchronization: OMi to SM

The following attributes are transferred to SM from OMi on a one-time basis, that is, when the event was initially created, and the transfer of control of the event was configured in the Connected Servers manager.

These attributes support bidirectional synchronization, but are disabled out-of-box:

- Title
- Severity
- Priority
- Operator: the operator assigned to the event who forwarded the event
- Category
- Subcategory
- Related CI

OMi event annotations are synchronized to SM activity log and there is no back synchronization from SM to OMi.

Bidirectional synchronization

Attributes that support bidirectional synchronization between OMi and SM are:

- Description
- Lifecycle state (the state is only updated when the state changes to closed)
- Solution
- Contents under the Forwarding tab in the Event Details

Attribute synchronization using Groovy scripts

If you want to change the out-of-the-box behavior regarding which attributes are updated, you can specify this in the Groovy script used on the OMi side for synchronization or incident creation. In the Groovy script, you can specify which fields are updated in SM, and which fields are updated in OMi. You can also specify custom attributes in the Groovy script.

For more information, see "Tips for customizing groovy scripts" below.

Tips for customizing groovy scripts

This section provides some tips about customizing Groovy scripts. It contains a few selected examples of what you can customize. To see further items that can be modified, see the configuration section of a Groovy script.

In the configuration section of the Groovy script, you can define and modify the attributes that are to be synchronized between OMi and SM. The configuration section of the Groovy script also contains the default value mappings for lifecycle state, severity, and priority. You can also modify these, and it is possible to define the mappings for in-going and out-going requests differently.

More advanced configuration can be done in other parts of the Groovy script if required.

The beginning and the end of the configuration section of the Groovy script is marked as follows:

```
//
// configuration section to customize the Groovy script
// BEGIN
...
...
//
// configuration section to customize the Groovy script
// END
```

Note: Modifications to Groovy scripts are not overwritten by patches and hotfixes. Your customized version of a script will remain after an update or a patch. If you want to use the newer version of a script, make a copy of your version, revert back to the predefined version, and then reapply your changes.

The mapping from OMi to SM is compliant to BDM 1.1 incident web service specifications. The mapping of the BDM 1.1 incident web service to SM is specified in SM in the BDM Mapping Manager. For more information about the BDM Mapping Manager, see the BDM Mapping Manager section of the HP Service Manager online help.

Controlling attribute synchronization

You can control how updates to certain attributes are synchronized between OMi and SM by setting some Boolean variables to `true` or `false`.

Examples:

- `SyncAllProperties` variable. By default, it is `false`. If you set it to `true`, all properties will be synchronized in both directions. The other variables will be ignored.
- `private static final SyncTitleToSMOnUpdate = false;`

  This line of the Groovy script disables the synchronization of changes to the title made in OMi to SM.
- `private static final Boolean SyncTitleToOPROnUpdate = false;`

  This line of the Groovy script disables the synchronization changes to the title made in SM to OMi.

The title is a required attribute in SM, and it is set, independently of the flags above, using the title given in OMi during the creation of the incident.

Mapping OPR Lifecycle States to BDM Lifecycle States

Individual OPR event state and SM incident status changes may be selected for synchronization. Out of the box, only the "closed" state is synchronized in both directions. To change this behavior, add the desired states to the appropriate list, `SyncOPRStatesToSM` or `SyncSMStatusToOPR` .

Examples:

- `private static final Set SyncOPRStatesToSM = ["closed", "in_progress", "resolved"]`
- `private static final Set SyncSMStatusToOPR = ["closed", "resolved"]`

In the example, the OPR event lifecycle states `closed`, `in_progress`, and `resolved` are synchronized to the SM incident status, and SM incident statuses `closed` and `resolved` are synchronized to the OPR event state.

Note: The special state `"*"` denotes all states, so to synchronize all OPR event states to the SM incident status property, specify the following:

```
private static final Set SyncOPRStatesToSM = ["*"]
```

Additionally, two maps are used to specify the mapping of the OPR event lifecycle state to the BDM incident status. The maps are named `MapOPR2SMStatus` and `MapSM2OPRState`. Out of the box, all possible states have a mapping.

Examples:

- `private static final Map MapOPR2SMStatus = ["open": "open", "in_progress": "work-in-progress", "resolved": "resolved", "closed": "closed"]`
- `private static final Map MapSM2OPRState = ["accepted": "open", "assigned": "open", "open": "open", "reopened": "open",`

  `"pending-change": "in_progress", "pending-customer": "in_progress", "pending-other": "in_progress",`

  `"pending-vendor": "in_progress", "referred": "in_progress", "suspended": "in_progress",`

  `"work-in-progress": "in_progress", "rejected": "resolved", "replaced-problem": "resolved",`

  `"resolved": "resolved", "cancelled": "resolved", "closed": "closed"]`

Avoiding Errors with Large TQL Queries

If the Groovy script executes a TQL query that produces a large number of results, an error message appears informing you about the TQL query result exceeding the size limit. As a consequence, the integration event is not sent. It is possible, however, to increase this limit by modifying the value of the `tql.compound.link.max.visited.objects` setting.

Note: To check the default value of the `tql.compound.link.max.visited.objects` setting, from the JMX console, select **UCMDB:service=Settings Services**, and then locate the

showSettingsByCategory method and enter **TQL Settings** as the category name.

To modify the value of the `tql.compound.link.max.visited.objects` setting, follow these steps:

1. From the JMX console, select **UCMDB:service=Settings Services**.
2. Click **setSettingValue**.
3. Enter `tql.compound.link.max.visited.objects` as the name of the setting you want to modify and a new value for it.

Caution: Increasing the value of the `tql.compound.link.max.visited.objects` setting also increases the load on the RTSM. Therefore, make sure to carefully consider how much to increase this value.

Syntax Errors

If you get a syntax error when customizing your Groovy scripts, you will get an event in the event browser with a detailed description of the error. In addition, you may view the `opr-event-sync-adapter.log` log file for information about how to resolve the error. You can find this log file at the following location:

`<Gateway Server root directory>/log/opr-event-sync-adapter.log`

Synchronization of incident changes back to Operations Manager i (OMi)

After OMi opens an incident in HP Service Manager, Service Manager will synchronize the incident changes back to OMi.

Operations Manager i (OMi) can forward an event record to Service Manager as an incident by calling a Service Manager Web Service. The incident ID is then stored in the event record.

When a user has updated the incident opened from OMi, Service Manager calls an OMi server RESTful Web Service to update the incident changes to the OMi event record.

If Service Manager fails to synchronize the incident changes back to OMi for some reasons (for example, because of a network problem), Service Manager behaves as follows:

- Displays a warning message, indicating that the incident failed to be synchronized to OMi.
- Saves the failed task in the SMIS task queue, and retries the task to re-synchronize the changes to OMi based on an interval time and a maximum retry times configured when adding the Incident Exchange (OMi - SM) integration in SMIS. When the re-synchronization is successfully completed, the failed task is removed from the task queue.

System Administrators can monitor failed tasks, and reset their retry times or rerun expired tasks. For more information, see "Monitor failover tasks" on page 90.

Working with the Incident Exchange (OMi - SM) integration

Once the integration is set up, Service Manager Incident Management users with the right permissions can view event details from OMi incidents and mark individual OMi incidents as eligible or ineligible for automatic closure (if their system administrator has enabled automatic closure for OMi incidents).

Drill down to the OMi event details from an incident

If all of the following conditions are met, you can view the related Operations Manager i (OMi) event details from an OMi incident:

- You are accessing the incident through the HP Service Manager standard Web client (not the employee self-service (ESS) interface).
- One or more SMOMi integration instances are set up and enabled in Integration Manager.
- You are also an OMi user who has been granted the permission **Events assigned to user** including the required actions.

To drill down to the OMi event details from an OMi incident, follow these steps:

1. Log on to the Service Manager Web client.
2. From **Incident Management**, search for the incident record created from OMi.
3. Click **More** and then select **View OMi Event**.

> **Note:** The **View OMi Event** option is displayed only when the **omi.mgr.id** parameter in the corresponding SMOMi integration instance is set correctly.

If Lightweight Single Sign-On (LW-SSO) is enabled in both the Service Manager Web client and OMi , the OMi event detail page opens in a new browser window, displaying the details of the related event in OMi. If LW-SSO is not enabled, an OMi login page opens, and the related OMi event detail page is displayed after you log on to OMi.

Mark an incident for automatic closure

Applies to User Roles:

Incident Coordinator

You can mark an OMi incident as eligible or ineligible for automatic closure after a predefined amount of time since it was last updated.

To mark an incident as ineligible or eligible for automatic closure:

1. From **Incident Management**, search for an incident record opened from OMi.
2. Select or deselect the **Do not close this incident automatically** check box to mark this incident as ineligible or eligible for automatic closure.

Note: By default, this check box is not selected.

Downtime Exchange between OMi and Service Manager

Operations Manager i (OMi) enables you to forward downtimes (also known as outages) from OMi to Service Manager (SM), and from SM to OMi. The downtime defined in OMi is converted to an incident in SM, and vice versa.

Integration Overview

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

- **SM > OMi.** When you create a downtime RfC (request for change) in SM, the RfC includes the CI that is under change and a start and end date/time of the downtime. If you do not want to waste effort 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 a data flow probe on the CMDB:

  - If you use OMi's RTSM as CMDB, install the data flow probe provided on the OMi installation media.
  - If you use UCMDB as CMDB, install the data flow probe as described in the UCMDB documentation. In this case, the synchronization must also be done from UCMDB to OMi, additionally to synchronizing SM with UCMDB. The RfC creates a planned downtime CI in the CMDB, and the data flow probe DFP1 sends the planned downtime CI to OMi to create a downtime.

- **OMi > SM.** When you define downtimes using OMi , the help desk should be aware of such operational downtimes: After you set up the integration, downtimes in OMi trigger events, which create corresponding incidents in SM.

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

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

Prerequisites

Supported Platforms

To set up the downtime integration, you must meet the following prerequisites:

- Service Manager 9.31 and higher.
- UCMDB 10.01 or higher with content pack 12 or higher.
- Before deploying the adapter, verify that CP11 or higher is installed. If it is not, install the content pack.
- If the adapter is installed on the RTSM, and the adapter is working behind a reverse proxy, the DPS must have the correct certificates installed to send requests to the reverse proxy.

If you are using a UCMDB as a CMS, make sure that the CMS integration is set up. When it is set up, it serves as the global ID generator.

Global ID Generator

If you are using OMi's RTSM you need to configure the RTSM to be the global ID generator, to enable the downtime integration:

1. Access the following location with your browser: http://<DPS name>:21212/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Multiple CMDB Instances Services
2. In the **setAsGlobalIdGenerator()** method, fill the **customerID** parameter with the value of **1**, and click **Invoke**.

Step 1: Send OMi Downtime Events to SM

To enable OMi to send downtime definitions to SM, follow these steps:

1. Access the following location in OMi:

   Administration > Setup and Maintenance > Infrastructure Settings > Foundations > Downtime
2. Change the value of the **Downtime Send Event** parameter to **true**.
3. Restart your OMi services on all Gateway Servers and Data Processing Servers.

This procedure generates events in OMi. After performing it, make sure you edit and enable the **Automatically forward "downtime started" and "downtime ended" events to Trouble Ticket System** event forwarding rule to forward downtime-start and downtime-end events to the SM server that should be specified in the alias connected server called "Trouble Ticket System". For details on event forwarding and connected servers, see *[[[Undefined variable OMi.Admin Guide]]]*.

Downtime events use the following formats:

- **Downtime Start**

Event field	OMi Downtime
Severity	Normal
Category	Downtime Notification

Event field	OMi Downtime
Title	Downtime for <CI Type><Affected CI Name>started at <Downtime Start Time>
Key	<OMi Downtime ID>:<Affected CI ID>:downtime-start
SubmitCloseKey	False
OutageStartTime	<Downtime Start Time>
OutageEndTime	<Downtime End Time>
CiName	<Affected CI Name>
CiId	<Affected CI Global ID>
CiHint	GUCMDB:<Affected CI Global ID>|UCMDB:<Affected CI ID>
HostHint	GUCMDB:<Related Host Global ID>|UCMDB:<Related Host ID>
EtiHint	downtime:start

- **Downtime End**

Event field	OMi Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name> ended at < Downtime End Time>
Key	<OMi Downtime ID>:<Affected CI ID>:downtime-stop
SubmitCloseKey	true
CloseKeyPattern	<OMi Downtime ID>:<Affected CI ID>:downtime-start
EtiHint	downtime:end
LogOnly	true

Step 2: Integrate SM Downtimes with OMi

To enable downtimes defined in SM to be sent to OMi, again, you need to distinguish between the two cases of where the CMDB is:

If you are using OMi's RTSM as CMDB, no further steps are required. See also "Point to point integration" on page 247.

If you are using an external UCMDB, you need to install the DFP2 in the OMi deployment. See also "Integration using a Universal Configuration Management Database (UCMDB)" on page 248

Important:

- Following the initial integration, a large amount of data may be communicated from SM to OMi. It is highly recommended that you perform this procedure during off-hours, to prevent negative impact on system performance.
- The integration consists of two parts: SM > CMS/UCMDB, and CMS/UCMDB > OMi adapter. 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 > CMSUCMDB part, and then wait a long time before setting up the CMS/UCMDB > OMi adapter part, the number of downtimes communicated to OMi initially may be extremely high.

Note:

- The following procedure does not describe the SM > CMS/UCMDB connection setup. SM should be configured to create its CIs in the CMS. This procedure connects the adapter between the CMS/UCMDB and OMi.
- The default job synch frequency is one minute.

Create a new integration point as follows:

1. Create the integration point credentials:

   If you use OMi's [[[Undefined variable OMi.RTSM short]]], do the following on your OMi. If you use a CMS, do the following on the UCMDB that fulfills the role of your CMS: Access the Data Flow Probe Setup:

   a. (missing or bad snippet)

      Note: You do not need a probe to perform this integration. Nevertheless you create credentials using the Data Flow Probe Setup tab.

   b. Click **Add domain or probe**, and enter a name and description of your choice.

   c. Expand the submenus and select **HTTP protocol**.

   d. Click the **+** sign (**Add new connection details**) and enter the OMi Gateway host name, Port 80,

and the OMi username and password. Leave the **Trust** fields blank. When you are done, click **OK** to save the credentials.

2. Create a new integration point:

   a. If you have OMi, do the following on your OMi. If you use a CMS, do the following on your CMS:

      Navigate to **Administration** > **RTSM Administration** > **Data Flow Management** > **Integration Studio**

   b. Click **New Integration Point**, enter a name and description of your choice, and select **BSMDowntimeAdapter/SM scheduled Downtime Integration into BSM**.

   c. Enter the following information for the adapter: OMi Gateway hostname and port, the integration point credentials you just created, communication protocol, and the context root (if you have a non-default context root).

   d. Click **OK**, then click the **Save** button above the list of the integration points.

3. You can 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, you can 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 error 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 the problem is fixed.

Downtime Exchange integration setup

To set up the downtime exchange integration between Operations Manager i (OMi) and Service Manager (SM), you need to perform the following tasks.

1. "Enable OMi to send downtime events to Service Manager" on the next page.
2. "Integrate Service Manager downtimes with OMi" on page 287.
3. "Add an integration instance in Service Manager " on page 289.

4. "Tailor Service Manager to handle phase change" on page 292.

5. "Verify the OMi-SM downtime synchronization setup" on page 293.

Enable OMi to send downtime events to Service Manager

Downtime events use the formats listed in the following tables.

Downtime Start

Event field	OMi Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name>started at <Downtime Start Time>
Key	<OMi Downtime ID>:<Affected CI ID>:downtime-start
SubmitCloseKey	False
OutageStartTime	<Downtime Start Time>
OutageEndTime	<Downtime End Time>
CiName	<Affected CI Name>
CiId	<Affected CI Global ID>
CiHint	GUCMDB:<Affected CI Global ID>|UCMDB:<Affected CI ID>
HostHint	GUCMDB:<Related Host Global ID>|UCMDB:<Related Host ID>
EtiHint	downtime:start

Downtime End

Event field	OMi Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name> ended at < Downtime End Time>
Key	<OMi Downtime ID>:<Affected CI ID>:downtime-stop
SubmitCloseKey	true

Event field	OMi Downtime
CloseKeyPattern	<OMi Downtime ID>:<Affected CI ID>:downtime-start
EtiHint	downtime:end
LogOnly	true

To enable OMi to send downtime definitions to Service Manager (SM), follow these steps:

1. Access the following location in OMi:

   Administration > Setup and Maintenance > Infrastructure Settings > Foundations > Downtime

2. Change the value of the **Downtime Send Event** parameter to **true**.

3. Restart your OMi services on all Gateway Servers and Data Processing Servers.

This procedure generates events in OMi. After performing it, make sure you edit and enable the **Automatically forward "downtime started" and "downtime ended" events to Trouble Ticket System** event forwarding rule to forward downtime-start and downtime-end events to the SM server that should be specified in the alias connected server called "Trouble Ticket System". For details on event forwarding and connected servers, see the *OMi Administration Guide*.

Integrate Service Manager downtimes with OMi

To enable downtimes defined in SM to be sent to OMi, again, you need to distinguish between the two cases of where the CMDB is:

If you are using OMi's RTSM as CMDB, no further steps are required. See also "Point to point integration" on page 247.

If you are using an external UCMDB, you need to install the DFP2 in the OMi deployment. See also "Integration using a Universal Configuration Management Database (UCMDB)" on page 248

Important:

- Following the initial integration, a large amount of data may be communicated from SM to OMi. It is highly recommended that you perform this procedure during off-hours, to prevent negative impact on system performance.

- The integration consists of two parts: SM > CMS/UCMDB, and CMS/UCMDB > OMi adapter. 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/UCMDB part, and then wait a long time before setting

up the CMS/UCMDB > OMi adapter part, the number of downtimes communicated to OMi initially may be extremely high.

Note:

- The following procedure does not describe the SM > CMS/UCMDB connection setup. SM should be configured to create its CIs in the CMS. This procedure connects the adapter between the CMS/UCMDB and OMi.
- The default job synch frequency is one minute.

Create a new integration point as follows:

1. Create the integration point credentials:

   If you use OMi's [[[Undefined variable OMi.RTSM short]]], do the following on your OMi. If you use a CMS, do the following on the UCMDB that fulfills the role of your CMS: Access the Data Flow Probe Setup:

   a. (missing or bad snippet)

   Note: You do not need a probe to perform this integration. Nevertheless you create credentials using the Data Flow Probe Setup tab.

   b. Click **Add domain or probe**, and enter a name and description of your choice.

   c. Expand the submenus and select **HTTP protocol**.

   d. Click the **+** sign (**Add new connection details**) and enter the OMi Gateway host name, Port 80, and the OMi username and password. Leave the **Trust** fields blank. When you are done, click **OK** to save the credentials.

2. Create a new integration point:

   If you have OMi, do the following on your OMi. If you use a CMS, do the following on your CMS: Access the Integration Studio:

   a. (missing or bad snippet)

   b. Click **New Integration Point**, enter a name and description of your choice, and select **BSMDowntimeAdapter/SM scheduled Downtime Integration into BSM**.

   c. Enter the following information for the adapter: OMi Gateway hostname and port, the

integration point credentials you just created, communication protocol, and the context root (if you have a non-default context root).

d. Click **OK**, then click the **Save** button above the list of the integration points.

3. You can 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, you can 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 error 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 the problem is fixed.

Add an integration instance in Service Manager

Applies to User Roles:

System Administrator

To set up the downtime exchange integration, you must add an instance of this integration in the Service Manager Integration Suite (SMIS).

To add the SMBSM_DOWNTIME instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The Integration Template Selection wizard opens.
3. Select **SMBSM_DOWNTIME** from the Integration Template list. Ignore the **Import Mapping** check box, which has no effect on this integration.
4. Click **Next**. The Integration Instance Information page opens.
5. Do the following:
   - Modify the **Name** and **Version** fields to the exact values you need.

- In the **Interval Time(s)** field, enter a value based on your business needs in regard to downtime exchange frequency. Note that a short interval time can be safe because the next scheduled task will not start until the previous task is completed and the interval time passed.
- In the **Max Retry Times** field, enter a value. This is the maximum allowed number of retries (for example, 10) for each failed task.
- In the **Log File Directory** field, specify a directory where log files of the integration will be stored. This must be a directory that already exists on the Service Manager server. By default, logging message is output to `sm.log`.
- (Optional) In the **SM Server** field, specify a display name for the Service Manager server host. For example: my_local_SM.
- (Optional) In the **Endpoint Server** field, specify a display name for the BSM server host. For example: my_BSM_1.
- (Optional) In the **Log Level** field, change the log level from INFO (default) to another level. For example: WARNING.
- (Optional) If you want this integration instance to be automatically enabled when the Service Manager Server service is started, select **Run at system startup**.

6. Click **Next**. The Integration Instance Parameters page opens.
7. On the **General Parameters** tab, complete the following fields as necessary:

Name	Category	Value	Description
WithdrawDowntime	General	true/false	Set this value to `true`: When authorized users are manually changing the phase of a change record which has 'valid' outage, a window will open and provide choices of withdrawing the outage. Set this value to `false`: The pop-up window is disabled. This operation may cause some unapproved planned downtimes be synchronized to BSM. By default, this value is set to `true`.
Category or	Change	The final	Set the final approval phase for downtime, which

Name	Category	Value	Description
workflow (Process Designer) name of changes		approval phase for changes	is the indication of valid downtime information.
Category or workflow (Process Designer) name of tasks	Task	The final approval phase for tasks	Set the final approval phase for downtime, which is the indication of valid downtime information.
sm.host	General	<sm server name >	Set the Service Manager server host name or DNS name to compose the External Process Reference and the Reference Number of Scheduled Downtime CI in UCMDB. **Note:** Do not include a colon in this field. Otherwise, the logic will be broken.
sm.reference.prefix	General	urn:x-hp:2009:sm	Set the prefix to compose the External Process Reference of Scheduled Downtime CI in UCMDB. **Note:** This field has a fixed value. Do not change it.

Notes:

a. Type category or workflow name of change/task in the **Name** column. This value is case-sensitive and it must match the record in Service Manager database.

b. Set the value to Change for changes in the **Category** column. Similarly, set the value to Task for tasks.

c. Type the final approval phase in the **Value** column. This value is case-sensitive and it must match the record in Service Manager database.You can separate multiple phases by semicolons, which must be the English character.

d. Detailed information will be displayed in the integration log when the following errors occur:
   - User input of categories/phases for the changes/tasks is not correct.
   - The category and phase pair does not exist in the database.

e. For Change Management categories which do not have approval phase, the downtime integration will treat its downtime information as final approved once created. You do not need to define any phases in SMIS parameters.

f. For the category or workflow name of the changes and the tasks, the integration will ignore all the final phases defined for the redundant category or workflow.

8. Click **Next** twice and then click **Finish**. Leave the Integration Instance Mapping and Integration Instance Fields settings blank. This integration does not use these settings.

   Service Manager creates the instance. You can edit, enable, disable, or delete it in Integration Manager.

9. Enable the integration instance. SMIS will validate all the final phases you filled in the Integration Instance Parameters page and print warning messages if there are errors.

Tailor Service Manager to handle phase change

Applies to User Roles:

System Administrator

Implementer

In the Service Manager Change Management module, authorized users can manually change the phase of a change record. If the phase is changed to the one prior to the final approval phase in the SMBSM_DOWNTIME instance, the system will check if there are existing planned downtimes that have been set to Ready. If such downtimes exist, a window will open and provide two options for the corresponding planned downtimes:

- Click **Yes** to withdraw the corresponding planned downtimes from UCMDB. The changes or tasks need to be approved again to synchronize with UCMDB at another time.
- Click **No**. There will be no change to the planned downtimes even if the actual status of the changes or tasks are not approved.

Note: To disable the pop-up window when withdrawing the planned downtimes, you need to set the `WithdrawDowntime` parameter to `false` in the SMBSM_DOWNTIME instance. This operation may cause some unapproved planned downtimes to be synchronized to Operations Manager i (OMi).

With Process Designer (PD) Content Pack 2 or later applied in Service Manager, you can tailor the process to transit changes or tasks from one phase that is after the final approval phase in the SMBSM_DOWNTIME instance to another that is prior to the final approval phase.To withdraw the related planned downtime for this kind of transition, you need to add a rule set for the transition in the Closed Loop Incident Process (CLIP) solution.

To do this, follow these steps:

1. Go to the target workflow that needs tailoring.
2. Select the transition that moves a phase from before the final approval phase to after the final approval phase.
3. In the Rule Sets section, click **Add** and select the **clip.downtime.withdraw** rule set.
4. Click **OK** to save the workflow.

Verify the OMi-SM downtime synchronization setup

Applies to User Roles:

System Administrator

When you have set up the Downtime Exchange integration, you can perform the following tasks to see if you have successfully set up your downtime synchronization.

Task 1. Open a new change of a category that has the final approval phase defined in SMIS

1. Click **Change Management** > **Changes** > **Create New Change**.
2. Select **Hardware** for example.
3. In the Affected CI field, set the name of the CI to be synchronized. For example: `adv-afr-desk-101`.
4. Set Scheduled Downtime Start and Scheduled Downtime End to a future time.
5. Select the **Configuration Item(s) Down** checkbox.
6. Set other required fields.
7. Click **Save & Exit**.

Task 2. Approve the change at the final approval phase

1. Click **Change Management** > **Changes** > **Search Change** and search for the change opened in Task 1.
2. Move the Change to the Change Approval phase.
3. Log on to Service Manager with user account `Change.Approver`.
4. Search for the change and approve it.

Task 3. Create new format for the intClipDownTime table

1. Click **Tailoring** > **Forms Designer**.
2. Create a new format for the intClipDownTime table by using the Form Wizard.
3. Add all fields to this format.

Task 4. Check the corresponding intClipDownTime record

1. From Database Manager, open the format of the intClipDownTime table.
2. Click **Search** to see the record created for this downtime.
3. Check the External Status field:

External Status values	Description
`NULL`	The downtime is waiting for final approval, or the scheduler has not proceeded this record yet.
`0` (Canceled)	The downtime is canceled before being implemented.
`1` (Ready)	The downtime has been approved and is ready to be synchronized to UCMDB or OMi (RTSM).
`2` (Withdrawn)	The downtime is approved firstly and then the approval is retracted (withdrawn).

Notes:

a. Only downtime records with External Status `1` can be synchronized.

b. If the External Status is not `1`, wait some time for background schedulers SLA and SMBSM_DOWNTIME to process this record.

Task 5. Populate downtime from Service Manager to UCMDB

1. From UCMDB, run the `CLIP Down Time Population` job and the `CI To Down Time CI With Connection` job in a fixed order.
2. Search for the `adv-afr-desk-101` CI in UCMDB. Check that a corresponding Scheduled Downtime CI is created, and a relationship between the Scheduled Downtime CI and the affected CI is created.

Note: If any of the aforementioned tasks fails, refer to and check if all the system prerequisites are met.

Computer Telephony Integration (CTI) with the Web client

You can integrate the Web client with Computer Telephony Integration (CTI) applications to automate the creation of interactions. To support CTI, each Web client computer system must have a Java Run-time Environment (JRE) installed and do a one-time download of the CTI support code. The download will start automatically the first time you connect, appending `?telephonyuser=1` to the URL. You must be logged in with administrative privileges to do the download. (This is not necessary on subsequent connections.)

Refer to the Web Tier Installation chapter of the *HP Service Manager Installation Guide* for further information.

Configure the CTI application

Applies to User Roles:

System Administrator

In order for the Web client to accept Computer Telephony Integration (CTI) events, an administrator must configure the CTI application to submit proper Service Manager events.

If you used CTI from previous versions, you can clone records from HP ServiceCenter 5.1 to Service Manager.

To configure the CTI application:

1. Call Service Manager with a System Event type (ReceiveInteraction) to open an interaction.

   ```
   DDEExecute channel, "[SystemEvent(""ReceiveInteraction"", ""Contact Name"",
   ""Jones, Jerry"")]"
   ```

2. The client receives this as a SystemEvent (this is a database) and finds the Record for that type of DDE.

3. The application us.router call the program "us.fill.from.event" that looks at the "pmtapi" table for the System Event details.

Case Exchange framework

HP Service Manager Case Exchange is a solution to exchange data between two Service Manager systems or between Service Manager and another product. The Case Exchange framework mainly facilitates the following operations:

- Sending and receiving data
- Viewing and processing the exchanged data in the native environment

To leverage Case Exchange capabilities, the systems to be connected must support REST-based Web Services in JSON format. SOAP-based Web Services are not supported. The following chapters describe the functionalities of Case Exchange and their expected behaviors.

It is highly recommended that the personnel who implement Case Exchange with another system have the experience in the following Service Manager technologies:

- REST-based Web Services
- DBDICT
- Process Designer framework
- JavaScript
- JSON
- Service Manager Integration Suite (SMIS)

During the implementation, you can refer to the following documentation:

- Web Services Guide
- Programmers Guide
- SMIS Integration Manager and SMIS developer guide
- Process Designer Framework

Note: The scope of support is limited to the behavior of APIs and product features documented. HP is responsible for the correct operation of those features and APIs. HP is not responsible for

debugging scripts or code created to utilize these features to implement a solution. In order to receive the best possible support, HP asks customers to provide a reproducible unit test scenario that demonstrates the error or unexpected behavior of the API or documented feature.

Case Exchange framework features

This chapter introduces the Case Exchange features.

Connector

Case Exchange is enabled by connectors, which can open, update, and close records in the system of another provider. Connectors can also perform the following tasks:

- Listen for events or updates related to record exchange.
- Take care of the physical communication to the system via REST-based web services in JSON format.
- Manage appropriate authentication and identity credentials required by the connected system.

Field mapping and value mapping

Field mapping and value mapping determine how the record data is transformed into the internal or external normalized case format.

Field mapping ensures that the data from one system is send to the correct field on the second system. To avoid interface failures the field names and the field name description should *not* contain any special characters.

Value mapping ensures the data is correctly transformed according to the rules required in each system. The value mapping supports expressions and calculations to ensure the data is correctly manipulated prior to sending or updating records in the local database.

For more information about field mapping and value mapping, see topics under the "Integration Instance Mapping" on page 78 section.

Outbound trigger rules

One of the core functions of Case Exchange is automated data exchange between HP Service Manager and integrated systems. For example, Case Exchange can automate the following activities:

- Opening records
- Exchanging record updates between Service Manager and integrated systems
- Tracking the status of related records in Service Manager and in integrated systems

Service Manager has a dedicated rule type in Rule Sets that can trigger Case Exchange between Service Manager and integrated systems. Use one of the following methods to invoke a Rule Set:

- If Process Designer is implemented in Service Manager, invoke the Rule Set from workflows.
- If Process Designer is not implemented in Service Manager, you must create a trigger and add the following API in the trigger's script:

  ```
  lib.CaseExchange_RuleExecute.executeSingleRuleSet(record,oldrecord,RuleSetID)
  ```

For more information about how to invoke a Rule Set, see the following section:

"Invoke Case Exchange Rule Sets" on page 314

Attachment handling

You can configure Case Exchange to transfer attachments in exchanging records from one system to the other system. When the attachment handling functionality is enabled, Case Exchange handles attachments differently in different integration mechanisms.

Service Manager and Service Anywhere integration

When a Service Manager (SM) system is integrated with a Service Anywhere (SAW) system, the Pull mechanism is used. If the attachment handling functionality is enabled in the SM system, Case

Exchange handles the attachments as follows:

- Attachments added in SM are transferred to the corresponding records in SAW.
- SM retrieves attachments from SAW when it handles the next Case Exchange task that is initialized by SAW.

For more information about the Pull mechanism for SM/SAW integration, see "The Pull mechanism" on page 317.

Service Manager and Service Manager integration

When an SM system is integrated with another SM system, either the Pull mechanism or the Push mechanism is used.

When the Pull mechanism is used, Case Exchange works in the same way as SM/SAW integration. That is, the SM system that has the attachment handling functionality enabled transfers attachments to the other SM system and retrieves attachments from that system when it handles the next Case Exchange task.

However, when the Push mechanism is used, the system that has the attachment handling functionality enabled only transfers attachments to the other system. It does not retrieve attachments from that system. When the functionality is enabled in both system, attachments are transferred in both directions.

For more information about the Pull mechanism for SM/SM integration, see "The Pull mechanism" on page 327. For more information about the Push mechanism in this case, see "The Push mechanism" on page 328.

Additional considerations for attachment handling

In addtion to the attachment handling functionality described for different SM/SAW or SM/SM integration scenarios, you also need to note the following when you use the functionality:

- No attachments are transferred if the attachment handling functionality is disabled in both systems.
- Even if the attachment handling functionality is enabled, Case Exchange does not remove attachments from ones system when you remove corresponding attachments from the other system.

- A system administrator can specify the type and maximum size of the attachment files that Case Exchange can transfer. In case the file type of an attachment does not match the listed file types or in case the file size of attachment exceeds the configured limit, Service Manager does not transfer the attachment.

For more information, refer to the *Service Manager Administrator's Guide*.

Audit and logging

The Case Exchange framework provides different portals for administrators and users to view the Case Exchange activity log.

The Case Exchange framework tracks and records all transactions of exchanged request in the Service Manager Integration Suite (SMIS) task log. Administrators can access this log from SMIS.

When a Case Exchange integration instance is active and a Case Exchange task has occurred to an Incident record, users can view the **Case Exchange** section in the Incident record for the details of the Case Exchange information. The **Case Exchange** section contains the following information:

- **Details**.

Field name	Description
External Id	The ID of the related record in the integrated system.
External Status	The status of the related record in the integrated system.
Creation Time	The time when the Incident record is created.
Active	This field indicates if Case Exchange is active for this record. Possible values of this field are `true` and `false`: `true`: The update in one of the systems can be exchanged to the other system. `false`: The update in one of the systems *cannot* be exchanged to the other system.
Originator System	The name of the integrated system where the record come from.
Integration Name	The name of the integration instance that transfers the record from the integrated system.

- **Log**.

Field name	Description
Date	The date and time when the task occurs. The link on the date and time can direct you to the **Task Log Details** page, which displays the detailed information of that Case Exchange task.
Status	The status of the task.
Message	A short description of the task.
Integration Name	The name of the integration instance that carries out the task.

The task log gives a first indication about potential issues of an error but does not contain detailed error messages, you can find the detailed information in the standard Service Manager log file (sm.log).

Error handling

HP Service Manager Integration Suite (SMIS) can automatically create a new Incident record for the error if all of the following conditions are met:

- The error handling feature is active in a Case Exchange integration instance.
- A Case Exchange task of this integration encounters an error.
- SMIS has performed the number of retries that is pre-defined, but still encounters error.

SMIS automatically set the following fields in the record according to the configuration in the integration instance:

- Title
- Assignment Group
- Impact
- Urgency
- Category
- Area

- Subarea
- Affected Service

The error handling feature works in the following manner:

- Case Exchange only creates one Incident record for each integration instance that has failed tasks.
- When the task fails for the first time, SMIS creates a new Incident record.
- When the task that has failed fails again, SMIS works in the following manner:
  - If the record for the previous failure is closed, SMIS creates a new Incident record.
  - If the record for the previous failure is not closed, SMIS does not create a new Incident record.

Ownership

At any time through out the life cycle of a record in Case Exchange, only one system owns the record. The owner of the record has the responsibility to resolve the record or transfer the record to another organization if necessary.

The ownership of record in Case Exchange relies on process definition rather than tooling. It is highly recommended to define clear rules of ownership for each step in a case exchange environment prior taking an interface live. These rules of ownership are required to avoid any potential data loss in case both parties update a record at the same time. HP is not responsible for issues during the case exchange in a situation where both parties are able to update a record at the same time.

See "Recommendations" below for other suggestions of implementing Case Exchange.

Enable Case Exchange with another system

This chapter introduces the tasks that you need to perform to set up a Case Exchange integration between Service Manager and another system:

Recommendations

Before you set up the Case Exchange integration, consider the following recommendations for preparation and configuration:

- Decide about the general connection method, which can be either of the following:
  - Pull the data from the target system
  - The target system pushes the data into Service Manager
- Ensure that you have a clear picture about the workflows in the systems you want to integrate.
- Ensure that you know how to map the workflows for incoming and outgoing data.
- Ensure that the attachment settings are correctly configured.
- Ensure security settings are defined and properly configured.
- Enable outbound events for easy usage in the RuleSets.
- Test the configurations properly in a test environment before go live.
- Ensure the ownership of the records is clearly defined for each stage.
- Align on re-open, resolve, and closure rules, follow Processes and Best Practices Guide.
- Perform sufficient performance tests, including test with attachments to ensure the system can handle the case exchange requirements of your environment.
- Do not underestimate the effort for the workflow and status mapping.

Configure Incident environment

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

To do this, follow these steps:

1. Go to **Incident Management** > **Administration** > **Environment**.
2. Select **Use Resolved Status?**.
3. Click **Save**.
4. Click **OK**.

Create a new integration template

Applies to User Roles:

System Administrator

An appropriate integration template must be ready before you integrate HP Service Manager with another system. You can either create a new template, or use and modify an existing template during integration.

To create a new integration template, refer to the *HP Service Manager Integration Suite (SMIS) Developer Guide*.

Service Manager provides out-of-box templates for Case Exchange integrations, for more information see "Out-of-box integration templates" on page 73.

Add and enable a Case Exchange integration instance

Applies to User Roles:

System Administrator

To add a Case Exchange integration instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The **Integration Template Selection** wizard opens.
3. Select a Case Exchange template from the **Integration Template** list. For example, select **CaseExchangeDefaultTemplate**.
4. If you want to use the field mappings provided with the template, select **Import Mapping**.

   Note: A template becomes unavailable when the number of integration instances based on this template reaches the maximum value predefined in the **Instance Count** filed in the template. For more information about how to add or edit an integration template, see Service Manager Integration Suite (SMIS) Developer Guide.

5. Click **Next**. The **Integration Instance Information** page opens. Verify or complete the fields as necessary. For the description of each field on this page, see the topics under "Configuration details" on the next page.

6. Click **Next**. The **Integration Instance Parameters** page opens. This page contains all predefined parameters for the integration.

   Note: You can modify the predefined parameter values as necessary. However, it is not recommended to add new parameters, modify parameter names or categories.

7. Click **Next**. The **Integration Instance Fields** page opens.
8. Enter the Service Manager fields and the endpoint fields in the following two tabs:
   - **SM Fields**: Enter the fields of the Service Manager system side that can be mapped to endpoint fields.
   - **Endpoint Fields**: Enter the fields of the endpoint system that can be mapped to Service Manager server fields.
9. Click **Next**. The **Integration Instance Mapping** page opens.

   This page contains all field mappings and value mappings between Service Manager server fields and endpoint fields. For more information about how to configure this page, see topics under "Integration Instance Mapping" on page 78.
10. Click **Finish**. The new integration instance is added.

For more information about how to enable an integration instance, see "Enable or disable an integration instance" on page 88.

Configuration details

This chapter provides detailed explanation to each field you need to configure when you set up the Case Exchange integration by using the out-of-box template: **CaseExchangeDefaultTemplate**.

Note: Currently, Case Exchange only supports the data transaction through RESTful APIs.

Integration Instance Information

For details about how to configure the **Integration Instance Information** page, see "Integration Instance Information fields" on page 75.

Integration Instance Parameters – General

The following table explains the fields under the **General** tab in the **Integration Instance Parameters** page.

Fields	Value	Description
Object	User-defined. For example, `Incident`.	The table name of the object in Service Manager.
Timeout	User-defined. For example: `30`.	This value specifies the time-out (in seconds) for each of these three activities: Connect, Send, and Receive.
Base URL	User-defined.	The base portion of the endpoint URL. The format of the URL is as follows: http(s)://*<host>.<domain>* For example, the Base URL for the Service Anywhere endpoint might be as follows: `https://<host name>.saas.hp.com`
Login URL	User-defined.	The login URL of the endpoint. The format of the URL is as follows: `<Base URL>/auth/authentication-endpoint/authenticate/login`
Tenant Id	User-defined.	The Tenant Id of the endpoint system.
User name	User-defined.	The endpoint user name for integration.
Password	User-defined.	The password of the user name.

Integration Instance Parameters – Inbound

The following tables explain the fields under the **Inbound** tab in the **Integration Instance Parameters** page.

Fields	Value	Description
External Id	User-	The relative path of the ID field in inbound JSON. This path is relative to the

Fields	Value	Description
Field	defined.	List path. The field name you entered must be a valid reference in the external system. For example, `properties.Id`.
External Status Field	User-defined.	The relative path of the Status field in inbound JSON. This path is relative to the List path. The field name you entered must be a valid reference in the external system. For example, `properties.Status`.
Internal Id Field	User-defined.	The name of the unique field of the Service Manager object. For example, enter “number” for the “probsummary” table. The field name you entered must be a valid dbdict field name in the selected Service Manager object.

If you select the **Activate Data Pulling** option, Service Manager pulls the data of the inbound tasks from the endpoint system. The following fields appears when you select this option.

Fields	Value	Description
Pulling From	User-defined.	The integration instance pulls all the records that are updated later than the time specified in this field from the end point. If you do not specify a time, system uses the current time.
Time difference (s)	User-defined. Default: `0`.	The time difference (in seconds) between Service Manager and the endpoint system.
Relative URL	User-defined.	The relative URL that specifies the resource to be exchanged in the endpoint system. The string in this field is directly appended after the string you configured in the **Base URL** field under the **General** tab.
Query	User-defined.	The additional query parameters. The string in this field is directly appended after the Relative URL that is configured in the previous field. For more information on how to edit the Query strings, see "Edit the query and pagination query strings" on page 367
List path	User-defined.	The root path of the list result in the JSON response from the endpoint for a pulling request. For example, the list path is `entities` in the following JSON response:

Fields	Value	Description

		<pre>{
		"entities": [
		{
		"entity_type": "Incident",
		"properties": {
		"Id": "***",
		...
		}
		},
		...
		]
		}</pre>

Pagination	Selected/not selected.	When you select this option, the result list from the endpoint is transferred in pages.
Page Size	User-defined.	Specify the maximum number of records in a page.
First Record Offset	User-defined.	This value defines the index of the first record in each page. Usually the value is `0` or `1`.
Pagination Query	User-defined.	Pagination parameters. The string in this field is directly appended after the query parameters that are configured under the **Inbound** tab. For more information on how to edit the Pagination Query strings, see "Edit the query and pagination query strings" on page 367

If you select the **Activate Data Pushing** option, the endpoint Service Manager system pushes the data of the inbound task to the native Service Manager system. This option only works for the integration between two Service Manager systems. The following fields appears when you select this option.

Fields	Value	Description
Incoming WebService Action	User-defined. For example, `Create` or `Update`.	The action name in the RESTful API of the endpoint Service Manager system. In an out-of-box Service Manager system, the action names are **Create** and **Update**.
SM Action to execute	User-defined. For example, `add` or `save`.	The action to be executed in the native Service Manager system for the corresponding incoming action. Possible values for this field are `add` and `save`.

Note: By default, the integration template uses the Web Service: **CaseExchange**. To view this Web Service, go to the following location in Service Manager and search for "CaseExchange":

Tailoring > **Web Service** > **Web Service Configuration**

Case Exchange only supports the Web Service inbound push call that **Action Type** is **Application Pass Through** and **Customer Action to Perform** is **CaseExchange.Pushing**. Any other type of inbound push features for Case Exchange via SMIS are not supported.

Integration Instance Parameters – Outbound

The following table explains the fields under the **Outbound** tab in the **Integration Instance Parameters** page.

Fields	Value	Description
Asynchronous Processing	Selected/not selected.	If you select this option, the outbound tasks work in asynchronous mode. If you do not select this option, the creation or update of an object triggers the outbound task immediately.
Event	User-defined.	The name of the outbound action.
Action Type	User-defined.	The action type of this event in the endpoint. The available options for this field are **Create only** and **Update only**.
URL	User-defined.	The relative URL. The string in this field is directly appended after the base URL in the outbound request URL.
HTTP method	User-defined.	Specify the HTTP method.
Entity path	User-defined.	Specify the root path of the list result in the JSON response from the endpoint. For more information about entity path, see "Entity path" on page 379.
Parameter	User-defined.	Additional parameters. The string in this field is directly appended after the relative URL in the outbound request URL. For example, if you specify the parameter as `?entitytype=incident`, the outbound request URL will be: *<BaseURL><URL>*`?entitytype=incident` This field is needed if the endpoint only accepts parameters in the

Fields	Value	Description
		URL.
Additional path	User-defined.	Additional paths or elements that are mandatory in outbound JSON but are not defined in field mapping or entity path. For more information about how to configure this field, see "Specify additional path" on page 378.

Integration Instance Parameters – Error Handling

The following table explains the fields under the **Error Handling** tab in the **Integration Instance Parameters** page.

Fields	Value	Description
Activate incident creation for Errors	Selected/not selected.	Enable or disable the error handling feature, which can automatically create an Incident record for a failed SMIS task.
Title	User-defined. Default: `SMIS Error`.	The title of the Incident records for error handling.
Assignment Group	User-defined.	Specify the Assignment Group of the Incident records for error handling.
Impact / Urgency	User-defined.	Specify the Impact and Urgency of the Incident records for error handling.
Category	User-defined.	Specify the Category of the Incident records for error handling.
Area	User-defined.	Specify the Area of the Incident records for error handling.
Subarea	User-defined.	Specify the Subarea of the Incident records for error handling.
Affected Service	User-defined.	Specify the Affected Service of the Incident records for error handling.

Integration Instance Parameters – Attachment Handling

The following table explains the fields under the **Attachment Handling** tab in the **Integration Instance Parameters** page.

All the parameters in this tab apply to inbound pull and outbound processes.

Fields	Value	Description
Activate attachment exchange	Selected/not selected.	Enable or disable attachment exchange.
Attachment REST URL	User-defined.	The REST API URL for endpoint attachments.
Unsupported File Extensions	User-defined. For example: `exe;rar;iso`.	Specify unsupported file types in the endpoint. Split multiple file types by using semicolons (;).
Timeout (s)	User-defined. Default: `20`.	This value specifies the time-out (in seconds) for each of these three attachment activities: Connect, Send, and Receive.
Size Limitation (kb)	User-defined. Default: `1024`	The endpoint limitation on the attachment size. This value is useful only when an attachment is sent to the endpoint.

Integration Instance Parameters – Additional Script

The following table explains the fields under the **Additional Script** tab in the **Integration Instance Parameters** page.

Section	Fields	Value	Description
Authentication	Set the HTTP header	User-defined.	Specify additional JavaScript function to set the HTTP header. If you do not specify this field, the default HTTP header only provides Basic Authentication and Content-Type.
	Login to the external system	User-defined.	Specify additional JavaScript function for login if the endpoint requires special login process. If you do not specify this field, Case Exchange does not perform any login process and only sets the authentication information into the HTTP header.
Inbound	Validate inbound response	User-defined.	Specify additional JavaScript function to validate the response body of an inbound request. When the data comes in, this script validates the data before the data is pushed into the SMIS task queue. If you do not specify this field, Case Exchange only validates the response HTTP code and does not validate the response body.

Section	Fields	Value	Description
	Inbound & Push post processing activities	User-defined.	Specify additional JavaScript function to perform post process for inbound tasks. This script performs post processing after SMIS processes the inbound task. If you do not specify this field, Case Exchange does not perform any post process for inbound tasks.
Outbound	Validate & Parse outbound response	User-defined.	Specify additional JavaScript function to validate and parse the response body of outbound request. The function works in the following way: • If the validation succeeds, the function returns the parsed external ID. • If the validation fails, the function returns “False”. If you do not specify this field, Case Exchange only validates the HTTP code and retrieves the ID according to the definitions in the **Inbound** tab.
	Outbound post processing activities	User-defined.	Specify additional JavaScript function to perform post process for outbound tasks. This script performs post processing after SMIS processes the outbound task. If you do not specify this field, Case Exchange does not perform any post process for outbound tasks.
Attachment	Set the HTTP header	User-defined.	Specify additional JavaScript function to set the HTTP header for attachment. If you do not specify this field, the default HTTP header only provides Basic Authentication and Content-Type.
	Set header string for the HTTP body	User-defined.	Specify additional JavaScript function to assemble the header of the attachment request if the attachment exchange uses the multipart/form-data transfer.
	Retrieve and parse Attachment Info	User-defined.	Specify additional JavaScript function to retrieve attachment information, such as attachment name, type, size, and so on.
	Parse response of attachment creation	User-defined.	Specify additional JavaScript function to parse the response body of an outbound attachment request.
	Update	User-	Specify additional JavaScript function to update the

Section	Fields	Value	Description
	outbound Attachment Info	defined.	attachment information to the record in the endpoint. The information can link the attachment with the record. You do not need to specify this field if the endpoint system can automatically update the attachment information.

Configure Case Exchange Rule Sets

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.

Invoke Case Exchange Rule Sets

This chapter introduces how to invoke Rule Sets to trigger automated data exchange for the Case Exchange integration.

Invoke Rule Sets from workflows

Applies to User Roles:

System Administrator

On a Service Manager system that has Process Designer implemented, you can invoke a Rule Set from a workflow phase.

To invoke a Rule Set from a workflow phase, follow these steps:

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.
3. Select the phase in which you want to invoke a Rule Set.
4. Add the Rule Set in the following tabs according to your needs:

- The **On enter**, **On exit**, **Initialization**, **On display**, **On update**, or **After successful update** tab under the **Rule Sets** tab.
- The **Actions** tab.

5. Save the workflow.

Invoke Rule Sets from triggers

Applies to User Roles:

System Administrator

If Process Designer is not implemented in Service Manager, you must invoke a Rule Set from a Service Manager trigger, by adding the following API in the trigger's script:

```
lib.CaseExchange_RuleExecute.executeSingleRuleSet(record,oldrecord,RuleSetID)
```

The following table explains the meaning of each parameter in this API.

Parameter	Description
record	The new record.
oldrecord	The old record.
RuleSetID	The ID of the Case Exchange Rule Set. For example, `CE_CREATE_INCIDENT`.

To add a trigger that invokes a Rule Set, follow these steps:

1. Click **Tailoring** > **Database Manager**. The Database Manager page opens.
2. Type `triggers` in the **Table** field, and then click **Search**. The Search Trigger Records page opens.

3. Complete the following fields:

Field	Description
Trigger Name	The name of the trigger.
Table Name	The file to be monitored by this trigger.
Trigger Type	Select the specific activity to react to: **1 - Before Add** - When adding a new record to this file, launch the application prior to committing the addition. **2 - After Add** - When adding a new record to this file, launch the application after committing the addition. **3 - Before Update** - When modifying a record in this file, launch the application prior to committing the change. **4 - After Update** - When modifying a record in this file, launch the application after committing the change. **5 - Before Delete** - When deleting a record in this file, launch the application prior to performing the deletion. **6 - After Delete** - When deleting a record in this file, launch the application after performing the deletion. **Note:** Only triggers of *type 4* (After Update), and *type 6* (After Delete) are supported by Cascade Updates.
Application	The RAD application to be launch by this trigger. If you only intend to invoke a Rule Set by using this trigger, leave this field empty.
Script	Call the following API by using appropriate parameters: `lib.CaseExchange_RuleExecute.executeSingleRuleSet (record,oldrecord,RuleSetID)`

4. Click **Add**.

Enable Case Exchange with Service Anywhere

This chapter provides detailed instructions on how to set up the Case Exchange integration for the Incident Management module between HP Service Manager and HP Service Anywhere.

Note: Service Manager must be 9.34 or higher.

Service Manager provides the integration template for the Case Exchange integration between Service Manager and Service Anywhere: **CaseExchangeSM_SAW**. You can modify this template as necessary. To modify the integration template, follow the instructions in the Service Manager Integration Suite (SMIS) Developer Guide.

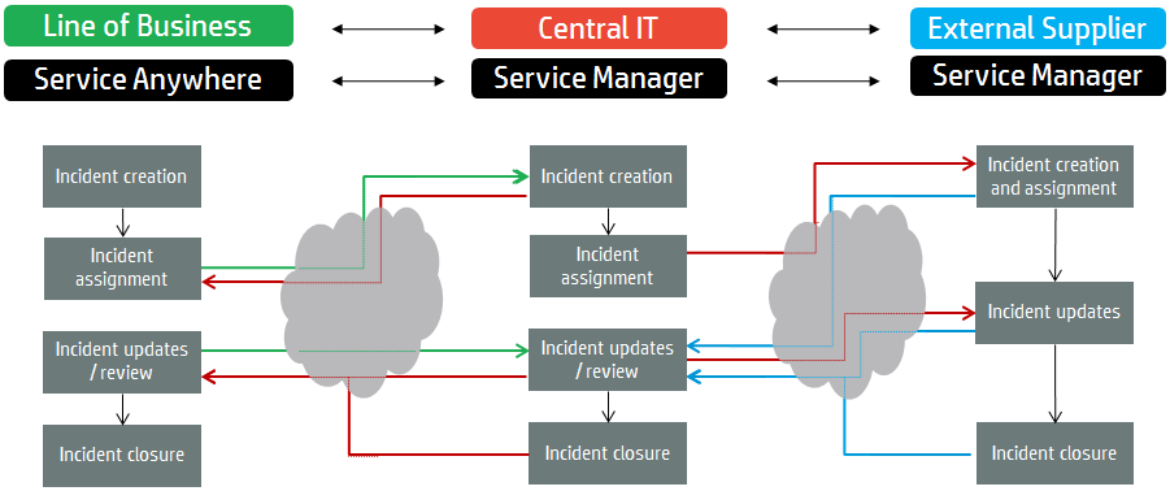
Before you start to set up the Case Exchange integration, we highly recommend that you read the following sections under "Case Exchange framework" on page 297:

- "Case Exchange framework features" on page 298: This section introduces the core features of the Case Exchange framework.
- "Enable Case Exchange with another system" on page 303 : This section provides recommendations and general instructions on how to enable Case Exchange with another system.
- "Incident exchange scenarios" on page 347: This section introduces typical Case Exchange use cases.
- "Common user tasks" on page 362: This section introduces the common user tasks that apply to the Incident Management module in the Case Exchange integration.
- "System administrator tasks" on page 365: This section introduces the system administrator tasks in the Case Exchange integration.

The Pull mechanism

The Case Exchange integration between HP Service Manager and HP Service Anywhere uses the Pull mechanism.

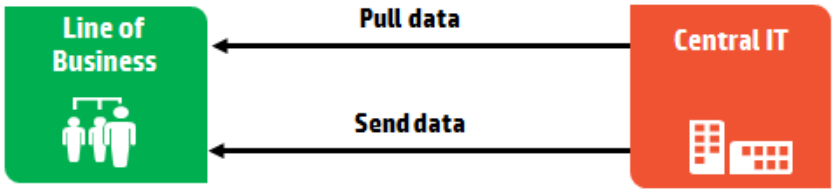
This chapter explains the Pull mechanisms between Line of Business (LOB) and Central IT (CIT) in the following typical ecosystem.



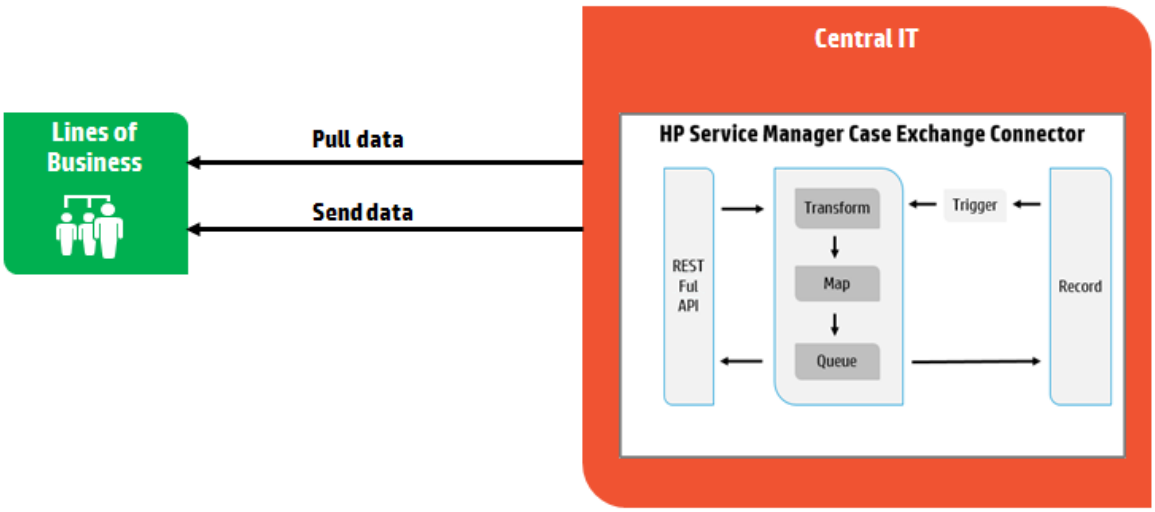
In the Pull mechanism, one system actively pulls data from and sends appropriate data to the other system.

Note: In the following diagrams, the arrows between the two systems represents the direction of the request, rather than the direction of the data flow.

In the following diagram, the CIT's system pulls data from and sends the updated data back to the LOB's system.



The following diagram shows the data flow of the Pull mechanism.


Central IT
Lines of Business
Pull data
Send data
HP Service Manager Case Exchange Connector
REST Ful API
Transform
Map
Queue
Trigger
Record

Add and enable an integration instance

Applies to User Roles:

System Administrator

The configuration of the Service Manager and Service Anywhere integration is mainly done on the Service Manager side. However, you must do some configuration in Service Anywhere before records can be exchanged between the two systems. The following subsections provide detailed instructions for adding and enabling the integration instance.

Note: The following instructions assume that you use the out-of-box settings of the **CaseExchangeSM_SAW** integration template. However, you can customize these out-of-box settings according to your need. For more information about how to customize the settings in the integration instance, see the following sections in the online help:

System Administration > Integrations > Case Exchange framework > Enable Case Exchange with another system > Add and enable a Case Exchange integration instance

System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Add or delete an integration instance > Integration Instance Mapping

Add an integration instance in Service Manager

To add the Case Exchange integration between HP Service Manager and Service Anywhere, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The Integration Template Selection wizard opens.
3. Select **CaseExchangeSM_SAW** from the **Integration Template** list, select the **Import Mapping** check box, and then click **Next**.
4. Complete the fields on the **Integration Instance Information** page as necessary, and then click **Next**.
5. In the **Integration Instance Parameters** page, configure the following settings in the **General** tab and use the default setup for all 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. In the **Post Script** tab, update `10019` to the corresponding Service ID in Service Anywhere in the following out-of-box code:

```
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, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select the integration instance that you want to enable.
3. Click **Enable**.
4. Click **Yes**.

Configure an integration instance in Service Anywhere

Before you can exchange records between Service Manager and Service Anywhere, you must do the following configuration in Service Anywhere:

1. Make sure your user account has the "SACM Integration" role assigned.
2. Add an external system.
   In Service Manager Case Exchange SMIS instance, an external system named "SM" is used by default for Service Anywhere 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. Assign the external system to a group by using the **External system** field on the **Groups** page. 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.

Create and invoke Rule Sets

HP Service Manager does not provide out-of-box Rule Sets for the Case Exchange integration between Service Manager and Service Anywhere, so you must create Rule Sets when you set up the integration. Refer to the following topics for how to create and invoke Rule Sets:

- *System Administration > Application Setup > Process Designer > Create a rule set*

  Note: When you create a Rule Set for incident exchange between Service Manager and Service Anywhere, set the **Table name** field to **probsummary**.

- *System Administration > Application Setup > Process Designer > Adding a rule > Add a Case Exchange rule*
- *System Administration > Application Setup > Process Designer > Using the Condition Editor*
- *System Administration > Integrations > Case Exchange > Enable Case Exchange with another system > Invoke Case Exchange Rule Sets*

Example Rule Sets

The following table provides example outbound rules that work in the out-of-box HP 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	Update

Condition (RAD expression)	Event
("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true	
sysmoduser in $L.file="<smis_scheduler_name>" **Note:** This rule is used to acknowledge the Update action.	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_name>" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true	Cancel

For more information about the **getExternalID** and **isExternalActive** functions, see "Functions used in rule conditions" on page 380.

Test and troubleshoot the integration

Once you have finished the above configurations in the HP Service Manager system, you can test the Case Exchange integration. The following procedure is an example that you can follow to test the basic functions of the integration:

1. In Service Anywhere, create a new Incident record.
2. Wait for a while (depending on the value that is configured in the **Interval Time** field) and the Incident record should be exchanged to the Service Manager system.
3. In Service Manager, update the Incident record so that the update can trigger the outbound rule that is configured in "Create and invoke Rule Sets" on page 323.
4. The update to the Incident record should be exchanged to Service Anywhere.

If all the above steps are successful, the integration between the two systems is properly configured.

If any of the above steps is unsuccessful, the following checklist can help you to troubleshoot possible problems.

Symptoms	Checklist
In step 2, the Incident record does not appear in Service Manager.	Check the following areas in Service Manager: • Check the Service Manager Integration Suite (SMIS) task queue and task log. • Check the integration instance: ◦ Is the integration instance active? ◦ Is the information in the **General** tab correct? ◦ Have you done any customization when you set up the integration instance? • Check the log file. For more information, refer to the following topic in the online help: *System Administration > Integrations > Case Exchange framework > System administrator tasks > Review log file*
In step 4, the update in Service Manager cannot be exchanged to Service Anywhere.	Check the following areas in Service Manager: • Check the SMIS task queue and task log.

Symptoms	Checklist
	• Have you done any customization when you set up the integration instance? • Check the outbound rule, and make sure that the update to the Incident record can trigger the outbound rule. See "Create and invoke Rule Sets" on page 323. • Check the log file. For more information, refer to the following topic in the online help: *System Administration > Integrations > Case Exchange framework > System administrator tasks > Review log file*

For additional tips about how to troubleshoot the Case Exchange integration, see "Troubleshooting tips" on page 386.

Enable Case Exchange between two Service Manager systems

This chapter provides detailed instructions on how to set up the Case Exchange integration for the Incident Management module between two HP Service Manager systems.

Note: Service Manager must be 9.34 or higher.

Service Manager provides two integration templates for the Case Exchange integration between two Service Manager systems: **CaseExchangeSM_SM_Pull** and **CaseExchangeSM_SM_Push**. You can modify these template as necessary. To modify the integration template, follow the instructions in the Service Manager Integration Suite (SMIS) Developer Guide.

Before you start to set up the Case Exchange integration, we highly recommend that you read the following sections under "Case Exchange framework" on page 297:

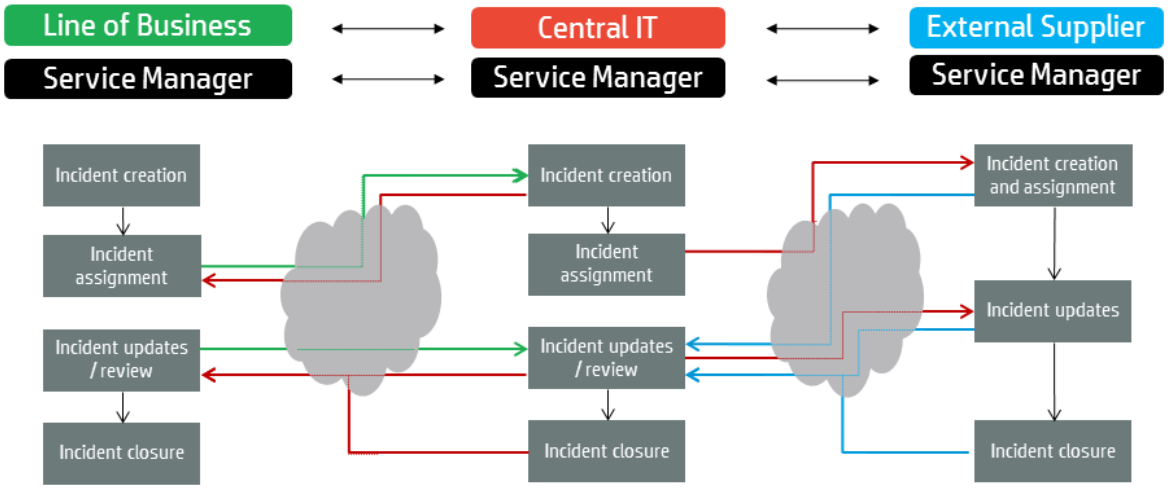
- "Case Exchange framework features" on page 298: This section introduces the core features of the Case Exchange framework.
- "Enable Case Exchange with another system" on page 303 : This section provides recommendations and general instructions on how to enable Case Exchange with another system.
- "Incident exchange scenarios" on page 347: This section introduces typical Case Exchange use cases.

- "Common user tasks" on page 362: This section introduces the common user tasks that apply to the Incident Management module in the Case Exchange integration.
- "System administrator tasks" on page 365: This section introduces the system administrator tasks in the Case Exchange integration.

Connection mechanisms

The Case Exchange integration between two HP Service Manager systems has two connection mechanisms: Pull and Push.

This chapter explains the two connection mechanisms between Line of Business (LOB) and Central IT (CIT) in the following typical ecosystem.

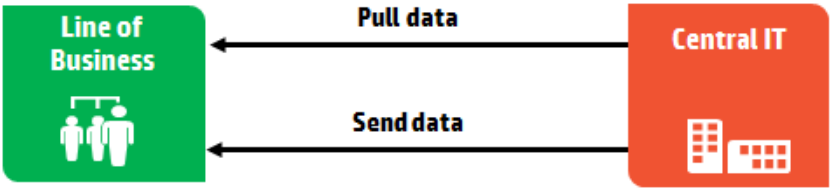


The Pull mechanism

In the Pull mechanism, one system actively pulls data from and sends appropriate data to the other system. The latter system does not need an integration instance.

In the following diagram, the Central IT (CIT) pulls data from and sends the updated data back to the Line of Business (LOB).

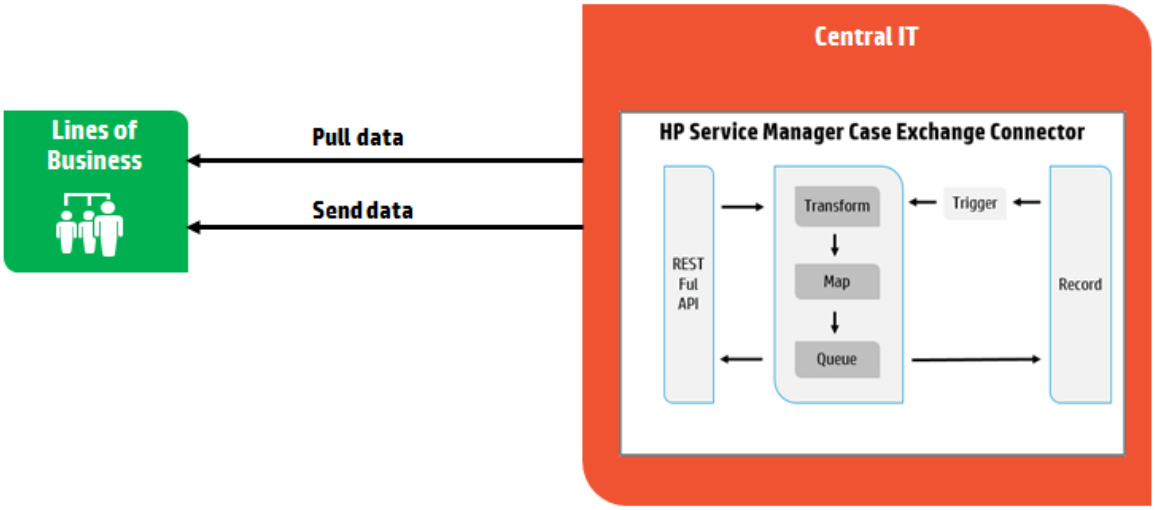
Note: In the following diagrams, the arrows between the two systems represents the direction of the request, rather than the direction of the data flow.



The Pull mechanism has the following advantages and disadvantages.

Advantages	Disadvantages
• Only one integration account is required. That is, an integration account in the LOB's system. • You do not need to configure the Case Exchange logic in the LOB's system. • The CIT's system manages all use cases for Case Exchange. • Only the CIT's system needs configurations of field mapping and value mapping.	• The LOB has very little control over the pulled data.

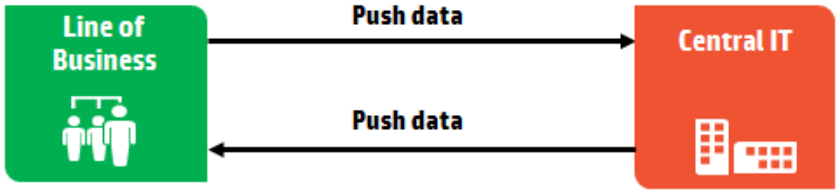
The following diagram shows the data flow of the Pull mechanism.



The Push mechanism

In the Push mechanism, both systems push data to each other. In this mechanism, both systems need an active integration instance.

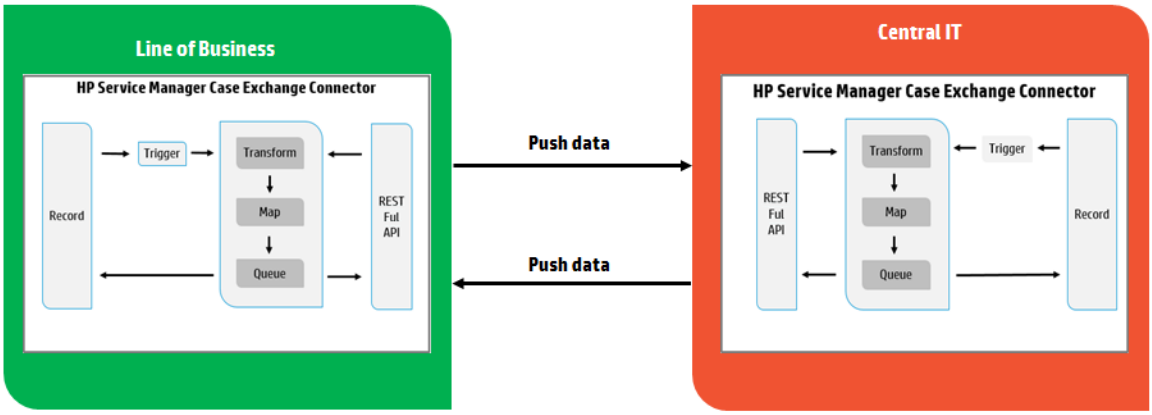
In the following diagram, the Line of Business (LOB) pushes data to the Central IT (CIT), and the Central IT pushes the updates back to the Line of Business.



The Push mechanism has the following advantages and disadvantages.

Advantages	Disadvantages
• The LOB defines the criteria to send data to the CIT. • The CIT receives data based on the LOB's decision. • Every party manages its own integration. • This mechanism provides flexibility on both sides. • The LOB can integrate with other Service Providers.	• Configuration is required in both systems. • Field mapping and data mapping are required in both systems.

The following diagram shows the data flow of the Push mechanism.



Using the Pull mechanism

This chapter describes how to set up the Case Exchange integration between two HP Service Manager systems (System 1 and System 2) by using the Pull mechanism.

In this mechanism, System 1 uses an integration instance that is based on the **CaseExchangeSM_SM_Pull** template, and System 2 does not need an integration instance.

Configure System 1

In System 1, you need to perform the following tasks:

Add and enable an integration instance

Applies to User Roles:

System Administrator

To add an integration instance in System 1, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The Integration Template Selection wizard opens.
3. Select **CaseExchangeSM_SM_Pull** from the **Integration Template** list, select the **Import Mapping** check box, and then click **Next**.
4. Complete the fields on the **Integration Instance Information** page as necessary, and then click **Next**.

   For more information about how to configure this page, refer to the following online help topic:

   System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Add or delete an integration instance > Integration Instance Information fields
5. In the **Integration Instance Parameters** page, configure the following settings in the **General** tab and use the default setup for all the other settings.

   Note: You can modify the other fields according to your needs. For more information about

how to modify the fields in this page, refer to the following section in the online help:

System Administration > Integrations > Case Exchange framework > Enable Case Exchange with another system > Add a Case Exchange integration > Configuration details

Endpoint System runs Process Designer on the exchanged Object: Select this option if Process Designer is implemented in system 2. Otherwise, do not select this option.

Base URL: The value of this field represents the base URL of the endpoint API. For example, `http://{endpoint server}:13080/SM/9`

User Name and **Password**: The credentials of the integration account in system 2.

Note:

- The **Password** field must not be empty.
- This account must be properly configured in system 2. For more information, see "Configure the integration account" on page 338.

6. Click **Next**. The **Integration Instance Fields** page opens.
7. Modify the default entries in the **SM Fields** and **Endpoint Fields** if you have customized fields. Otherwise, go to the next step.

   Note: Endpoint field names must be the same as the caption names in web service **CEIncidentsPull**. For more information about the caption names configured in **CEIncidentsPull**, click **Tailoring** > **Web Service** > **Web Service Configuration** in Service Manager. In addition, you can refer to the out-of-box settings of the **Field Name** field in the **Endpoint Fields** tab.

8. Click **Next**. The **Integration Instance Mapping** page opens.
9. Configure field and value mappings if you have customized fields. Otherwise, go to the next step.

   For more information about how to edit the settings in this page, refer to the following section in the online help:

   System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Add or delete an integration instance > Integration Instance Mapping

10. Click **Finish**.

To enable the integration instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select the integration instance that you want to enable.
3. Click **Enable**.
4. Click **Yes**.

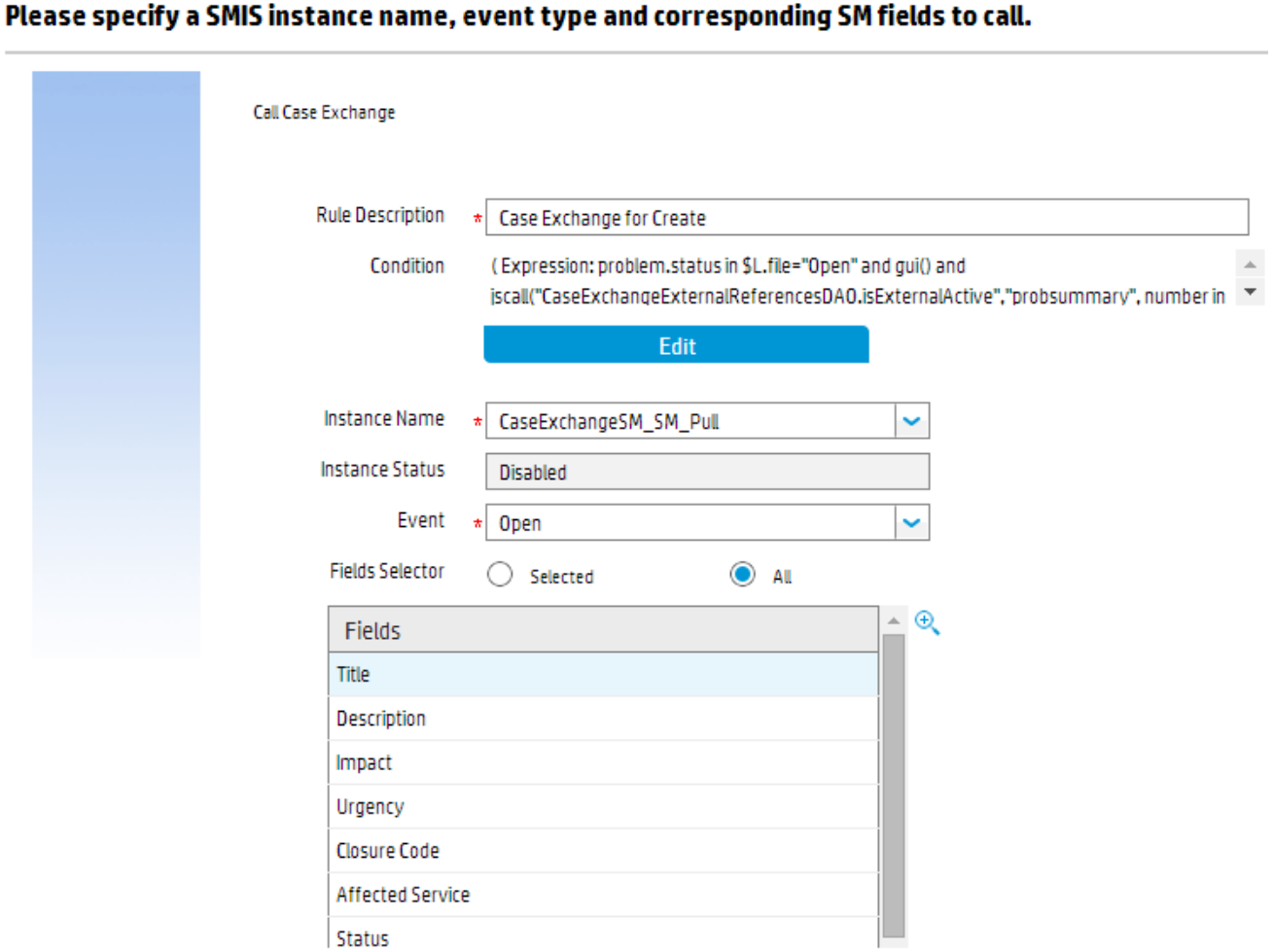
Create and invoke outbound rules

This chapter introduces how to create and invoke outbound rules when you use the Pull mechanism.

In Case Exchange, outbound rules implement business logic to drive a workflow or a process. Rules can help perform calculations, validate fields based on data or Rule Sets, set required fields, and more. A Rule Set uses role-based security.

Create outbound rules

The following screen shot shows an example outbound rule configuration for a Case Exchange integration.



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

Note: When you create a Rule Set for Incident exchange, set the **Table name** field to `probsummary`.

Condition (RAD expression)	Event
assignment in $L.file="*<assignment group>*" and problem.status in $L.file isin {"Pending Customer", "Pending Vendor"} and sysmoduser in $L.file~="*<smis_scheduler_name>*" and jscall("CaseExchangeExternalReferencesDAO.getExternalID",number in $L.file)=""	Create
(not same(problem.status in $L.file, problem.status in $L.file.save) or $apm.activity isin {"Communication with customer","Communication with vendor"}) and not (problem.status in $L.file isin {"Rejected","Resolved","Closed"}) and sysmoduser in $L.file~="*<smis_scheduler_name>*" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true	Update
not same(problem.status in $L.file, problem.status in $L.file.save) and problem.status in $L.file isin {"Resolved","Closed"} 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	Resolve
not same(problem.status in $L.file, problem.status in $L.file.save) and problem.status in $L.file isin {"Rejected","Resolved","Closed"} 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
(sysmoduser in $L.file="*<smis_scheduler_name>*")	Acknowledge

For more information about the **getExternalID** and **isExternalActive** functions, see "Functions used in rule conditions" on page 380.

For more information about how to create Rule Sets, refer to the following topics in the 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*

- *System Administration > Application Setup > Process Designer > Using the Condition Editor*

Invoke Rule Sets

If Process Designer is implemented in HP Service Manager, you can invoke Rule Sets from workflows. For more information, see "Invoke Rule Sets from workflows" on page 314.

If Process Designer is not implemented in Service Manager, you must invoke Rule Sets from triggers. The following table contains example configurations for two triggers: Incident update and Incident creation.

Trigger	Incident update	Incident creation
Trigger Name	case.exchange-update	case.exchange-creation
Table Name	probsummary	probsummary
Trigger Type	4 - After Update	2 - After Add
Script	lib.CaseExchange_RuleExecute.executeSingleRuleSet(record, oldrecord,"CERule4SM2SM")	lib.CaseExchange_RuleExecute.executeSingleRuleSet(record, oldrecord,"CERule4SM2SM")

Note: In this example, the Rule Set ID is `CERule4SM2SM`.

For more information about how to invoke Rule Sets from triggers, see "Invoke Rule Sets from triggers" on page 315.

Configure System 2

In System 2, you only need to configure the account for the Case Exchange integration.

Configure the integration account

System 1 needs the credentials of an account in System 2 to successfully enable the integration. This account must meet the following requirements:

- In case System 2 needs to control what data is pulled by System 1, System 2 can apply mandanten security on this account. For more information, see Mandanten file security.
- This account must have the **RESTful API** execution capability.

  For more information about how to configure this execution capability, see "Configure the integration account" on page 340.
- This account must have the rights to retrieve and update Incident records.
- This account must use the same **Time Zone** and **Date Format** settings as the endpoint HP Service Manager system. See also "Time difference issue" on page 380.

Test and troubleshoot the integration

Once you have finished the above configurations in the HP Service Manager systems, you can test the Case Exchange integration. The following procedure is an example that you can follow to test the basic functions of the integration:

1. In System 2, create a new Incident record that is accessible by the integration account that is configured in "Configure the integration account" above.
2. Wait for a while (depending on the value that is configured in the **Interval Time** field) and the Incident record should be exchanged to System 1.
3. In System 1, update the Incident record so that the update can trigger the outbound rule that is configured in "Create and invoke outbound rules" on page 333.
4. The update to the Incident record should be exchanged to System 2.

If all the above steps are successful, the integration between the two systems is properly configured.

If any of the above steps is unsuccessful, the following checklist can help you to troubleshoot possible problems.

Symptoms	Checklist
In step 2, the Incident record does not appear in System 1.	• In System 1, check the Service Manager Integration Suite (SMIS) task queue and task log. • In System 1, check the integration instance: ◦ Is the integration instance active? ◦ Is the information in the **General** tab correct? ◦ Have you done any customization when you set up the integration instance? • In System 1, check the log file. For more information about how to check the log file, see "Review log file" on page 365. • In System 2, check the account setting, and make sure that the Incident record is accessible by the integration account. see "Configure the integration account" on the previous page.
In step 4, the update in System 1 cannot be exchanged to System 2.	• In System 1, check the SMIS task queue and task log. • In System 1, have you done any customization when you set up the integration instance? • In System 1, check the outbound rule, and make sure that the update to the Incident record can trigger the outbound rule. See "Create and invoke outbound rules" on page 333. • Check the log file. For more information about how to check the log file, see "Review log file" on page 365.

For additional tips about how to troubleshoot the Case Exchange integration, see "Troubleshooting tips" on page 386.

Using the Push mechanism

This chapter describes how to set up the Case Exchange integration between two HP Service Manager systems (System 1 and System 2) by using the Push mechanism.

In this mechanism, both systems use an integration instance that is based on the **CaseExchangeSM_SM_Push** template. You need to perform the following configurations in both HP Service Manager systems:

Configure the integration account

Each system must have a properly configured account for the integration so that the other system can connect by using this account. This account must meet the following requirements:

- This account must have the **RESTful API** execution capability.
- This account must have the rights to retrieve and update Incident records.
- This account must use the same **Time Zone** and **Date Format** settings as the HP Service Manager systems. See also "Time difference issue" on page 380.

Add and enable an integration instance

Applies to User Roles:

System Administrator

To add an integration instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Click **Add**. The **Integration Template Selection** wizard opens.
3. Select **CaseExchangeSM_SM_Push** from the **Integration Template** list, select the **Import Mapping** check box, and then click **Next**.
4. Complete the fields on the **Integration Instance Information** page as necessary, and then click **Next**.

   For more information on how to configure this page, refer to the following online help topic:

System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Add or delete an integration instance > Integration Instance Information fields

5. In the **Integration Instance Parameters** page, configure the following settings and use the default setup for all the other settings.

   Note: You can modify the other fields according to your needs. For more information about how to modify the fields in this page, refer to the following section in the online help:

   System Administration > Integrations > Case Exchange framework > Enable Case Exchange with another system > Add a Case Exchange integration > Configuration details

   a. In the **General** tab, configure the following fields or options:

      Endpoint System runs Process Designer on the exchanged Object: Select this option if Process Designer is implemented in the endpoint system. Otherwise, do not select this option.

      Base URL: The value of this field represents the base URL of the endpoint API. For example, `http://{endpoint server}:13080/SM/9`

      User Name and **Password**: The credentials of the integration account in the endpoint system.

      Note:

      - The **Password** field must not be empty.
      - This account must be properly configured in the endpoint system. For more information, see "Configure the integration account" on the previous page.

   b. On the **Outbound** tab, set the *<Endpoint_instance_ID>* in all rows of the **Additional path** column:

      ```
      {"CEIncidentPush": {"InstanceID": "<Endpoint_instance_
      ID>","InternalID":"${context.externalId}", "ExternalID":
      "${context.internalId}", "IncidentID":"${context.externalId}",
      "ExternalStatus":"${context.internalObject['problem.status']}"}}
      ```

      <Endpoint_instance_ID> is the ID of the SMIS integration instance in the other Service Manager system. You can find this ID under the **Id** column when you open Integration Manager in the other Service Manager system.

c. If you need to exchange attachments, select the **Activate attachment exchange** option on the **Attachment Handling** tab.

6. Click **Next**. The **Integration Instance Fields** page opens.
7. Modify the default entries in the **SM Fields** and **Endpoint Fields** if you have customized fields. Otherwise, go to the next step.

   Note: Endpoint field names must be the same as the caption names in web service **CEIncidentsPush**. For more information about the caption names configured in **CEIncidentsPush**, click **Tailoring** > **Web Service** > **Web Service Configuration** in Service Manager. In addition, you can refer to the out-of-box settings of the **Field Name** field in the **Endpoint Fields** tab.

8. Click **Next**. The **Integration Instance Mapping** page opens.
9. Configure field and value mappings if you have customized fields. Otherwise, go to the next step.

   For more information about how to edit the settings in this page, refer to the following section in the online help:

   System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Add or delete an integration instance > Integration Instance Mapping

10. Click **Finish**.

To enable the integration instance, follow these steps:

1. Click **Tailoring** > **Integration Manager**. Integration Instance Manager opens.
2. Select the integration instance that you want to enable.
3. Click **Enable**.
4. Click **Yes**.

Create and invoke outbound rules

This chapter introduces how to create and invoke outbound rules when you use the Push mechanism.

In Case Exchange, outbound rules implement business logic to drive a workflow or a process. Rules can help perform calculations, validate fields based on data or Rule Sets, set required fields, and more. A Rule Set uses role-based security.

Create outbound rules

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

For an example of the outbound rule configuration, see the screen shot on page 334.

Note: When you create a Rule Set for Incident exchange, set the **Table name** field to `probsummary`.

Condition (RAD expression)	Event
assignment in $L.file="*<assignment group>*" and problem.status in $L.file isin {"Pending Customer", "Pending Vendor"} and sysmoduser in $L.file~="*<smis_scheduler_name>*" and sysmoduser in $L.file~="*<endpoint_integration_user>*" and jscall ("CaseExchangeExternalReferencesDAO.getExternalID",number in $L.file)=""	Create
(not same(problem.status in $L.file, problem.status in $L.file.save) or $apm.activity isin {"Communication with customer","Communication with vendor"}) and not (problem.status in $L.file isin {"Rejected","Resolved","Closed"}) and sysmoduser in $L.file~="*<smis_scheduler_name>*" and sysmoduser in $L.file~="*<endpoint_integration_user>*" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true	Update
not same(problem.status in $L.file, problem.status in $L.file.save) and problem.status in $L.file isin {"Resolved","Closed"} and resolution.code in $L.file~="Request Rejected" and sysmoduser in $L.file~="*<smis_scheduler_name>*" and sysmoduser in	Resolve

Condition (RAD expression)	Event
$L.file~=" *<endpoint_integration_user>*" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true	
not same(problem.status in $L.file, problem.status in $L.file.save) and problem.status in $L.file isin {"Rejected","Resolved","Closed"} and resolution.code in $L.file="Request Rejected" and sysmoduser in $L.file~=" *<smis_ scheduler_name>*" and sysmoduser in $L.file~=" *<endpoint_integration_user>*" and jscall ("CaseExchangeExternalReferencesDAO.isExternalActive","probsummary",number in $L.file)=true	Reject
(sysmoduser in $L.file=" *<smis_scheduler_name>*" or sysmoduser in $L.file=" *<endpoint_integration_user>*") and (jscall ("CaseExchangeExternalReferencesDAO.getExternalID",number in $L.file)="" or not same(problem.status in $L.file, problem.status in $L.file.save))	Acknowledge

Note: Be careful with the outbound conditions to avoid a loop between the integrated systems.

For more information about the **getExternalID** and **isExternalActive** functions, see "Functions used in rule conditions" on page 380.

For more information about how to create Rule Sets, refer to the following topics in the 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*
- *System Administration > Application Setup > Process Designer > Using the Condition Editor*

Invoke Rule Sets

If Process Designer is implemented in HP Service Manager, you can invoke Rule Sets from workflows. For more information, see "Invoke Rule Sets from workflows" on page 314.

If Process Designer is not implemented in Service Manager, you must invoke Rule Sets from triggers. The following table contains example configurations for two triggers: Incident update and Incident creation.

Trigger	Incident update	Incident creation
Trigger Name	case.exchange-update	case.exchange-creation
Table Name	probsummary	probsummary
Trigger Type	4 - After Update	2 - After Add
Script	lib.CaseExchange_RuleExecute.executeSingleRuleSet(record, oldrecord,"CERule4SM2SM")	lib.CaseExchange_RuleExecute.executeSingleRuleSet(record, oldrecord,"CERule4SM2SM")

Note: In this example, the Rule Set ID is `CERule4SM2SM`.

For more information about how to invoke Rule Sets from triggers, see "Invoke Rule Sets from triggers" on page 315.

Test and troubleshoot the integration

Once you have finished the above configurations in the two HP Service Manager systems, you can test the Case Exchange integration. The following procedure is an example that you can follow to test the basic functions of the integration:

1. In System 2, create a new Incident record. This Incident record must be able to trigger the outbound rule that is configured in System 2. See "Create and invoke outbound rules" on page 343.
2. The Incident record should be exchanged to System 1.
3. In System 1, update the Incident record so that the update can trigger the outbound rule that is configured in System 1. See "Create and invoke outbound rules" on page 343.
4. The update to the Incident record should be exchanged to System 2.

If all the above steps are successful, the integration between the two systems is properly configured.

If any of the above steps is unsuccessful, the following checklist can help you to troubleshoot possible problems.

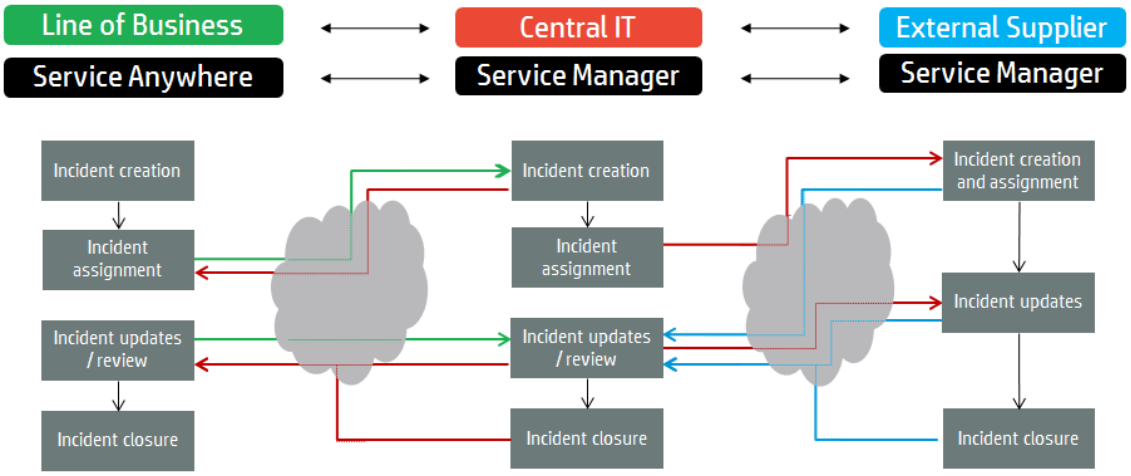
Symptoms	**Checklist**
In step 2, the Incident record does not appear in System 1.	• In System 2, check the Service Manager Integration Suite (SMIS) task queue and task log. • In System 2, check the integration instance: ◦ Is the integration instance active? ◦ Is the information in the **General** tab correct? ◦ Have you done any customization when you set up the integration instance? • In System 2, check the log file. For more information about how to check the log file, see "Review log file" on page 365. • In System 2, check the outbound rule, and make sure that the update to the Incident record can trigger the outbound rule. See "Create and invoke outbound rules" on page 343. • In System 1, check the account setting. See "Configure the integration account" on page 340.
In step 4, the update in	• In System 1, check the SMIS task queue and task log.

Symptoms	Checklist
System 1 cannot be exchanged to System 2.	• In System 1, have you done any customization when you set up the integration instance? • In System 1, check the outbound rule, and make sure that the update to the Incident record can trigger the outbound rule. See "Create and invoke outbound rules" on page 343. • In System 1, check the log file. For more information about how to check the log file, see "Review log file" on page 365. • In System 2, check the account setting. See "Configure the integration account" on page 340.

For additional tips about how to troubleshoot the Case Exchange integration, see "Troubleshooting tips" on page 386.

Incident exchange scenarios

This chapter describes various scenarios that are supported by Case Exchange in the Incident Management module. The following diagram shows a typical Case Exchange environment.



The description of the following scenarios uses the following simplifications to keep the scenarios generic:

- These scenarios refer to an Incident record in the target system as an "Incident". However, an Incident in Service Manager may correspond to an Incident, a Work Order, a Service Request, or something else in the connected system.
- The terminology used for the described scenarios is limited to the domain of Service Manager.

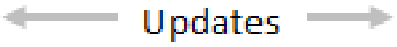
The following scenario diagrams in this chapter contain the following elements:

User actions:

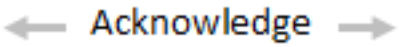
 Actions that move a record from one stage to another. For example, open, assign, solve, close, and so on.

 Updates that do not move a record from one stage to another. For example, an update to description or attachments.

Background system actions:



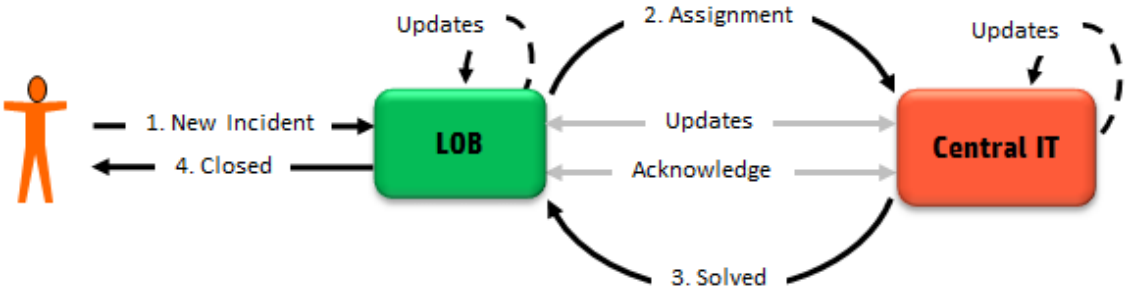
Updates transferred to the connected systems.



Always sent as soon data is exchanged (both directions).

Scenario 1

The Line of Business registers and assigns an Incident to the Central IT, who then solves the Incident.



Scenario description:

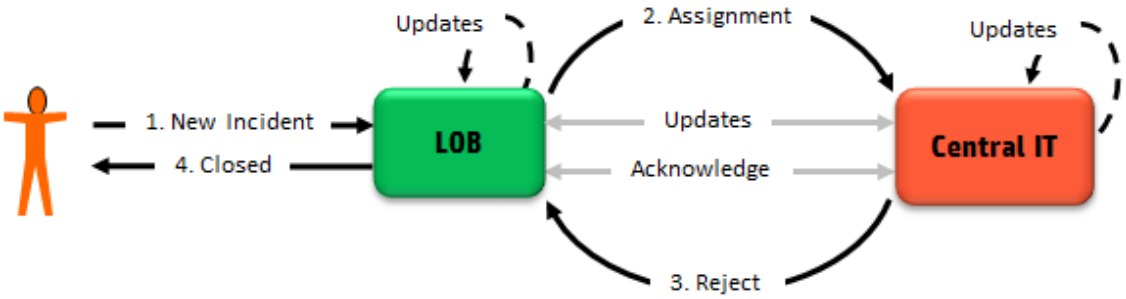
In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT solves the Incident.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT. With this assignment the Incident data is exchanged from the Line of Business to the Central IT.
Updates	Updates can happen on either side. Case Exchange transfers the update to the other side when needed.

Action	Description
3 Solved	The Central IT solves the Incident.
4 Closed	The Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 2

The Line of Business registers and assigns an Incident to the Central IT, who then rejects the Incident.



Scenario description:

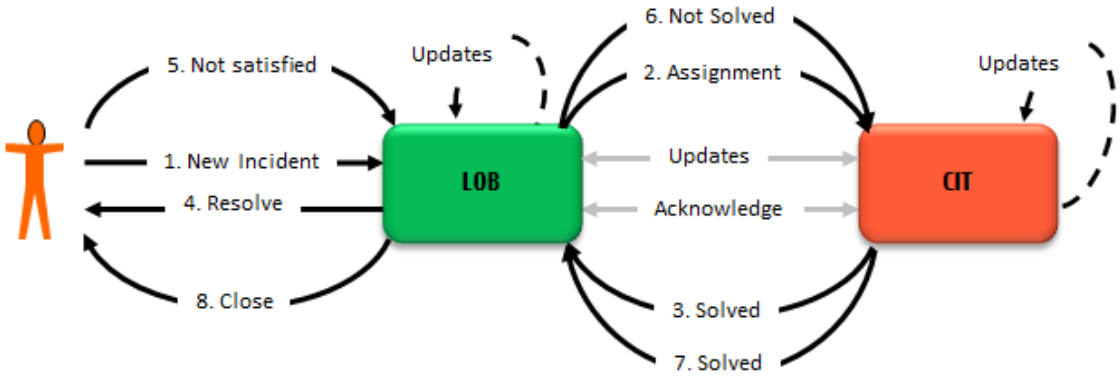
In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT rejects the Incident.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Reject	The Central IT sends a `Reject` update, which indicates the Incident is rejected (external Incident status). The responsibility is back to the Line of Business, who then solves the Incident internally.
Updates	Updates can happen on either side. Case Exchange transfers the update to the other side when needed.
4 Closed	The Line of Business confirms the solution with the end user and closes the Incident.

Action	Description
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 3

The Line of Business registers an Incident and the Central IT solves the Incident. The solution does not satisfy the customer. The Central IT must solve the Incident again.



Scenario description:

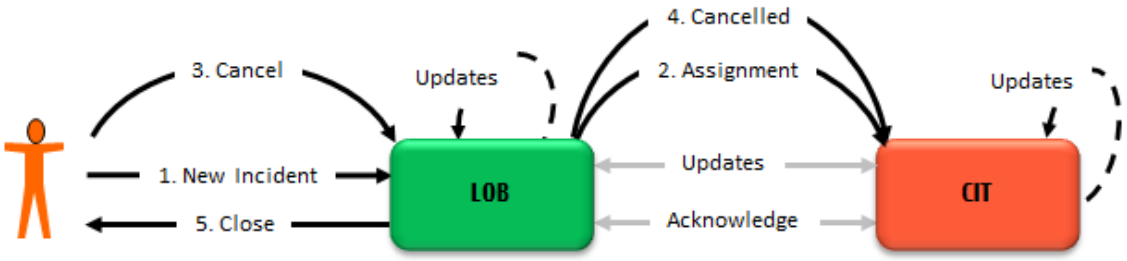
In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT solves the Incident. The Line of Business confirms the solution with the end user, but the end user is not satisfied. Therefore, the Incident is reassigned (re-opened or re-created) to the Central IT.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
Updates	The Central IT analyzes and updates the Incident. Case Exchange transfers the update to the other side when needed.
3 Solved	The Central IT solves the Incident.
4 Resolve	The Line of Business confirms the solution with the end user for the closure of the Incident.

Action	Description
5 Not satisfied	The end user is not satisfied. The Incident needs to be re-opened or re-created.
6 Not solved	The Line of Business reassigns the Incident to the Central IT. In this case, Case Exchange handles the Incident as follows: • In case the Incident is **Closed** in the Central IT, ◦ If the Central IT does not support the re-open of an Incident, Case Exchange recreates the Incident. ◦ If the Central IT supports the re-open of a Incident, Case Exchange sets the Incident status to **Work in progress**. • In case the Incident is just **Resolved** in the Central IT, Case Exchange sets the status to **Work in progress**.
7 Solved	The Central IT solves the Incident.
8 Closed	The Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 4

The Line of Business registers and assigns an Incident to the Central IT. However, the Incident is no longer relevant for customer (cancel and withdrawal).



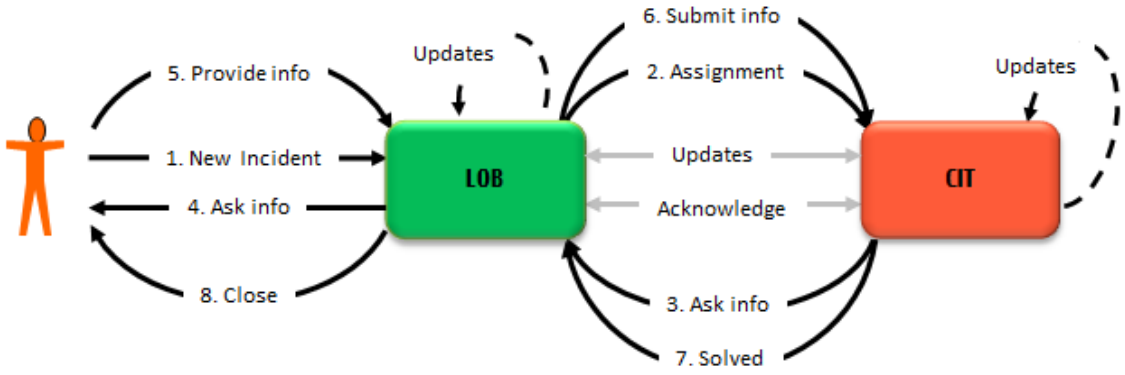
Scenario description:

In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. However, the end user indicates that the issue no longer exists and cancels the Incident.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
Updates	The Central IT analyzes and updates the Incident. Case Exchange transfers the update to the other side when needed.
3 Cancel	The end user cancels the Incident.
4 Cancelled	The Line of Business cancels the Incident. Once cancelled, the Incident is directly closed.
5 Closed	The Line of Business closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 5

The Line of Business registers and assigns an Incident to the Central IT. The Central IT asks for additional information (Pending Customer).



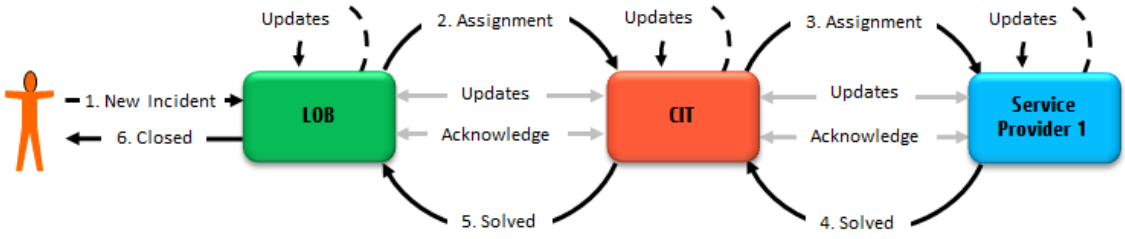
Scenario description:

In this scenario, an end user creates an Incident. The Line of Business registers and assign the Incident to the Central IT. The Central IT requests for missing information and sets the status to **Pending Customer**. The Incident ownership is back to the Line of Business, who must collect the missing information.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
Updates	The Central IT analyzes and updates the Incident. Case Exchange transfers the update to the other side when needed.
3 Ask info	The Central IT assigns the Incident back to the Line of Business to request for additional information. The Incident status in the Central IT's system is **Pending customer**.
4 Ask info	The Line of Business receives the update and contacts the end user.
5 Provide info	The end user provides the information.
6 Submit info	The Line of Business updates the Incident, and then re-assigns the Incident to the Central IT.
Updates	Updates can happen on either side. Case Exchange transfers the update to the other side when needed.
7 Solved	The Central IT solves the Incident.
8 Closed	Service Desk confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 6

The Line of Business registers an Incident, which is then assigned to the Central IT. The Central IT then assigns the Incident to Service Provider 1.



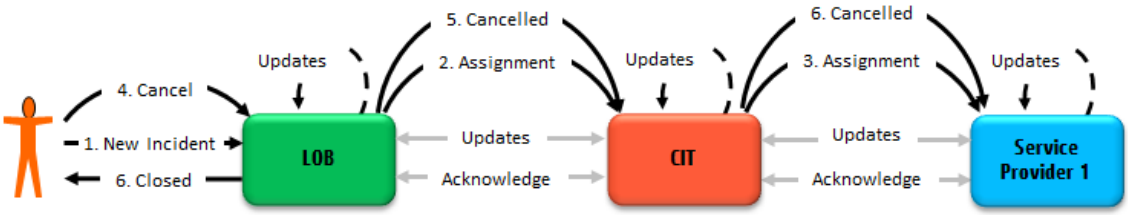
Scenario description:

In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT then assigns the record to Service Provider 1. Service Provider 1 solves the record.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Assignment	The Central IT assigns the Incident to Service Provider 1.
Updates	Updates can happen on any side. Case Exchange transfers the update to other sides when needed.
4 Solved	Service Provider 1 solves the Incident. The responsibility is back to the Central IT, who reviews the resolution.
5 Solved	The Central IT passes the Incident back to the Line of Business.
6 Closed	The Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 7

The Line of Business registers and assigns an Incident to the Central IT. The Central IT then assigns the Incident to Service Provider 1. However, the Incident is no longer relevant for customer.



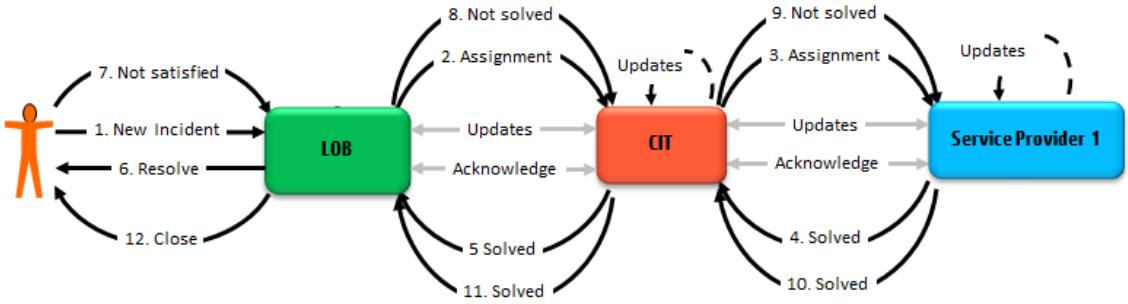
Scenario description:

In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT then assigns the Incident to Service Provider 1. However, the end user indicates that the issue no longer exists and cancels the Incident.

Action	Description
1 New Incident	A user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Assignment	The Central IT assigns the Incident to Service Provider 1.
Updates	Updates can happen on any side. Case Exchange transfers the update to other sides when needed.
4 Cancel	The end user cancels the Incident.
5 Cancelled	The Line of Business sends the cancellation to the Central IT.
6 Cancelled	The Central IT sends the cancellation to Service Provider 1.
7 Closed	The Line of Business closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 8

The Line of Business registers and assigns an Incident to the Central IT. The Central IT assigns the Incident to the Service Provider 1. Service Provider 1 solves the Incident. The solution does not satisfy the customer, Service Provider 1 must solve the Incident again.



Scenario description:

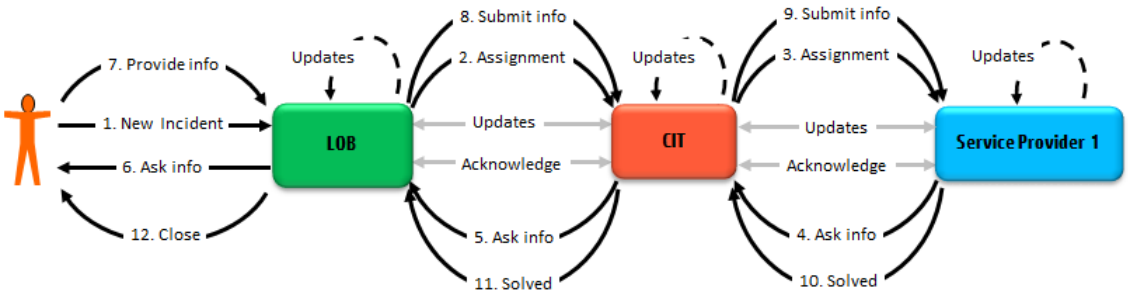
In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT then assigns the Incident to Service Provider 1. Service Provider 1 solves the Incident and the solution is passed to the Line of Business. The Line of Business confirms the

solution with the customer, but the customer is not satisfied. Therefore, the Incident is reassigned (re-opened or re-created) to the Service Provider 1.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Assignment	The Central IT assigns the Incident to Service Provider 1.
Updates	Updates can happen on any side. Case Exchange transfers the update to other sides when needed.
4, 5 Solved	Service Provider 1 solves the Incident, and the solution is passed to the Line of Business.
6 Resolve	The Line of Business confirms the solution with the end user for the closure of the Incident.
7 Not satisfied	The end user is not satisfied.
8, 9 Not solved	The Incident is reassigned to Service Provider 1.
10, 11 Solved	Service Provider 1 solves the Incident, and the solution is passed to the Line of Business.
12 Closed	The Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 9

The Line of Business registers and assigns an Incident to the Central IT. The Central IT assigns the Incident to Service Provider 1. Service Provider 1 asks for additional information (Pending Customer).



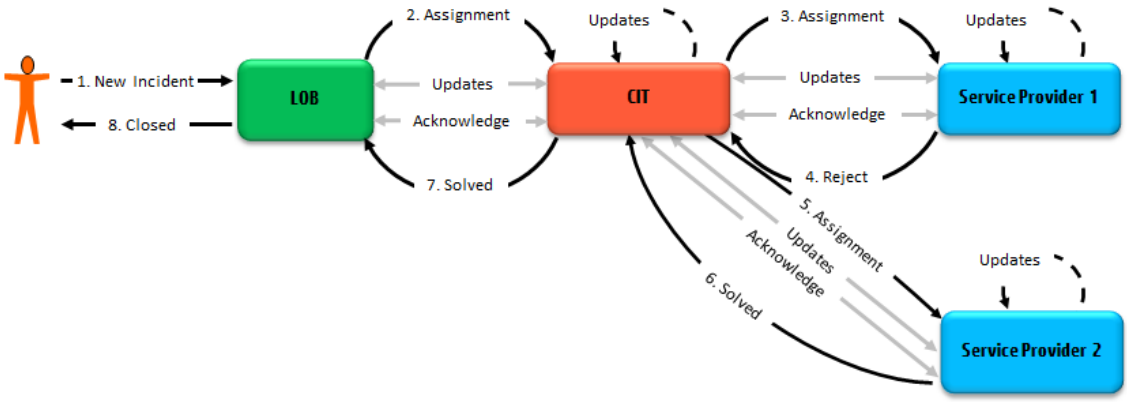
Scenario description:

In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT assigns the Incident to Service Provider 1. Service Provider 1 requests for missing information and sets the status to **Pending Customer**. The Incident ownership is then back to the Central IT and then back to the Line of Business, who must collect the missing information.

Action	Description
1 New Incident	An end user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Assignment	The Central IT assigns the Incident to Service Provider 1.
4, 5 Ask info	The Service Provider 1 assigns the Incident back to the Central IT to request for additional information. The Incident is passed back to the Line of Business.
6 Ask info	The Line of Business receives the update and contacts the end user.
7 Provide info	The end user provides the information.
8, 9 Submit info	The Incident is updated and re-assigned to Service Provider 1.
Updates	Updates can happen on any side. Case Exchange transfers the update to other sides when needed.
10, 11 Solved	Service Provider 1 solves the Incident, and the solution is passed back to the Line of Business.
12 Closed	The Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 10

The Line of Business registers and assigns an Incident to the Central IT. The Central IT should assign the Incident to Service Provider 2, but incorrectly assigns the Incident to Service Provider 1.



Scenario description:

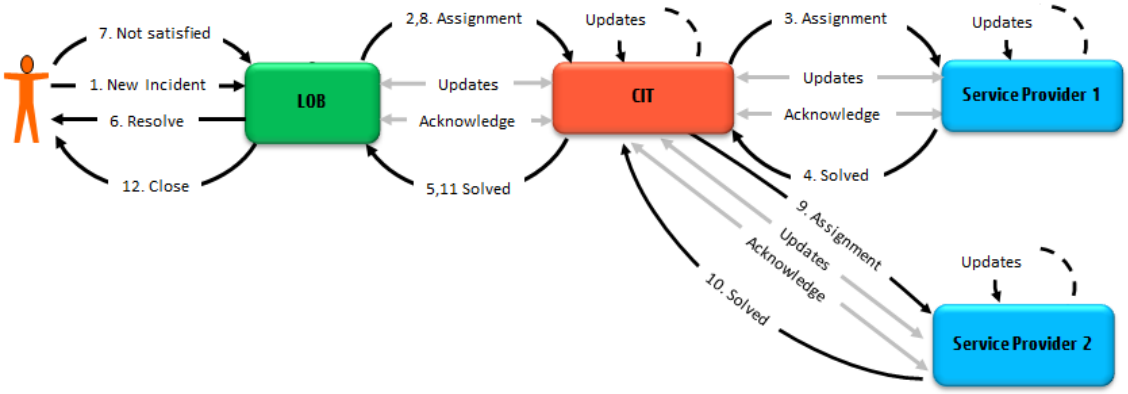
In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT incorrectly assigns the Incident to Service Provider 1, who is not responsible for the Incident and then rejects the Incident. The Central IT then assigns the Incident to Service Provider 2.

Action	Description
1 New Incident	A user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Assignment	The Central IT assigns the Incident to Service Provider 1.
4 Reject	Service Provider 1 rejects the Incident. The Incident ownership is back to the Central IT, who reviews the update from Service Provider 1.
5 Assignment	The Central IT assigns the Incident to Service Provider 2.
6,7 Solved	Service Provider 2 solves the Incident, and the solution is passed to the Line of Business.
Updates	Updates can happen on either side. Case Exchange transfers the update to the other

Action	Description
	side when needed.
8 Closed	Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 11

The Line of Business registers and assigns an Incident to the Central IT. The Central IT assigns the Incident to Service Provider 1. Service Provider 1 provides an unsatisfactory solution. The Central IT then assigns the Incident to Service Provider 2.



Scenario description:

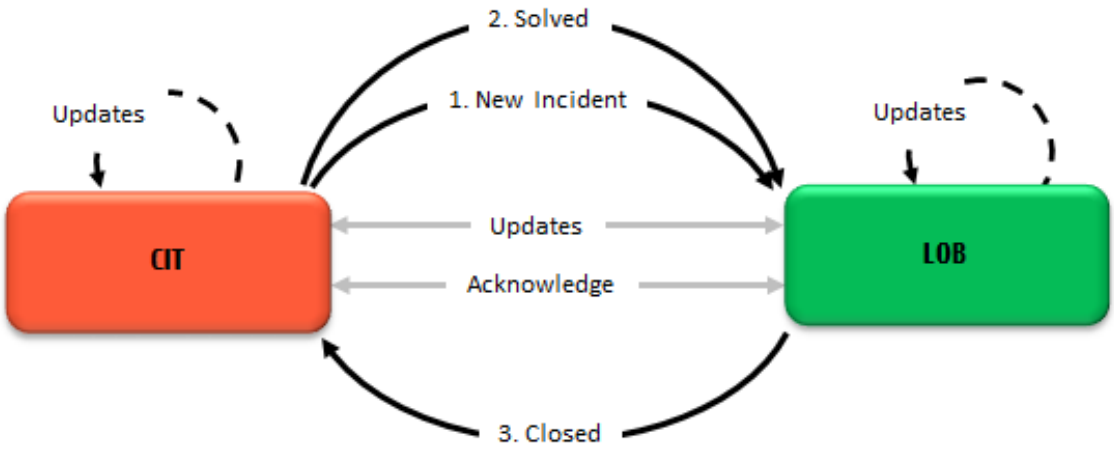
In this scenario, an end user creates an Incident. The Line of Business registers and assigns the Incident to the Central IT. The Central IT assigns the Incident to Service Provider 1, who then provides a solution that does not satisfy the end user. The Central IT then assigns the Incident to Service Provider 2.

Action	Description
1 New Incident	A user calls the Line of Business to create a new Incident.
2 Assignment	The Line of Business assigns the Incident to the Central IT.
3 Assignment	The Central IT assigns the Incident to Service Provider 1.

Action	Description
Updates	Updates can happen on any side. Case Exchange transfers the update to other sides when needed.
4,5 Solve	Service Provider 1 solves the Incident, and the solution is passed to the Line of Business.
6 Resolve	The Line of Business confirms the solution with the end user for the closure of the Incident.
7 Not satisfied	The end user is not satisfied.
8,9 Assignment	The Incident is assigned to Service Provider 2.
10,11 Solved	Service Provider 2 solves the Incident, and the solution is passed to the Line of Business.
12 Closed	The Line of Business confirms the solution with the end user and closes the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 12

The Central IT detects and solves an Incident, and sends the Incident to the Line of Business.



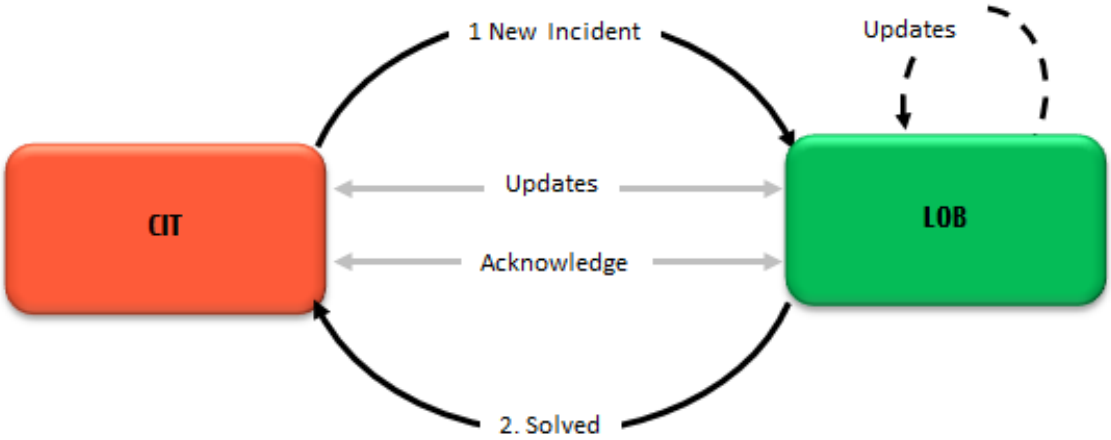
Scenario description:

In this scenario, the Central IT creates and solves an Incident, which affects the Line of Business. The Central IT sends the Incident to the Lind of Business for informational purposes. The Line of Business confirms the resolution of the Incident.

Action	Description
1 New Incident	The Central IT creates a new Incident and forward the Incident to the Line of Business.
2 Solved	The Central IT solves the Incident and sends a `Solved` update to the Line of Business.
3 Closed	Service Desk confirms the solution to close the Incident.
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 13

The Central IT creates an Incident that must be solved by the Line of Business.



Scenario description:

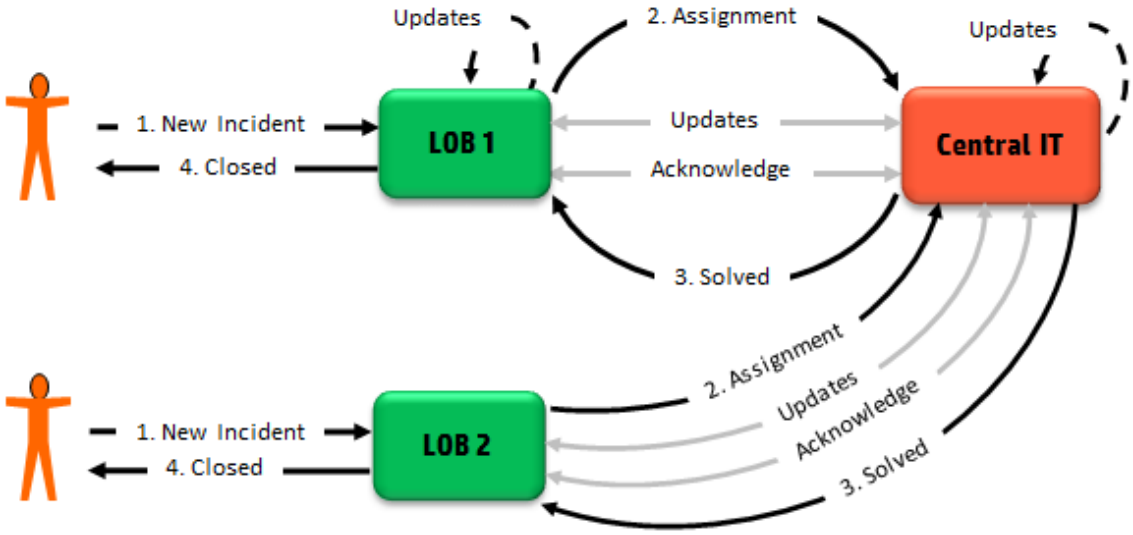
In this scenario the Central IT creates an Incident, which has to be solved by the Line of Business.

Action	Description
1 New Incident	The Central IT creates a new Incident and assigns the Incident to the Line of Business.
Updates	Updates are transferred between both systems.
2 Solved	The Line of Business solves the Incident.

Action	Description
Background	
Updates	Updates in any of the systems are transferred to the other side.
Acknowledge	Each time data is transferred, an Acknowledgment has to happen.

Scenario 14

Two Line of Business systems are connected to the Central IT.



Scenario description:

In this scenario, two Line of Business systems connect to the Central IT. The actions in the above scenarios (for example, pending customer, reject, customer dissatisfaction, and so on) are still valid.

Common user tasks

This chapter introduces the common user tasks that apply to the Incident Management module in the Case Exchange integration:

Update an Incident

When HP Service Manager owns an Incident record, you can directly make any update you want. The configuration of the Case Exchange integration determines if the update will be transferred to the endpoint.

When the endpoint system owns a record, the Incident record is read-only in Service Manager. However, you can still provide additional information to the record, and Case Exchange can transfer the information to the record in the endpoint system. To do this, follow these steps:

1. Open the Incident record.
2. Click **Update**.
3. Choose an appropriate value in the **Activity type** field, provide the information in the **Description** field.
4. Make sure the **Take back control** check box is not selected.
5. Click **Finish**.

Case Exchange then transfers the information to the record in the endpoint. In Service Manager, you can view the information in the **Journal Updates** field under the **Activities** section.

Take back an Incident

When the endpoint system owns a record, the related Incident record is read-only in Service Manager. In case the endpoint system does not respond or something unforeseen happens, you may want to take back the ownership of the record. To take back the ownership of an Incident record, follow these steps:

1. Open the Incident record.
2. Click **Update**.
3. Choose an appropriate value in the **Activity type** field, fill the **Description** field.
4. Select the **Take back control** check box.
5. Click **Next**.

The ownership of the record then returns to Service Manager.

Check activity logs of an Incident record

You can view the log of the activities that occurred to an Incident record in two sections:

- The **Activities** section: This section displays the log of all the activities that occurred to the Incident record, including the Case Exchange tasks.
- The **Case Exchange** section: This section only displays the log of all the Case Exchange tasks. This section is available only when the following conditions are true:
  - A Case Exchange integration instance is active.
  - The Incident record had a Case Exchange task.

  For more information about the **Case Exchange** section, see "Audit and logging" on page 301.

To check the activity log of an Incident record from the **Activities** section, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Expand the **Activities** section and check the activity log.

To check the log of Case Exchange tasks, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Expand the **Case Exchange** section, expand the **Log** subsection, and then check the log of the Case Exchange tasks.

Restart an unsuccessful Case Exchange task

Once a Case Exchange task occurs to an Incident record, the Incident record has a **Case Exchange** section that displays the history of all Case Exchange tasks. You can restart an unsuccessful Case Exchange task from the **Case Exchange** section. To do this, follow these steps:

Note: If you want to restart an unsuccessful Case Exchange task of an Incident record, you must

have the Update right on that Incident record.

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Select the Incident record.
4. Expand the **Case Exchange** section, and then expand **Log**.
5. Click the link on the date and time link of the unsuccessful Case Exchange task. The **Integration Task Log** page opens.
6. Click the **View** button after the **Task ID** field. The **Integration Failover Task Queue** page opens.
7. Click **Run Now**.

System administrator tasks

This chapter introduces the system administrator tasks in the Case Exchange integration:

Review log file

Applies to User Roles:

System Administrator

The standard Service Manager log file contains detailed information about the actions of a Case Exchange integration instance.

When you create the Case Exchange integration instance, you can define the following settings for the Service Manager log file:

- Log Level: Level of diagnostic information that the Service Manager server logs to the log file directory.
- Log File Directory: The location where log files will be stored. If you do not configure this option, the default log for this integration instance is ***<Server home directory>*/logs/sm.log**.

For more information, see "Integration Instance Information fields" on page 75.

Handle long-running tasks

Applies to User Roles:

System Administrator

Follow the these steps to identify a "long-running" task:

1. Log in to Service Manager as system administrator.
2. Click **Tailoring** > **Integration Manager**.
3. Click **Log**, set the **Status** field to **In Progress**, and then click **Filter**.

If a task remains in the **In Progress** status for a long time, then this task is a "long-running" task.

Follow these steps to handle a "long-running" task:

1. Log in to Service Manager as system administrator.
2. Click **Tailoring** > **Integration Manager**.
3. Select the integration instance to which the "long-running" task belongs, and then click **Disable**.
4. Click **Miscellaneous** > **System Status**, and then wait until the scheduler for the integration instance disappears.

   Note: You need to click the **Refresh Display** button to see the latest system status.

5. Go back to Integration Manager, select the corresponding integration instance, and then click **Task**.
6. Open the "long-running" task.
7. Perform one of the following actions according to your needs:
   - Click the **Merge** button and then manipulate the data in the task.

     This action only applies to the outbound tasks.
   - Select the **Expired** check box.

In this way, the task will not be processed.

- Click the **Delete** button to delete the task.

  In this way, you may have to ask the integration partner to resend the record. Be careful when you delete a task, this action may results in data loss.

Case Exchange reference material

This section provides the Case Exchange reference material.

Edit the query and pagination query strings

This topic provides specifications to explain how to configure the strings for the query parameter and pagination query parameter under the **Inbound** tab when you set up a Case Exchange integration instance. This topic includes the following collections:

- Filter
  The *filter* query parameter specifies a filtering condition for a resource collection. The service must return only resources that meet the specified condition. The following table lists the operators.

Operator/Variable	Logical operator	Boolean operator	Description	Example
General Variables	${*object*}	${*object*}	A placeholder for all parameters in SMIS configuration, in which the value cannot be predefined but during running time or depends	${param.lastPullingTime} ${vars.$epfieldsAlias}

Operator/Variable	Logical operator	Boolean operator	Description	Example
			on other parameters. The *object* placeholder can be *sm*, *ep*, *param*, *context*,or *vars*.	
	Service Manager records	sm	Query the record in Service Manager.	Get the description of an incident in Service Manager: ${sm.action}
	End point	ep	Query the record in the end point.	Get the description of an incident in the end point: ${ep['properties.description']}
	Parameters	param	Query all parameters defined in the Service Manager configuration.	Get the object defined in the Service Manager configuration: ${param.object}
	Context information	context	Query all task-related information such as internal ID and external ID.	Get the incident Id in Service Manager: ${context.internalId}
	Variables	vars	Query all variables in Service Manager.	Get the current login users: ${vars.$lo_operator}

Operator/Variable	Logical operator	Boolean operator	Description	Example
Special variables for Case Exchange	Current page offset	$currentPageOffset	Query the index of the first record on the current page in all records. This variable is defined in the Case Exchange framework and is only used by the pagination parameter.	${vars.$currentPageOffset}
Logical Operators	And	and	Evaluates to true if the left and right operands evaluate to true, otherwise evaluates to false.	http://domain/resource?filter=Id gt 1000 and Name eq 'Jake' http://domain/resource?filter=Id > 1000 and Name = 'Jake'
	Or	or	Evaluates to true if at least one of the left and right operands evaluates to true, otherwise evaluates to false.	http://domain/resource?filter=Id gt 1000 or Name eq 'Jane' http://domain/resource?filter=Id > 1000 or Name = 'Jane'

Operator/Variable	Logical operator	Boolean operator	Description	Example
Comparison Operators	Equals	eq =	Evaluates to true if the left and right operands are equal, otherwise evaluates to false.	http://domain/resource?filter=Rank eq 2 http://domain/resource?filter=Rank = 2
	Not Equals	ne !=	Evaluates to true if the left and right operands are not equal, otherwise evaluates to false.	http://domain/resource?filter=Rank ne 2 http://domain/resource?filter=Rank != 2
	Greater Than	gt >	Evaluates to true if the left operand is greater than the right operand, otherwise evaluates to false.	http://domain/resource?filter=Rank gt 2 http://domain/resource?filter=Rank > 2
	Greater or Equals	ge >=	Evaluates to true if the left operand is greater than or equals to the right operand, otherwise evaluates	http://domain/resource?filter=Rank ge 2 http://domain/resource?filter=Rank >= 2

Operator/Variable	Logical operator	Boolean operator	Description	Example
			to false.	

Operator/Variable	Logical operator	Boolean operator	Description	Example
	Less Than	lt <	Evaluates to true if the left operand is less than the right operand, otherwise evaluates to false.	http://domain/resource?filter=Rank lt 2 http://domain/resource?filter=Rank < 2
	Less or Equal	le <=	Evaluates to true if the left operand is less than or equals to the right operand, otherwise evaluates to false.	http://domain/resource?filter=Rank le 2 http://domain/resource?filter=Rank <= 2
	Between	btw	Evaluates to true if the leftmost operand is in the range defined by the two comma-separated operands in the parenthesis, otherwise evaluates to false. The first	http://domain/resource?filter=LastUpdate btw(2012.01.01, 2013.01.01)

Operator/Variable	Logical operator	Boolean operator	Description	Example
			operand in the parenthesis represents the low limit of the range and the second operand represents the high limit of the range.	
	Not Between	not btw	Evaluates to true if the leftmost operand is not in the range defined by the two comma-separated operands in the parenthesis, otherwise evaluates to false. The first operand in the parenthesis represents the low limit of the range and the second	http://domain/resource?filter=LastUpdate not btw(2012.01.01, 2013.01.01)

Operator/Variable	Logical operator	Boolean operator	Description	Example
			operand represents the high limit of the range. Range boundaries are inclusive.	
	In	in	Evaluates to true if the leftmost operand is equal to one of the expressions in the parenthesis, otherwise evaluates to false.	http://domain/resource?filter=Id in (1,2,3)
	Not In	not in	Evaluates to true if the leftmost operand is not equal to any of the expressions in the parenthesis, otherwise evaluates to false.	http://domain/resource?filter=Id not in(1, 2, 3)
Arithmetic Operators	Add	add +	Evaluates to the sum of the left	http://domain/resource?filter=PreviousRank gt (CurrentRank add 3)

Operator/Variable	Logical operator	Boolean operator	Description	Example
			operand and the right operand in the parenthesis.	http://domain/resource?filter=PreviousRank > (CurrentRank + 3)
	Subtract	sub -	Evaluates to the value that the left operand minus the right operand in the parenthesis.	http://domain/resource?filter=PreviousRank gt (CurrentRank sub 3) http://domain/resource?filter=PreviousRank > (CurrentRank - 3)
	Multiply	mul *	Evaluates to the product that the left operand multiplies the right operand in the parenthesis.	http://domain/resource?filter=PreviousRank lt (CurrentRank mul 3) http://domain/resource?filter=PreviousRank < (CurrentRank * 3)
	Modulo	mod %	Evaluates to the remainder that the left operand divides the right operand in the parenthesi	http://domain/resource?filter=Actual gt Planned and (Planned mod Actual) gt 5 http://domain/resource?filter=Actual > Planned and (Planned % Actual) > 5

Operator/Variable	Logical operator	Boolean operator	Description	Example
			s.	
	Divide	div /	Evaluates to the value that the left operand divides the right operand in the parenthesis.	http://domain/resource?filter=PlannedHours div 10 http://domain/resource?filter=PlannedHours / 10
Parenthesis Operator	Parenthesis	()	Like in math, parenthesis can be used around conditions and expressions to define priority.	http://domain/resource?filter=(x add y) mul (x sub z) http://domain/resource?filter=(x + y) * (x - z)
Unary Operators	Unary Plus	+	Syntax: +number	N/A
	Unary Minus	-	Syntax: -number	N/A

For more information about the *sm*, *ep*, *param*, *context*, and *vars* objects, refer to the following online help topic:

System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Add or delete an integration instance > Integration Instance Mapping > Use placeholders > Placeholder objects

- Layout
  The *layout* query parameter specifies which properties or sub-structure of a data resource should be returned by a service. Similar to SQL, this parameter provides a comma-separated list of properties or multipart properties. The following table lists the operators.

Operator	Description	Example
Selecting Resource Properties	Resource properties are specified by a property name directly.	http://domain/resource?layout=Id,Name,Description
Selecting Related Resource Properties	Related resource properties are specified by a relationship name and a property name.	http://domain/Person?layout=PrimaryAddress.City
Selecting a Sub-Structure Using Multipart Properties	Resources that hold complex object structures can be queried for a sub-structure using multi-part property conventions.	Query a resource named “UserSetting” for a “Select” object, which is a sub-structure of a “Filter” object, which is a sub-structure of a “UserSetting” object. http://domain/UserSetting?layout=Settings.Filter.Select
Selecting Calculated Values	The query protocol supports function and Arithmetic operators.	**Note:** Functions listed in examples below have to be supported by concrete services in order to be valid – these are only examples. ◦ Query a “Formula” resource for the product of a property named “X” and a property named “Y”: http://domain/Formula?layout=X mul Y ◦ Query a “Person” resource for “FirstName” and “LastName” and return a concatenation so “FirstName”, space (“ “) and “LastName”: http://domain/Person?layout=Concat(FirstName, Concat(‘ ’, LastName))

- Size
  The *size* parameter specifies the maximum number of resources requested to be returned.

  Syntax: size=<integer>

  Example: Fetch the first 10 persons with age lower than 30 in ascending order.

  http://domain/Person?layout=FirstName,LastName,Email&filter=Age<30&order=Age asc&size=10

- Skip

The *skip* parameter specifies how many resources should be skipped. In other words, it specifies the starting index of the returned result. When not specified, it is assumed to be zero, meaning that the first resource returned from the data-store is the first resource returned by the queried service.

Syntax: skip=<integer>

Example: Fetch persons, starting from person number 51.

http://domain/Person?layout=FirstName,LastName,Email&skip=50

Specify additional path

In case the outbound JSON request contains a path or element that is mandatory but is not defined in field mapping or entity path, you need to specify this path or element in the **Additional path** field.

For example, in the following scenario:

- An outbound JSON request contains the following content:

```
{
	"entities": [{
		"properties": {
			"DisplayLabel": "sadf",
			"Description": "sdf",
			"ImpactScope": "Enterprise",
			"Status": "Ready",
			"Urgency": "TotalLossOfService",
			"RegisteredForActualService": "10874",
			"Category": "10707"
		},
		"entity_type": "Incident"
	}],
	"operation": "CREATE"
}
```

- The SMIS field mapping defines all the fields under `properties`: `DisplayLabel`, `Description`, `ImpactScope`, `Status`, `Urgency`, `RegisteredForActualService`, and `Category`.
- Field mapping and entity path do not define `entity_type` and `operation`.

In this scenario, you must define the `entity_type` and `operation` fields in the **Additional path** field by using the following string:

```
{"entities":[{"properties":{}, "entity_type":"Incident"}],"operation":"CREATE"}
```

Note: RESTful protocols other than JSON are *not* supported.

Entity path

In an outbound JSON request, entity path is the path above the endpoint field defined in the field mapping.

For example, in a Case Exchange integration instance, all endpoint fields are defined as `properties.****` in the field mapping. The following example is an outbound request body in the endpoint:

```
{
	"entities": [{
		"properties": {
			"DisplayLabel": "Create New Incident",
			"Description": "create the new incident record",
			"ImpactScope": "MultipleUsers",
			"Urgency": "SlightDisruption",
			"Solution": "",
			"Id": "IM118216"
		},
		"ext_properties": {
			"Operation": "Update",
			"ExternalStatus": "Open",
			"ExternalId": "IM45167",
			"ExternalSystem": "SM",
			"ExternalEntityType": "Incident"
		},
		"Comments": [{
			"Body": "IM45167",
			"CreatedTime": 1402038076398
		}],
		"entity_type": "Incident"
	}]
}
```

In this particular example, one of the endpoint fields is `properties.Displaylabel`, so the entity path is `entities[0]`.

Note: RESTful protocols other than JSON are *not* supported.

Technical hints

This chapter provides technical information that helps you better understand Case Exchange.

The `$G.CEOwnershipSM` variable

The `$G.CEOwnershipSM` variable is proprietary for Case Exchange. This variable identifies whether the native system has ownership of a record.

If Process Designer is not implemented, this variable is set in the **im.view.init** process record, and used in the **I/O (If RIO)** field of the **apm.edit.problem** display screen record.

If Process Designer is implemented, this variable is set in the **im.CEUpdate.init** Rule Set, which is injected to the **Incident** workflow under **Workflow Based Rule Sets** > **On display**.

Functions used in rule conditions

The example condition configurations in this document call the following functions:

CaseExchangeExternalReferencesDAO.getExternalID: This function judges if the record is exchanged to the external system. If the record is exchanged to the external system, the following expression returns true:

```
jscall("CaseExchangeExternalReferencesDAO.getExternalID",number in $L.file) ~=""
```

CaseExchangeExternalReferencesDAO.isExternalActive: If a record is in an active Case Exchange life cycle, this function returns TRUE; otherwise, this function returns FALSE.

Time difference issue

In the Pull mechanism, date and time of the last Pull activity is the conclusive query filter to distinguish the new updates in the endpoint system, which will be retrieved in the next Pull activity.

Even the same time zone is applied for the integration, the time difference can occur between the two systems (for example, one system is one minute ahead of another system). Therefore, the system that initiates the Pull request must compensate the time difference between the two systems so that each Pull activity can retrieve the exact updates after the last Pull activity from the endpoint system.

To achieve this goal, you can configure the **Time difference (s)** setting in the integration instance.

Note: For each Pull activity, the time for the query filter is the time in the **Pulling From** field plus

the time (in seconds) defined in the **Time difference (s)** field.

Dealing with HTML tags from Service Anywhere

HP Service Anywhere uses HTML tags for rich text in the **Description**, **Solution**, and **Discussion** fields of an Incident, for example, `<p>`, `<strong>`, `<ul>`, and so on. By default, Service Manager does not parse these tags, but displays these tags directly. To improve the readability of these fields in Service Manager, the out-of-box integration template (**CaseExchangeSM_SAW**) uses pre script to handle these tags in the following manner:

Inbound exchange:

- Automatically removes HTML tags.
- If the content contains an image and the address of the image does not start with "http://" or "https://", the image is downloaded and stored as an attachment, and the following description is appended:

  ```
  And Images are referenced as:
  (1 embedded image(s) <image_name> were downloaded as attachment, please check attachment section)
  ```

  If the download of an image fails, the following description is appended :

  ```
  And Images are referenced as:
  (1 embedded image(s) <image_name> were downloaded failed)
  ```

- If the content contains an image and the address of the image starts with "http://" or "https://", the image is not downloaded and the following description is appended:

  ```
  And Images are referenced as:
  (Images http://<domain_name_or_IP_address>/<image_name> are from internet)
  ```

Outbound exchange:

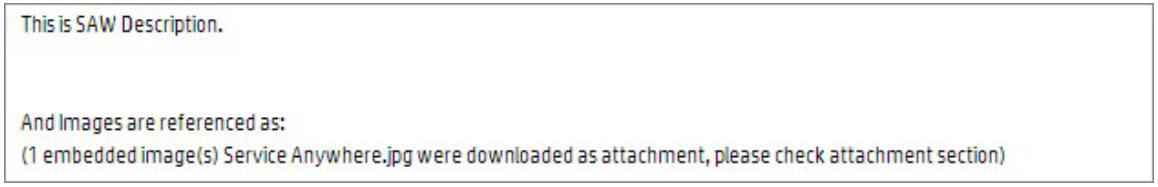
If the content of a field is modified in Service Manager, then all the text in this field will be appended after the original content in Service Anywhere as follows:

```
This is the original text in Service Anywhere.
#####SM START#####
This is the modified text in Service Manager.
#####SM END#####
```

The following example illustrates how this mechanism works in each Case Exchange transfer:

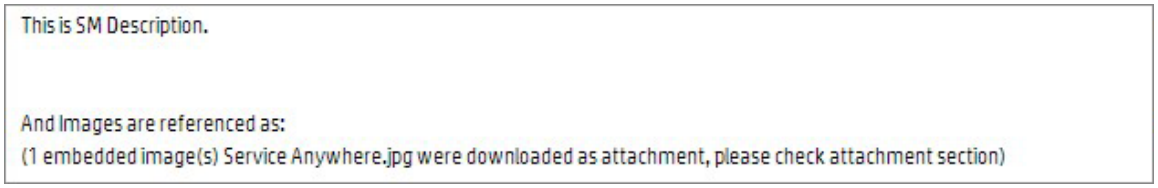
1. The **Description** field of an Incident has the following content in Service Anywhere.

2. After the Incident is exchanged, the Description field has the following content in Service Manager.



And you can find the image in the **Attachments** section.

3. You modify this field in Service Manager as follows.



4. After your update is exchanged to Service Anywhere, the **Description** field in Service Anywhere contains the following information.

If you want to remove or modify this mechanism from the out-of-box integration template, remove or modify the following code in pre script:

```
//remove html tags from SAW
    if(ep['properties.Description']) ep['properties.Description'] = lib.CaseExchange_SAWUtil.processHtmlText(param, context, 'description', ep
['properties.Description']);
    if(ep['properties.Solution']) ep['properties.Solution'] = lib.CaseExchange_SAWUtil.processHtmlText(param, context, 'solution', ep['properties.Solution']);
    if (ep['Comments'] && ep['Comments'].length > 0) {
        for (var i = 0; i < ep['Comments'].length; i++) {
            ep['Comments'][i]['Body'] = lib.CaseExchange_SAWUtil.processHtmlText(param, context, 'comment', ep['Comments'][i]['Body']);
        }
    }

//process the value which will be posted to SAW rich text field
    if(sm['action'] && sm['action'] !== "") {
        if(sm['oldvalues']['action']) sm['action'] = lib.CaseExchange_SAWUtil.processOutboundText(context, 'description', sm['action']);
        if(sm['oldvalues']['action'] === undefined) sm['action'] = null;
    }
    if(sm['resolution'] && sm['resolution'] !== "") {
        if(sm['oldvalues']['resolution']) sm['resolution'] = lib.CaseExchange_SAWUtil.processOutboundText(context, 'solution', sm['resolution']);
        if(sm['oldvalues']['resolution'] === undefined) sm['resolution'] = null;
    }
```

Troubleshooting tips

Consider the following tips when you troubleshoot the Case Exchange integration:

- Incorrect configuration of the **Base URL**, **User Name**, and **Password** fields in the **General** tab usually causes authentication failure. In this scenario, 401 errors are recorded in the log file.
- You can enable the error-handling feature when you configure the integration instance. SMIS can automatically create a new Incident record if a Case Exchange task fails. The **Description** field of this Incident record contains the details of the failed task record. For more information about the error-handling feature, see "Error handling" on page 302.
- Due to a known limitation, the error message in the SMIS task log may be insufficient to identify the root cause of a failed task. For more information about this known limitation and the workaround, see "Insufficient message for a failed Case Exchange task" on page 394.

Out-of-box functions for additional scripts

When you set up the Case Exchange integration, you can specify functions in the **Additional Script** tab in the **Integration Instance Parameters** page to customize the Case Exchange integration in various different environments. This chapter explains the out-of-box functions that you can specify in the **Additional Script** tab.

Set the HTTP header - for authentication

Besides `username` and `password`, the endpoint system (Service Anywhere) also requires `cookie` in the request header to perform authentication. The Javascript function below has the following purposes:

- Set `cookie` to the header for inbound requests
- Set additional 'Content-type' into the header for outbound requests

Out-of-box function:

CaseExchange_SAWUtil.getHttpHeader

The function has the following parameters:

- `direction`: The direction of the action. This parameter has only two values:
  - `lib.smis_Constants.MAPPING_DIRECTION_LEFTRIGHT()`
  - `lib.smis_Constants.MAPPING_DIRECTION_RIGHTLEFT()`

  You can call the `lib.CaseExchange_CommonLib.isOutbound(direction)` or `lib.CaseExchange_CommonLib.isInbound(direction)` function to judge if the action is inbound or outbound.
- `param`: All parameters defined in the SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax. If you change any value in this parameter, the change is saved to the SMIS configuration.

The function returns the following result:

Object: The HTTP Header object

Log in to the external system

Besides user name and password, the endpoint system (Service Anywhere) also requires a cookie in the request header to perform authentication. This cookie comes from another URL of a Software as a Service (SAAS) portal.

The function below performs the following tasks:

1. Log in to the SAAS portal by using the user name and password
2. Extract the cookie from the response
3. Set the cookie to `param`.

The Case Exchange framework then saves the cookie to the SMIS configuration. The succeeding calls can directly retrieve the cookie from the SMIS configuration until the cookie expires.

Out-of-box function:

CaseExchange_SAWUtil.doLoginRequest

The function has the following parameters:

- `param`: All parameters defined in the SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax. If you change any value in this parameter, the change is saved to the SMIS configuration.

The function returns the following result:

N/A

Validate inbound response

Besides the HTTP code in the GET REST response from Service Anywhere, the HTTP body also contains the information of whether the current request is successful. The function below checks the response body to validate this request.

Out-of-box function:

CaseExchange_SAWUtil.validateInboundResponse

The function has the following parameters:

- `param`: All parameters defined in the SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax. The change to any value in this parameter is not saved to the SMIS configuration.
- `response`: The HTTP body of the REST response from end point.

The function returns the following result:

Boolean or String:

- `false`(Boolean): if the request is not validated
- Id of the record in the endpoint (String): if the request is validated

Validate and parse outbound response

Besides the HTTP code in the POST REST response from Service Anywhere, the HTTP body also contains the information of whether the current request is successful. The function below checks the response body to validate this request and extract the Id if the request is validated.

Out-of-box function:

CaseExchange_SAWUtil.validateOutboundResponse

The function has the following parameters:

- `param`: All parameters defined in the SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax. The change to any value in this parameter is not saved to the SMIS configuration.
- `response`: The HTTP body of the REST response from end point.

The function returns the following result:

Object: The HTTP Header object

Inbound and Push post processing activities

The function below retrieves comments of an Incident record from Service Anywhere and insert these comments into the activity log in Service Manager right after the Incident record is exchanged.

Out-of-box function:

CaseExchange_SAW_PostProcessing.postInbound

The function has the following parameters:

- `mapObj`: Final Service Manager value object after field mapping and value mapping.
- `sm`: Temporary Service Manager value object after copying basic data from end point according to field mapping.
- `ep`: Original value object from the end point.
- `context`: Context of the SMIS task. You can get a specific value by using the `context['internalId']` syntax.
- `param`: All parameters defined in SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax.

For more information about these parameters, see "Placeholder objects" on page 86.

The function returns the following result:

N/A

Outbound post processing activities

The function below sends activity log of the current Incident record to Service Anywhere right after the Incident record is exchanged.

Out-of-box function:

CaseExchange_SAW_PostProcessing.postOutbound

The function has the following parameters:

- `mapObj`: Final Service Manager value object after field mapping and value mapping.
- `sm`: Temporary Service Manager value object after copying basic data from end point according to field mapping.
- `ep`: Original value object from the end point.
- `context`: Context of the SMIS task. You can get a specific value by using the `context['internalId']` syntax.
- `param`: All parameters defined in SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax.

For more information about these parameters, see "Placeholder objects" on page 86.

The function returns the following result:

N/A

Set the HTTP header - for attachment

Besides `cookie` in the HTTP header, the endpoint system (Service Anywhere) also requires `fs_filename` to perform attachment exchange. The function below adds `cookie` and `fs_filename` into the HTTP header.

Out-of-box function:

CaseExchange_SAWUtil.getAttachHttpHeader

The function has the following parameters:

- `direction`: The direction of the action. This parameter has only two values:
  - `lib.smis_Constants.MAPPING_DIRECTION_LEFTRIGHT()`
  - `lib.smis_Constants.MAPPING_DIRECTION_RIGHTLEFT()`

  You can call the `lib.CaseExchange_CommonLib.isOutbound(direction)` or `lib.CaseExchange_CommonLib.isInbound(direction)` function to judge if the action is inbound or outbound.
- `param`: All parameters defined in the SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax. If you change any value in this parameter, the change is saved to the SMIS configuration.

- `attachObj`: For inbound activities, this is an instance of `CEAttachment`. For outbound activities, this is an instance of the `Attachment` object in Service Manager.

The function returns the following result:

Object: The HTTP Header object

Retrieve and parse attachment info

The function below performs the following tasks:

- Retrieves attachment information from the endpoint, such as file name, extension, size, and mime_type.
- Set all these information to the `CEAttachmentInfor` object and return the `CEAttachmentInfor` object in an array.

For Service Anywhere, all attachment information comes from the REST response of Incident. For other endpoints, an additional REST request may be required to retrieve the information.

Out-of-box function:

CaseExchange_SAWUtil.getAttachmentInfor

The function has the following parameters:

- `mapObj`: Final Service Manager value object after field mapping and value mapping.
- `sm`: Temporary Service Manager value object after copying basic data from end point according to field mapping.
- `ep`: Original value object from the end point.
- `context`: Context of the SMIS task. You can get a specific value by using the `context['internalId']` syntax.
- `param`: All parameters defined in SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax.

For more information about these parameters, see "Placeholder objects" on page 86.

The function returns the following result:

Array: Array of the `CEAttachmentInfo` object

Parse response of attachment creation

Because the endpoint system (Service Anywhere) needs an additional REST request to update attachment information after the creation of the attachment, the function below parses the endpoint response to the outbound attachment creation request.

Out-of-box function:

CaseExchange_SAWUtil.parseSAWCreateAttachResponse

The function has the following parameters:

- `response`: The HTTP body of the REST response from the end point.
- `action`: Action type to process attachment. Currently this parameter has only two values: `FETCH_ATTACHMENT` and `CREATE_ATTACHMENT`.
- `param`: All parameters defined in SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax.

The function returns the following result:

CEAttachmentInfo: An instance of `CEAttachmentInfo` parsed from the response

Update outbound Attachment Info

The function below calls the REST request to update attachment information. Before sending the information to the endpoint system (Service Anywhere), new information should be merged to the existing one.

Out-of-box function:

CaseExchange_SAWUtil.updateAttachmentInfo

The function has the following parameters:

- `mapObj`: Final Service Manager value object after field mapping and value mapping.
- `sm`: Temporary Service Manager value object after copying basic data from end point according to field mapping.
- `ep`: Original value object from the end point.

- `context`: Context of the SMIS task. You can get a specific value by using the `context['internalId']` syntax.
- `param`: All parameters defined in SMIS configuration. You can get a specific parameter value by using the `param['object']` syntax.

For more information about these parameters, see "Placeholder objects" on page 86.

The function returns the following result:

Array: Array of the `CEAttachmentInfo` object

Limitations and known issues

This chapter introduces the limitations and known issues of the Case Exchange integration.

Insufficient message for a failed Case Exchange task

The SMIS task log does not contain sufficient information for a failed Case Exchange task (QCCR1E114322)

When a Case Exchange task fails, the SMIS task log does not contain sufficient information for you to troubleshoot the root cause of the failure.

Workaround

Use the following workaround if the SMIS task log does not contain sufficient information:

> **Note:** Remember to adjust the **Log Level** setting in the SMIS integration instance before you debug the error. For more information about how to configure this setting, see "Integration Instance Information fields" on page 75.

- For an inbound task, the native system internally handles the exchange request from the endpoint system. In this scenario, you can find more information by using one of the following methods:
  - Check the latest message in the **sm.log** log file. For more information about how to view the **sm.log** file, see "Review log file" on page 365.
  - Run the failed task again and then check the messages in the message history box.
- For an outbound task, the native system sends the exchange request to the endpoint system and the endpoint system handles the request through RESTful APIs. In this scenario, you need a third-party tool (for example, SoapUI or Postman) to simulate and debug the exchange request.

  You need to collect the following information from the **Task Log Detail** page of the failed task to simulate and debug the exchange request in the third-party tool:
  - The request URL. You can find this URL in the latest message in the **Journal Messages** field.
  - The request data in the **Task Request Data** field.

  For more information about how to access the **Task Log Detail** page, refer to the following online help topic:

System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Monitor SMIS task log

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Integrations help topics for printing (Service Manager 9.41)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-ITSM@hp.com.

We appreciate your feedback!


Java™
COMPATIBLE