



HP Operations Manager i

Software Version: 10.01

OMi Integrations Guide

Document Release Date: 16 October 2015
Software Release Date: May 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

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Google™ and Google Maps™ are trademarks of Google Inc.

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

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

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are trademarks of the Microsoft group of companies.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

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/group/softwaresupport/search-result?keyword=.](https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=)

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to <https://softwaresupport.hp.com> and click **Register**.

To find more information about access levels, go to:

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software Solutions & Integrations and Best Practices

Visit HP Software Solutions Now at <https://h20230.www2.hp.com/sc/solutions/index.jsp> to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at <https://hpln.hp.com/group/best-practices-hpsw> to access a wide variety of best practice documents and materials.

Contents

Part I: Introduction	7
Chapter 1: Integrating with Other Applications - Overview	8
Part II: Operations Manager i - Application Performance Manager Integration ..	9
Chapter 2: OMi - Application Performance Management Overview	10
Chapter 3: How to Integrate BSM-APM with OMi	11
Integrate a BSM - APM deployment updated from a running BSM 9.24 or earlier to BSM 9.25 or later	12
Install the UCMDB Data Flow Probe	16
Set Up TLS and Root Certificates	18
Configure Lightweight Single Sign-On	18
Create the Integration User	19
Set Up an APM Connected Server in OMi and Start the Topology Synchronization	21
Verify the Topology Synchronization	22
Continue the Setup of APM in OMi and Start the Integration	22
Adjust KPI Assignments	23
Configure Initial KPI Status and Downtime Synchronization	24
Chapter 4: How to Display APM Data in OMi	25
Part III: Operations Manager i - HP SiteScope Integration	27
Chapter 5: SiteScope Integration - Overview	28
Chapter 6: SiteScope Integration - Tasks	29
Chapter 7: How to Create a Connection to a SiteScope Server	35
Part IV: Operations Manager i - HP Operations Manager Integration	38
Chapter 8: Operations Manager i - HP Operations Manager Integration Overview	39
Chapter 9: Workflow: Configuring Connections Between Operations Manager i and HPOM ..	40
Chapter 10: How to Establish a Trust Relationship for a Server Connection	41
Chapter 11: How to Verify the Trusted Relationship	44
Chapter 12: How to Create a Connection to an HPOM Server	45
Chapter 13: How to Run Topology Synchronization	48
Chapter 14: How to Configure the HPOM for Windows Forwarding Policy	53
Chapter 15: How to Configure the HPOM for UNIX or Linux Forwarding Policy	56
Chapter 16: How to Validate Event Synchronization	59
Chapter 17: How to Set up Operations Manager i in an Environment Managed by HPOM	61
Chapter 18: OMi Field Mapping	62
Chapter 19: Troubleshooting	65
Part V: Operations Manager i - Service Manager Integration	66

Chapter 20: Operations Manager i-Service Manager Integration Overview	67
Versions	67
Integration Options	67
Chapter 21: OMi-SM Integration with RTSM	71
Data Flow Probe	71
Create User Accounts for the OMi-SM Integration (RTSM)	72
RTSM-Service Manager Integration	73
Enable LW-SSO for the OMi-SM Integration (RTSM)	73
View Actual State in SM (RTSM)	80
Event Forwarding from OMi to SM (RTSM)	81
Step 1: Configure the Service Manager server as a connected server in OMi	81
Step 2: (optional) Configure an Event Forwarding Rule	84
Step 3: Configure the OMi integration in Service Manager	84
Step 4: Configure Launch of Service Manager Incident Details from OMi	89
(optional) Step 5: Attribute Synchronization	90
Step 6: Test the Event Forwarding and Cross Launches	94
Advanced Configuration	95
Downtime Forwarding from Service Manager to OMi (RTSM)	98
Step 1: Add an SMBSM_DOWNTIME integration instance in SM	98
Step 2: Tailor Service Manager to handle phase change	101
Step 3: Set up downtime sync jobs in OMi	101
Step 4: Set up creation of BSM Downtime CIs	102
Step 5: Verify the SM-OMi downtime synchronization setup	102
Sending downtime notifications from OMi to SM (RTSM)	104
Step 1: Send OMi Downtime Events to SM	104
View Changes and Incidents in OMi (RTSM)	106
Prerequisite	106
Step 1: Configure the Service Manager Adapter Time Zone	106
Step 2: Create an Integration Point in OMi	108
Step 3: Edit Integration TQLs	109
Step 4: Verify View changes and incidents	110
How to Customize the Changes and Incidents Component	110
Naming Constraints for New Request for Change TQLs	111
Naming Constraints for New Incident TQLs	112
Business Impact Report (BIR) (RTSM)	113
Step 1: Add a Business Impact Report Integration in SM	113
Step 2: Launch a Business Impact Report from an Incident	114
Chapter 22: OMi-SM Integration with UCMDB	115
Data Flow Probes	115
Create User Accounts for the OMi-SM Integration (UCMDB)	116
UCMDB-Service Manager Integration	117
OMi-UCMDB Integration	117
Enable LW-SSO for the OMi-SM Integration (UCMDB)	117
View Actual State in SM (UCMDB)	125
Event Forwarding from OMi to SM (UCMDB)	125
Step 1: Configure the Service Manager server as a connected server in OMi	126

Step 2: (optional) Configure an Event Forwarding Rule	128
Step 3: Configure the OMi integration in Service Manager	129
Step 4: Configure Launch of Service Manager Incident Details from OMi	133
(optional) Step 5: Attribute Synchronization	134
Step 6: Test the Event Forwarding and Cross Launches	139
Advanced Configuration	140
Downtime Forwarding from Service Manager to OMi (UCMDB)	143
Step 1: Add an SMBSM_DOWNTIME integration instance in SM	143
Step 2: Tailor Service Manager to handle phase change	145
Step 3: Set up downtime sync jobs in UCMDB	146
Step 4: Set up creation of BSM Downtime CIs	147
Step 5: Verify the SM-OMi downtime synchronization setup	147
Sending downtime notifications from OMi to SM (UCMDB)	149
Step 1: Send OMi Downtime Events to SM	149
View Changes and Incidents in OMi (UCMDB)	151
Prerequisite	151
Step 1: Configure the Service Manager Adapter Time Zone	151
Step 2: Create an Integration Point in OMi	153
Step 3: Edit Integration TQLs	154
Step 4: Verify View changes and incidents	155
How to Customize the Changes and Incidents Component	155
Naming Constraints for New Request for Change TQLs	156
Naming Constraints for New Incident TQLs	157
Business Impact Report (BIR) (UCMDB)	158
Step 1: Add a Business Impact Report Integration in SM	158
Step 2: Launch a Business Impact Report from an Incident	159
Part VI: Operations Manager i - Network Node Manager i Integration	161
Chapter 23: Operations Manager i - Network Node Manager i Integration Overview	162
Chapter 24: How to Integrate Network Node Manager i with Operations Manager i	163
Chapter 25: NNMi Components in My Workspace	165
Part VII: Operations Manager i - Operations Orchestration Integration	167
Chapter 26: Operations Manager i - Operations Orchestration Integration Overview	168
Chapter 27: How to Integrate Operations Manager i and Operations Orchestration	169
Chapter 28: Troubleshooting Integration Problems	174
Chapter 29: Examples of Operations Manager i and Operations Orchestration Integrations ..	175
Part VIII: BSM Connector Integrations	176
Chapter 30: BSM Connector Integration Administration	177
Send Documentation Feedback	179

Part I: Introduction

Chapter 1: Integrating with Other Applications - Overview

Supported Integrations

The primary integrations with OMi are:

- OMi - Application Performance Management (APM)
- OMi - HP Operations Agent
- OMi - SiteScope
- OMi - HP Operations Manager (HPOM)
- OMi - Service Manager (SM)
- OMi - Network Node Manager i (NNMi)
- OMi - Operations Orchestration (OO)
- OMi - Service Health Reporter
- OMi - BSM Connectors

For a list of supported application versions, see the OMi support matrix at:

<http://support.openview.hp.com/selfsolve/document/KM323488>

OMi-OMi Integrations

Integrations between multiple OMi deployments enable the exchange of events using event synchronization and topology synchronization.

For more information on working with multiple OMi deployments, see the Manager-of-Manager Configuration section in the OMi Administration Guide.

OMi-Configuration Management Systems Integrations

OMi integrates with HP Universal CMDB to enable sharing topologies (CIs and relationships) between instances and enabling a consistent CI ID in an environment. The integration uses the Configuration Management System (CMS) topology. A single instance is configured to be the CMS and the global ID generator; synchronization is achieved using the topology synchronization.

For details on setting up these integrations, see the Data Flow Management Guide.

Part II: Operations Manager i - Application Performance Manager Integration

Chapter 2: OMi - Application Performance Management Overview

Integrating Application Performance Management (APM) into OMi enables you to:

- Design a dashboard in which you see OMi and APM data displayed side by side. It is possible to drill down into the APM data from this dashboard.
- Integrate user interface components from separately deployed APM systems directly into the OMi user interface workspaces. In this way, relevant information is shown directly within the OMi user interface, although this data comes from the APM system.
- Use the OMi embedded graphing component to show performance data stored within the profile database of the APM system. For detailed information around business transactions, business transaction flows, or specific information about location-based monitoring within APM, it will be required to drill down into the APM user interface. For this purpose, OMi provides drill-down operations that allow to launch the APM user interface in the context of a specific CI or event.
- See some specific, detailed views. For example, OMi provides in-context drill-down launches into APM for specific subject matter experts.

Supported Versions

- OMi 10.0x
- BSM - APM 9.25 IP 1
- UCMDB Data Flow Probe 10.11

To enhance readability, the term APM is used when referring to BSM - APM 9.25.

Chapter 3: How to Integrate BSM-APM with OMi

To integrate BSM - APM with an OMi deployment, complete the following steps:

1. To integrate a BSM - APM 9.25 (or later) that has been updated from a running BSM 9.24 (or earlier), you need to complete the following step first: ["Integrate a BSM - APM deployment updated from a running BSM 9.24 or earlier to BSM 9.25 or later" on the next page.](#)
If you start from 9.25, continue with step 2.
2. Make sure the Data Flow Probe is installed. For details, see ["Install the UCMDB Data Flow Probe" on page 16.](#)
3. Set Up TLS and Root Certificates. For details, see ["Set Up TLS and Root Certificates" on page 18.](#)
4. Align the Lightweight Single Sign-On configuration on both deployments. This enables you to view APM components in the OMi user interface. For details, see ["Configure Lightweight Single Sign-On" on page 18.](#)
5. Create the integration user. For details, see ["Create the Integration User" on page 19.](#)
6. Set up an APM connected server in OMi and start the topology synchronization. For details, see ["Set Up an APM Connected Server in OMi and Start the Topology Synchronization" on page 21.](#)
7. Verify the Topology Synchronization. For details, see ["Set Up an APM Connected Server in OMi and Start the Topology Synchronization" on page 21.](#)
8. Continue the APM setup in OMi and start the integration. In this step, you configure the following:
 - Event forwarding in APM
 - Status forwarding in APM
 - Setting the APM URL in APM
 - Downloading and installing APM user interface components
 - Importing UCMDB enrichment rules

For details, see ["Set Up an APM Connected Server in OMi and Start the Topology Synchronization" on page 21.](#)

9. Configure the initial KPI Status and Downtime Synchronization. For details, see ["Adjust KPI Assignments" on page 23.](#)

Note: The JMX Console can only be used remotely when its use is configured in APM or OMi respectively. For information on how to configure your JMX Console remotely, see [How to Enable Accessing JMX Console Remotely in OMi Help Home > Administration Guide > Additional Configuration > JMX Console.](#)

To log in the JMX Console, use the user name `sysadmin` and the password `admin`.

Integrate a BSM - APM deployment updated from a running BSM 9.24 or earlier to BSM 9.25 or later

To integrate a BSM - APM 9.25 (or later) that has been updated from a running BSM 9.24 (or earlier), you need to complete the following steps first.

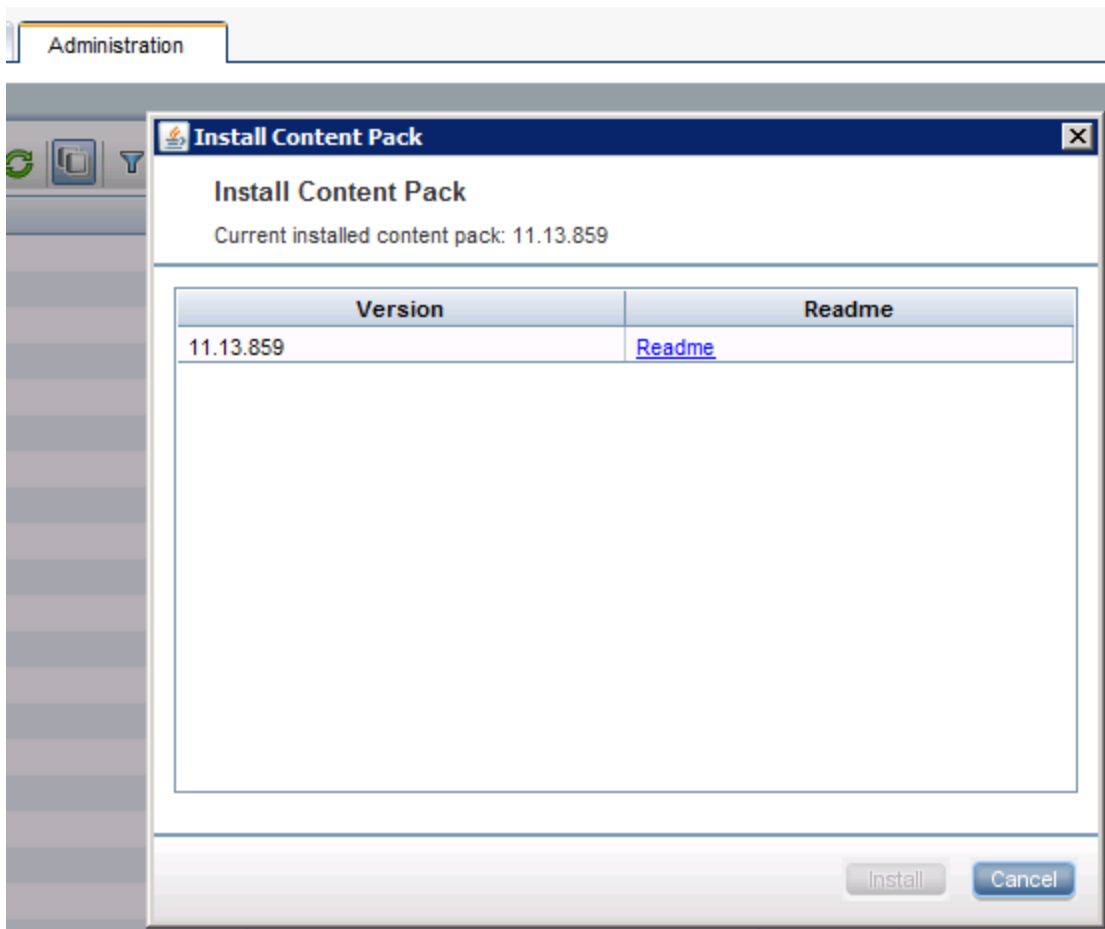
If you install remotely, copy all the content packs to your computer and then point to the local location to deploy the package.

If you are using a web-browser, follow the instructions below:


1. On your APM server, check if uCMDB content pack 11.13.859 is installed. On the APM system, navigate to:

Admin > RTSM Administration > Administration > Package Manager.

Click the **Install Content Pack** icon to open the **Install Content Pack window**. It should show the following:



If you see this, it is installed and you can carry on with the next step. If it is not yet installed, install it using the **Package Manager**:

- a. Navigate to **Admin > RTSM Administration > Administration > Package Manager** to open the RTSM Package Manager.
 - b. Click  **Install Content Pack** to open the **Install Content Pack** window.
 - c. Select 11* from **Version** and click **Install** to install the content pack version 11. Note that you will only see content packs that are available but not yet installed. Those that are installed, you will not see here.
2. On your APM server, import individual TQLs from the packages listed below. Note that you need to import the TQLs from the following .zip files, even if these packages are already present on the APM server:

BLE.zip



Business.zip

Diagnostics.zip



OMi_Integration.zip

Sitescope.zip



To get the TQLs from BLE.zip:

- a. Navigate to **Admin > RTSM Administration > Administration > Package Manager** to open the RTSM Package Manager.
- b. Click  to open the **Deploy Packages to Server** window and click .
- c. Navigate to `<BSM_HOME>/odb/conf/factory_packages`.
- d. Open BLE.zip, then click BLE.zip to see the list of resources.
- e. In the resource list, scroll down to and select `tql - CIs_For_CIStatusChange_in_OMi`.
- f. Click **Deploy** to deploy your resource and click **ok** in the box **Resources have been deployed successfully**.

To get the TQLs from Business.zip:



- a. Navigate to **Admin > RTSM Administration > Administration > Package Manager** to open the RTSM Package Manager.
- b. Click  to open the **Deploy Packages to Server** window and click .
- c. Navigate to `<BSM_HOME>/odb/conf/factory_packages`.
- d. Open Business.zip, then click Business.zip to see the list of resources.
- e. In the resource list, scroll down to and select `tql - OMi_Sync_BPI`.
- f. Click **Deploy** to deploy your resource and click **ok** in the box **Resources have been deployed successfully**.

To get the TQLs from Diagnostics.zip:



- a. Navigate to **Admin > RTSM Administration > Administration > Package Manager** to open the RTSM Package Manager.
- b. Click  to open the **Deploy Packages to Server** window and click .
- c. Navigate to `<BSM_HOME>/odb/conf/factory_packages`.
- d. Open Diagnostics.zip, then click Diagnostics.zip to see the list of resources.

- e. In the resource list, scroll down to and select `tq1 - OMi_Sync_Diag_TV`.
- f. Click **Deploy** to deploy your resource and click **ok** in the box **Resources have been deployed successfully**.

To get the TQLs from OMi_Integration.zip:

- a. Navigate to **Admin > RTSM Administration > Administration > Package Manager** to open the RTSM Package Manager.
- b. Click  to open the **Deploy Packages to Server** window and click .
- c. Navigate to `<BSM_HOME>/odb/conf/factory_packages`.
- d. Open `OMi_Integration.zip`, then click `OMi_Integration.zip` to see the list of resources.
- e. In the resource list, select `tq1 - OMi_Sync_BIZ`.
- f. Click **Deploy** to deploy your resource and click **ok** in the box **Resources have been deployed successfully**.

To get the TQLs from Sitescope.zip:

- a. Navigate to **Admin > RTSM Administration > Administration > Package Manager** to open the RTSM Package Manager.
- b. Click  to open the **Deploy Packages to Server** window and click .
- c. Navigate to `<BSM_HOME>/odb/conf/factory_packages`.
- d. Open `Sitescope.zip`, then click `Sitescope.zip` to see the list of resources.
- e. In the resource list, scroll down to select `tq1 - OMi_Sync_SIS` and `tq1 - OMi_Sync_SIS_EMS`.
- f. Click **Deploy** to deploy your resource and click **ok** in the box **Resources have been deployed successfully**.

To validate that these packages containing individual TQLs have been loaded correctly, you can look them up in the Modeling Studio. Navigate to:

- a. **Administration > RTSM Administration > Modeling > Modeling Studio**
 - b. Select **Resource Type: Queries**. In the list, expand **Root** and scroll down to verify that `CIS_For_CISstatusChange_in_OMi` is present. Next, expand **Root > Integration > OMi_Integration** to verify that the following packages are present:
 - `OMi_Sync_Biz`
 - `OMi_Sync_BPI`
 - `OMi_Sync_Diag_TV`
 - `OMi_Sync_SiS`
 - `OMi_Sync_SiS_EMS`
3. On your APM deployment, proceed as follows to check whether OMi is configured for single sign-on configuration. First, read out the values from the JMX console to determine whether further steps are required:
- a. Open the JMX console on your APM gateway server by typing in a web browser:
`http://localhost:8080/jmx-`

```
console/HtmlAdaptor?action=inspectMBean&name=Foundations%3Aservice%3DInfrast  
ructure+Settings+Manager
```

- b. Find the method **java.lang.String getGlobalSettingValue()**.
- c. Change **contextName** to SingleSignOn.
- d. Change **settingName** to lw.sso.configuration.xml.
- e. Click **Invoke**.

In the resulting output, search for the string `omi`. If the string `omi` is present twice, your deployment is configured correctly and no further steps are required.

4. If the resulting output does not contain the string `omi`, APM is not yet correctly configured for integrating with OMi. In this case, you need to append the necessary data:

- a. On your APM gateway server, copy and paste the entire result output in a text editor and append the following URLs between the `<restURLs>` and the `</restURLs>` tags:

```
<url>.*topaz.*omi.*integration.*</url>  
<url>.*topaz.*acweb.*</url>  
<url>.*topaz.*personalization.*</url>  
<url>.*topaz.*bsmLight.*</url>  
<url>.*topaz.*ldapContext.*</url>  
<url>.*topaz.*bsmLight.*BPM.*</url>
```

- b. Also append the following between the `<inbound>` and `</inbound>` tag:

```
<service service-pattern=  
".*/topaz.*omi.*integration.*" service-type="rest">  
<in-lwssso refid="ID000001"/>  
<in-custom  
classname="com.mercury.topaz.reportsExt.login.BsmLwSsoBasicAuthHandler"/>  
<in-lwsssoAutoCreate refid="ID000002"/>  
</service>
```

- c. Copy the entire content from the two steps above.
- d. Open the JMX console on your APM gateway server by typing in a web browser, preferably Firefox:

```
http://localhost:8080/jmx-  
console/HtmlAdaptor?action=inspectMBean&name=Foundations%3Aservice%3DInfrast  
ructure+Settings+Manager
```


- e. Find the method **void setGlobalSettingValue()**.
- f. Change the **contextName** to SingleSignOn.
- g. Change the **settingName** to lw.sso.configuration.xml.
- h. Paste the new content into the **Value** field.
- i. Click **Invoke**.
- j. Restart the Mercury AS process.

Note: If you are using a distributed environment, you need to exchange the BBCTrust manually on your BSM APM processing server, run

```
<OMi_HOME>/opr/bin/BBCTrustServer.[bat, sh] <FQND of OMi processing server>
```

Install the UCMDB Data Flow Probe

To install the UCMDB Data Flow Probe:

1. Get the UCMDB Data Flow Probe installation bits from the OMi media kit. The UCMDB Data Flow Probe needs to have the same version as the UCMDB or RTSM that OMi uses. The UCMDB Data Flow Probe can be installed on the OMi gateway server or data processing server. For more details on the installation of the Data Flow Probe, see the Data Flow Probe ReadMe on the media kit.
2. Install the UCMDB Data Flow Probe according to the instructions in the UCMDB Data Flow Probe Installation Guide. Make sure:
 - The UCMDB Data Flow Probe is connected to OMi.
 - HP BSM is selected as the application server.
 - The OMi gateway server or virtual server name is specified.
3. Set credentials so that the domain name appears in a drop-down list during configuration of the connected server:
 - a. Navigate to:
Administration > RTSM Administration > Data Flow Management > Data Flow Probe Setup
 - b. Select **Default Domain(Default)** and open **Credentials** to go to **Generic Protocol**.
 - c. Click  **New** in the **Generic Protocol** pane to open the **Generic Protocol Parameters** wizard.
 - d. Leave the default values in the **General** section.
 - e. Enter any user name and any password in the **Generic** section.
4. Start the Data Flow Probe before integrating BSM - APM 9.25 using
`<INSTALL_DIR>/UCMDB/DataFlowProbe/bin/gateway.bat|sh start.`
To see whether the UCMDB Data Flow Probe started successfully, check the following logfile :
`<INSTALL_DIR>/UCMDB/DataFlowProbe/runtime/log/WrapperProbeGw.log`
Allow approximately 10 minutes for this process to finish as the Data Flow Probe is uploading a large number of files from the RTSM.
5. Set up a global filter to block configuration items contained in APM but not in OMi from being synchronized from APM to OMi, such as Business Transaction or Business Transaction Flow.
 - a. On your OMi deployment navigate to **Administration > RTSM Administration > Data Flow Management > Adapter Management**.
 - b. Go to the **Packages** pane and double click **DDMInfra**.
 - c. Select and open the file **globalFiltering.xml** from the **ConfigurationFiles**.
 - d. It is recommended to exclude the CI types that should not be synchronized by adding these entries between `<excludeFilter>` and `</excludeFilter>`:


```
<vector>
<object class="sitescope_group"></object>
<object class="sitescope_measurement"></object>
<object class="sitescope_measurement_group"></object>
<object class="sitescope_monitor"></object>
<object class="sitescope_profile"></object>
<object class="sitescope_profile_monitor"></object>
<object class="sitescope_webservice_monitor"></object>
<object class="business_transaction"></object>
<object class="end_user_group"></object>
<object class="rum_eug_subnet"></object>
<object class="business_transaction_flow"></object>
<object class="location"></object>
</vector>
```

Make sure `recursiveFilter="true"` is set in the `<resultFilters>` section.

In some setups it might be necessary to synchronize one or all of the CI types `location`, `business_transaction`, `business_transaction_flow`, `end_user_group` or `rum_eug_subnet`. In this case, do not exclude them.

- e. Save the file.
6. Increase the RTSM timeout in these two places if network latency is likely:

Note: The JMX Console can only be used remotely when its use is configured in APM or OMi respectively. For information on how to configure your JMX Console remotely, see [How to Enable Accessing JMX Console Remotely in OMi Help Home > Administration Guide > Additional Configuration > JMX Console](#).

To log in the JMX Console, use the user name `sysadmin` and the password `admin`.

- a. On your OMi deployment , open the RTSM JMX console in a web browser:
`http://localhost:21212/jmx-console/HtmlAdaptor`.
Click **UCMDB:service=Settings Services**.
Click **setSettingValue**.
For **customerID**, enter value 1.
For **name**, enter value `task.DataAccess.Manager.getAdapterClassesConfig.timeOut`.
For **value**, enter value *<timeout in milliseconds>* (default is 20000).
- b. Also, in the RTSM JMX console `http://localhost:21212/jmx-console/HtmlAdaptor`,
Click **UCMDB:service=Settings Services**.
Click **setSettingValue**.
For **customerID**, enter value 1.
For **name**, enter value `configuration.remote.action.timeout`.
For **value**, enter value *<timeout in milliseconds>* (default is 35000).

Set Up TLS and Root Certificates

If you have hardened your OMi server, you need to configure TLS in the Data Flow Probe and establish trust between the Data Flow Probe server and the OMi server.

1. Enable TLS in the DFP to connect to OMi:
 - a. Open `<DFP_HOME>/conf/DataFlowProbe.properties`.
 - b. Change the property `appilog.agent.probe.protocol` from HTTP to HTTPS.
 - c. Change the property `serverPortHttps` from 8443 to 443.
2. Establish trust between the DFP server and the OMi server:
 - a. Import issue of OMi server certificate into JRE's trust store:

```
<UCMDB_HOME>/UCMDB/DataFlowProbe/bin/jre/bin/keytool -import -trustcacerts -file <CA cert>.pem -alias <ca cert alias> -keystore <UCMDB_HOME>/UCMDB/DataFlowProbe/bin/jre/lib/security/cacerts
```
 - b. Import issue of APM server certificate into JRE's trust store:

```
<UCMDB_HOME>/UCMDB/DataFlowProbe/bin/jre/bin/keytool -import -trustcacerts -file <CA cert>.pem -alias <ca cert alias> -keystore <UCMDB_HOME>/UCMDB/DataFlowProbe/bin/jre/lib/security/cacerts
```

You need to import the root certificate from your certification authority to the OMi and the APM data processing servers and gateway servers.

1. On the OMi gateway and data processing servers, run the following command:

```
<OMi_HOME>/JRE/bin/keytool.[exe, sh]-import -trustcacerts -file <Root Certificate of your Certificate Authority> -alias <any name> -keystore <OMi_HOME>/JRE/lib/security/cacerts
```
2. On the APM gateway and data processing servers, run the following command:

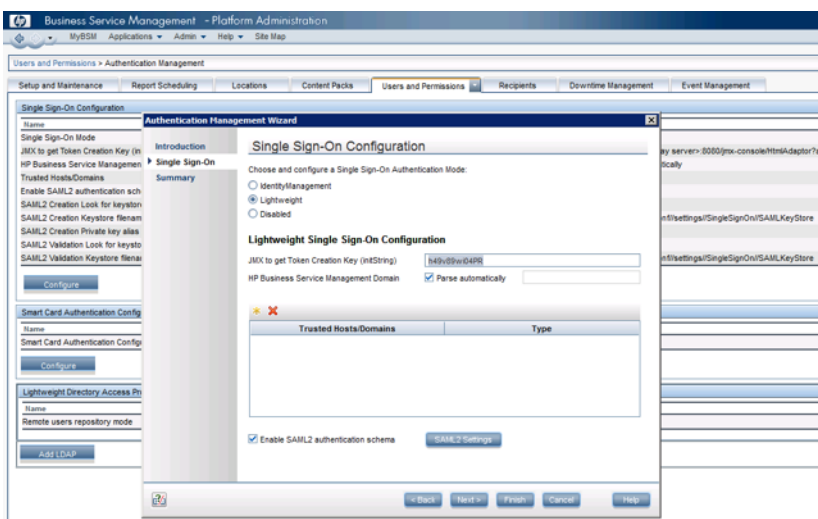
```
<APM_HOME>/JRE/bin/keytool.[exe, sh]-import -trustcacerts -file <Root Certificate of your Certificate Authority> -alias <any name> -keystore <APM_HOME>/JRE/lib/security/cacerts
```

Configure Lightweight Single Sign-On

Set up Lightweight Single Sign-On (LW-SSO) and align `initString` on both systems. It is good practice that the product added to the existing environment gets the same key as the already existing deployments. For example, if OMi is added last, the key needs to be changed in OMi:

- In your APM deployment:
 - a. Open **Admin > Platform > Users and Permissions > Authentication Management**.
 - b. Click **Configure** under the **Single Sign-On Configuration** list to open the **Single Sign-On Configuration** wizard.
 - c. Select **Lightweight** in the **Single Sign-On** dialog.

- d. Copy the `initString` from **JMX to get Token Creation Key (initString)**.
- e. Click **Finish** to save your configuration.



- In OMi:
 - a. Navigate to Authentication Management:
Administration > Users > Authentication Management
 - b. Click the **Configure** button under the **Single Sign-On Configuration** list to open the Single Sign-On Configuration wizard.
 - c. In the **Single Sign-On** dialog, select **Lightweight**.
 - d. Paste the `initString` you copied above from **JMX to get Token Creation Key (initString)** to the Token Creation String.
 - e. Click **Finish** to save your configuration.

Create the Integration User

You need to first create your user in APM's jmx console. Then you need to configure the user through the APM UI.

1. In your APM deployment, go to the jmx console: `http://localhost:21212/jmx-console`
2. Select **UCMDB Service:Security Services**.
3. Go to **createIntegrationUser()** and create your integration user. If you use user admin here, no further action is required later. If not, use the following values:
`customerID: 1`
`userName: <intergration user name>`
`password: <pwd>`
`dataStoreOrigin: <any value>`
4. Click **Invoke**.
5. Invoke the **getUsersList MBean** with **customerID=1** to check if the user is shown in the list of integration users.

6. In your APM deployment go to **Admin > Platform > User and Permissions > User Management**.
7. Select **Create New Users** with the same user name as the integration user created previously.
8. Click the icon of the user you have just created.
9. Go to the tab **Permissions**.
10. Grant the **Administrator** role to your integration user.
11. Click **Apply Permissions** to finish.

Note: You need to wait at least ten minutes for the changes to take effect. You can define this in the following setting:

Navigate to: **Admin > Platform > Setup and Maintenance > Infrastructure Settings**


Select the context: **Applications - Operations Management**

Scroll to **Operations Management - Topaz Authorization Service Settings**

Click the edit button in the line **Refresh Interval** and enter 10 in the field **Value** in the **Edit Setting** dialog box.

Set Up an APM Connected Server in OMi and Start the Topology Synchronization

To synchronize the configuration items (CIs) that exist in APM to OMi, perform the following steps:

1. Make sure port 383 is open.
2. On your OMi deployment, navigate to:
Administration > Setup and Maintenance > Connected Servers
3. Click  **New** and select **APM** from the drop-down list. The **General** page of the **Create New Server Connection - APM** wizard opens.
4. Enter a **Display Name** (the **Name** is entered automatically) and click **Next**. The **Server Properties** page opens.
5. Enter the FQDN of the **Application User**:
 - a. On your APM deployment, navigate to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**
 - b. Click the radio button **Foundations**, then scroll down and select **Platform Administration**
 - c. Scroll down to the section **Platform Administration - Host Configuration**
 - d. Copy the FQDN part of the URL in the **Value** field of the row with the **Name: Default Virtual Gateway Server for Application Users URL**. The FQDN part of the URL is the URL without **https://** and without **<port number>**
 - e. Paste this into **Fully Qualified DNS Name** in **Target Server** in the **Create New Server Connection** wizard on your OMi deployment.

Note: Step 4 is particularly important when you are configuring a High Availability setup.

6. Enter the user name and password of your integration user.
7. *Optional.* if the URL Path has changed, you need to add the new URL, otherwise leave this field empty.
If you click **Test Connection** now, you will receive an error, because no synchronization has happened at this point.
8. Click **Next** to go to the Synchronization pane of the **Create New Server Connection - APM** wizard.
9. Click the box on the left of **Step 1: Topology** in the **Create New Server Connection - APM** wizard.
 - a. If the option **Use OMi as Global ID Generator** is editable, you need to select your desired global ID generator.
 - b. If the option **Use OMi as Global ID Generator** is grayed out, a global ID generator already exists in your environment. In this case, proceed with selecting your Data Flow Probe.
 - c. Select the name of your Data Flow Probe from the drop-down list. The **Domain Name** is inserted automatically.
 - d. Click **OK** to start the topology synchronization and to create the integration point in APM.

Verify the Topology Synchronization

1. On the OMi server, navigate to:
Administration > Setup and Maintenance > Connected Servers
2. The tooltip in the Connected Servers pane to the right of your connected server tells you the status of the last executed job. Wait until one integration job ran successfully before continuing. To update the status, click the **Refresh** button in the Connected Servers pane.
Additionally, you can check the status of the integration jobs in the RTSM Integration Studio:
3. Navigate to:
Administration > RTSM Administration > Data Flow Management > Integration Studio
On the left-hand side of the Integration Studio, you see a list of all integration points.
4. Select the APM2OMi integration point. You see two integration jobs:
sync_continuous
sync_initial
Wait until at least one of these completes before continuing.
You can start manually either integration job by clicking the **full synchronization** icon or the **delta synchronisation** icon.

Continue the Setup of APM in OMi and Start the Integration

1. On the OMi server, navigate to:
Administration > Setup and Maintenance > Connected Servers
3. Double-click your APM connected server to open the **Edit Server Connection** wizard.
4. Go to the **Synchronization** tab.
5. Click the check box next to **Step2: OMi to APM Setup**.
6. Click **Finish** to complete the integration.

Note: Deleting a Connected Server

If a connected server is deleted or disabled in your OMi deployment, the following happens on the OMi deployment:

The job schedule is deleted from the connected server definition. The integration points are retained in the **Integration Studio**. If a connected server with the same name is recreated, it will reuse this integration point and enable the existing schedules.

The following happens on the APM deployment:

The connected servers **OMi Operations Bridge 10** and **OMi Operations Manager Server 10** are retained in APM and remain in the active state.

The event forwarding rule is retained in APM and remains enabled.

Adjust KPI Assignments

BSM will create one Improved/Worsened CI Status event that is forwarded to **OMi**:

Time Received	Title	F
1/26/15 02:10:16 AM	Improved CI Status forwarded to OMI - Advantage Inc Applic	A
1/26/15 02:10:16 AM	Improved CI Status forwarded to OMI - Online Banking Applic	O

These events are processed specially in **OMi**, will set an Application Performance or Application Availability HI and will then be deleted. Those event do not appear in the **OMi** event browser or database. In BSM, these events can be closed, for example via a time-based event automation rule.




To set KPI status, the KPI assignments in **OMi** first have to be adjusted so that the automatically created HIs influence corresponding KPIs in **OMi**.


Note: These adjustments can only be done once a corresponding CI status event has been received in **OMi**. Otherwise you will not see the Application Performance or Application Availability HIs. In **OMi**:

1. Go to **Administration > Service Health > KPI Assignments**
2. Select the **BusinessApplication CIT**.

On a new **OMi** 10.00 installation there are two KPI assignments with conditions for BPM and RUM. They are not suitable for an **OMi** system and can be stopped. Note, that they cannot be deleted as they are pre-defined.

In principal, you create a new KPI assignment for Application Availability and Application Performance KPIs. As condition use no condition. Then you add the Application Performance HI to the Application Performance KPI. Finally, you add the Application Availability HI to the Application Availability KPI:

1. Navigate to:
Administration > Service Health > CI Status Calculation > KPI Assignments
2. Navigate to **Configuration Item > Business Element > Business Application** in **CI Types** to open the **Assignments for CI Type: BusinessApplication** pane.
3. Select the **Assignment Name** of the assignment that contains **Application Availability, Availability Performance** in the **KPIs** column and click  to edit the KPI assignment. The **Edit KPI Assignment for CI Type** window opens.
4. Click **KPI Configurations** to open the **KPI Configuration** pane.
5. Select the KPI **Application Availability** and click  to open the **Edit KPI for Assignment** editor.
6. Click **KPI Configurations** to expand the KPI configurations pane.
7. Double-click the KPI **Application Availability** to open the **Edit KPI For Assignment** editor.
8. Click  in **Related Health Indicators** to open the **Edit Related Health Indicators** window.
9. Select the HI **Application Availability** and click

 to add this HI to the list of selected Health Indicators.

Note: If you do not see any HIs in the **Edit Related Health Indicators**, wait until CI status changes have been forwarded from APM to OMi. The forwarding of CI status changes is triggered by the first change of a CI status of any CI that is present in APM and has been synchronized to OMi.

10. Click **Apply** to apply your changes, click **Save** to save your changes in the **Edit KPI For Assignment** editor, click **Save** to save your changes in the **Edit KPI Assignment for CI Type** window.
11. Perform steps 3 to 10 for the **Application Performance** HI and KPI.
12. Click **Synchronize CI Type** for the assignment to take effect on existing CIs.

Configure Initial KPI Status and Downtime Synchronization

1. On the OMi server, navigate to:
Administration > Setup and Maintenance > Connected Servers
2. Double-click your APM connected server to open the **Edit Server Connection** wizard.
3. Click the check box on the left of **Step 3: Synchronization**. This triggers:
 - The initial synchronization of all KPI states for all APM CIs. This initial synchronization is necessary if you want to see the current state on the APM system.
 - The downtime definition synchronization of OMi to APM.
4. *Optional:* click the box **Synchronize Downtime** if you want to also synchronize APM's downtime definitions to your OMi deployment.

Chapter 4: How to Display APM Data in OMi

APM user interface components can be directly integrated into OMi **Workspaces** to view and drill down to detailed APM information.

Create an APM User Interface Element

1. On the OMi server, navigate to:
Workspaces > My Workspace
2. Create a new page:
 - a. Click the **New Page** icon on the top left of the toolbar.
 - b. Click **Add Component** in the graphics on the left to open the **Component Gallery**.
 - c. Select APM from the list on the left of the **Component Gallery** to display the APM components.
 - d. Double-click the desired APM.

It is not possible to apply a filter to the user interface components from APM that are displayed in OMi.

The following use cases are supported:

1. Selecting APM components from the OMi components gallery and opening them in a frame inside the OMi components dashboard.
2. Wiring in case of a CI change. For example, a CI 1 is selected and its associated data is displayed. If now a different CI, CI 2, is selected, the data displayed changes to data associated with CI 2.

The following components are currently available in OMi:

1. **Platform Components**
 - Top View
 - Hierarchy View
 - APM Based Impact
2. **BPM Components**
 - Application Summary
 - BPM Performance Matrix
 - BPM Performance Status
 - BPM Error Summary Distribution by Category/Type
 - Application Health Business Summary
 - BPM Error Summary Distribution by Location/BPM Custom Attributes
 - BPM Error Summary Distribution by Transaction
 - Metrics Over Time
3. **RUM Components**

- Application Health Performance
- Application Health Availability
- RUM Event Count By classification

4. **SiS components**

- Cross Performance Reports
- SiS Multi View

Part III: Operations Manager i - HP SiteScope Integration

This part of the guide contains the following chapters:

- ["SiteScope Integration - Overview" on page 28](#)
This chapter provides the SiteScope integration overview.
- ["SiteScope Integration - Tasks" on page 29](#)
This chapter describes various tasks that you need to perform to configure and use the SiteScope integration.
- ["How to Create a Connection to a SiteScope Server" on page 35](#)
This chapter describes how to create a connection to a SiteScope server and explains how configured SiteScope connected servers are chosen for deployment.

Chapter 5: SiteScope Integration - Overview

HP SiteScope (SiteScope) is an agentless monitoring solution that enables you to remotely monitor the availability and performance of your IT infrastructure (for example, servers, operating systems, network devices, network services, applications, and application components). OMi provides a script that enables you to import templates from a SiteScope server so that you can include them in aspects.

SiteScope templates contain information about the remote servers they monitor. When you import SiteScope templates, OMi exports the templates from the SiteScope and transforms them into the OMi policy templates. For more information on importing templates and important considerations that need to be taken into account, see the OMi Administration Guide.

Before deploying the policy template, OMi replaces the value `%%HOST%%` with the list of remote servers to which the policy template is assigned. Based on the connected server configuration, OMi then selects the SiteScope server that qualifies for monitoring the remote servers and deploys the policy template to that server. The SiteScope server finally creates the corresponding monitors and starts monitoring the remote servers.

To be able to assign and deploy a SiteScope policy template, the SiteScope server must be set up as a connected server in OMi and a node CI must exist for the system in Monitored Nodes. In addition, the remote systems that SiteScope monitors must be represented as node CIs in the RTSM.

Note: Inactive SiteScope connected servers cannot be used for deployment. For example, if you deactivate a SiteScope connected server that has SiteScope policy templates assigned to it, this server will not be used for deployment until you activate it using the Connected Servers manager or the ConnectedServers command-line interface. See the OMi Administration Guide for more information.

Chapter 6: SiteScope Integration - Tasks

This section describes the tasks that you need to perform to configure and use the SiteScope integration:

- ["How to Migrate the SiteScope Integration from BSM 9.2x" below](#)
- ["How to Set Up the SiteScope Integration" on the next page](#)
- ["How to Connect to a SiteScope Server That Requires SSL" on the next page](#)
- ["How to Import Templates from a SiteScope Server" on page 32](#)
- ["How to Assign SiteScope Policy Templates to Remote Servers" on page 32](#)
- ["How to Combine Policy Templates into an Aspect or Management Template" on page 32](#)
- ["How to Configure Drill Down to SiteScope" on page 33](#)
- ["How to Drill Down to SiteScope" on page 34](#)

How to Migrate the SiteScope Integration from BSM 9.2x

The SiteScope systems integrated with BSM 9.2x are imported into OMi automatically during the upgrade.

However, if you customized the Health Indicator and CI Type Mapping content delivered by BSM 9.2x (this content consists of the `ciSubTypes.xml`, `meas2eti.xml`, and `userDefinedCiType.xml` files and is downloaded and used by SiteScope systems when they connect to BSM), the updated files are not imported automatically during the upgrade. Therefore, you need to retrieve them from the SiteScope system integrated with BSM 9.2x and import them to OMi manually.

You can skip the import step if no customizations were made. In this case, the default Health Indicator and CI Type Mapping content located in the `<OMi_HOME>/conf/sis/content` directory will be used.

To import the Health Indicator and CI Type Mapping content modified in the BSM version you are upgrading from, proceed as follows:

1. On the SiteScope system, copy the following files to a temporary directory on the OMi system:

```
<SiteScope_install_dir>/conf/integration/bsm/ciSubTypes.xml  
<SiteScope_install_dir>/conf/integration/bsm/meas2eti.xml  
<SiteScope_install_dir>/conf/integration/bsm/userDefinedCiType.xml
```

2. Change to the temporary directory on the OMi system and run the following command:


```
<OMi_HOME>/bin/opr-sis-file-manager.[bat|sh] -import ciSubTypes.xml  
meas2eti.xml userDefinedCiType.xml
```

As a result, the specified files are uploaded to the OMi database.

To edit the uploaded content, use the `opr-sis-file-manager.[bat|sh]` command-line interface located in the `<OMi_HOME>/bin` directory. To retrieve the uploaded content, use the `-export` option. To commit the changes, use the `-import` option. For more information on the `opr-sis-file-manager` command-line interface, see the OMi Administration Guide.

Post-Migration Steps

The SiteScope systems are migrated as inactive connected servers that do not get registered by OMi until they get activated. To activate (enable) a migrated SiteScope connected server:

1. Open the Connected Servers manager from Administration:
Administration > Setup and Maintenance > Connected Servers
2. Select the SiteScope connected server you want to enable and click  **Activate**.

Note: Inactive SiteScope connected servers appear dimmed in the list of connected servers.

How to Set Up the SiteScope Integration

Before you can start monitoring a configuration item (CI) with SiteScope, you need to configure the SiteScope integration with OMi by carrying out the following steps:

1. Install the HP Operations Agent on the SiteScope system. For details, see the HP SiteScope Deployment Guide.
2. Connect the agent to OMi (in SiteScope, navigate to **Preferences > Integration Preferences > New Integration > HP Operations Manager Integration**). To establish the connection, the agent sends a certificate request to OMi, which must be granted in OMi. For details, see the SiteScope Help.
3. *For HP Operations Agent v. 11.11 and below.* Set up the agent on the SiteScope system to accept the OMi server as the authorized manager by configuring `MANAGER_ID` on the SiteScope system (`MANAGER_ID` defines who is allowed to access the agent from outside).

Proceed as follows:

- a. On the OMi Gateway Server system, type the following command to find out the core ID:
`ovcoreid -ovrg server`
 - b. On the SiteScope system, set `MANAGER_ID` to the core ID of the OMi Gateway Server:
`ovconfchg -ns sec.core.auth -set MANAGER_ID <core ID of OMi Gateway Server>`
 - c. Restart the agent processes by typing:
`ovc -restart`
 - d. *Optional.* Verify `MANAGER_ID` by typing:
`ovconfget sec.core.auth`
4. Set up the SiteScope system as a connected server. For details, see ["How to Create a Connection to a SiteScope Server" on page 35](#).
 5. Verify that a node CI has been created for the SiteScope system and make sure that the systems monitored by SiteScope are represented as node CIs in the RTSM.
 6. Configure templates in SiteScope and import them. For details, see the OMi Administration Guide.

How to Connect to a SiteScope Server That Requires SSL

To connect to a SiteScope server that requires SSL, OMi must trust the root certificate that was used to sign the SiteScope certificate. This is done by adding the root certificate to the CA keystore of the OMi server and to the CA keystore of the SiteScope server.

Complete one of the following procedures depending on the type of certificate that was used to sign the SiteScope certificate:

Note: If the OMi server runs a Linux operating system, replace the paths in the following procedures with their Linux equivalents.

- **Certificate from a certificate authority.** If the SiteScope certificate was signed with a certificate from a certificate authority, import the certificate to the SiteScope CA keystore and to the CA keystore of the OMi server:
 - a. Obtain the root certificate (and any other intermediate certificate) from the certificate authority.
 - b. On the SiteScope server to which you want to deploy policies, import the root certificate (and any other intermediate certificate) to the SiteScope CA keystore. Type:


```
C:\SiteScope\java\bin\keytool -importcert -alias <yourCA> -file
<CAcertificateFile> -keystore C:\SiteScope\java\lib\security\cacerts
```

 When prompted for the password, type the keystore password. (The default password is changeit.)
 - c. On the OMi server to which you want to export SiteScope templates, import the root certificate (and any other intermediate certificate) to the OMi CA keystore. Type:


```
<OMi_HOME>\JRE\bin\keytool -importcert -alias <yourCA> -file
<CAcertificateFile> -keystore <OMi_HOME>\JRE\lib\security\cacerts
```

 When prompted for the password, type the keystore password. (The default password is changeit.)
- **SiteScope self-signed certificate.** If the SiteScope certificate is a self-signed certificate (for example, a certificate that was created and configured with the SiteScope tool **ssl_util**), export the self-signed certificate from SiteScope and import it to the CA keystores of the OMi server and SiteScope:
 - a. On the SiteScope server, export the self-signed certificate, type:


```
C:\SiteScope\java\bin\keytool -exportcert -keystore
C:\SiteScope\groups\serverKeystore -alias sitescope -file <certificateFile>
```

 When prompted for the keystore password, type the password that was specified when using the **ssl_util** tool.
 - b. On the SiteScope server, import the self-signed certificate to the SiteScope CA keystore. Type:


```
C:\SiteScope\java\bin\keytool -importcert -file <certificateFile> -keystore
C:\SiteScope\java\lib\security\cacerts
```

 When prompted for the password, type the keystore password. (The default password is changeit.)
 - c. Copy the certificate to the OMi server to which you want to export SiteScope templates.
 - d. On the OMi server, import the self-signed certificate to the OMi CA keystore. Type:


```
<OMi_HOME>\JRE\bin\keytool -importcert -file <certificateFile> -keystore <OMi_
HOME>\JRE\lib\security\cacerts
```

 When prompted for the password, type the keystore password (the default password is changeit).

How to Import Templates from a SiteScope Server

1. Make sure the SiteScope templates that you want to import meet the requirements. See the OMi Administration Guide for more information.
2. On the OMi server, open a command prompt and run the ConfigExchangeSIS command-line interface to import templates from a SiteScope server.

For example, the following command loads the templates that are in the template container called "Template Examples" from sitescope1.example.com:

```
<OMi_HOME>\opr\bin\ConfigExchangeSIS.bat -sis_group_container "Template
Examples" -sis_hostname sitescope1.example.com -sis_user integrationViewer -
sis_passwd password -bsm_hostname bsm1.example.com -bsm_user admin -bsm_passwd
password -bsm_port 80
```

For more information on the ConfigExchangeSIS command-line interface, see the OMi Administration Guide.

How to Assign SiteScope Policy Templates to Remote Servers

1. *Prerequisites:* Make sure the tasks described in ["How to Set Up the SiteScope Integration" on page 30](#) are completed.
2. Assign the SiteScope policy template to the remote servers (that is to the node CIs) that you want to monitor. Do not assign the template to the SiteScope server itself. For information about assigning a policy template, aspect, or management template to a CI, see the OMi Administration Guide.
3. Every SiteScope policy template typically includes a hostname parameter that resolves to the remote server to be monitored. If this value is not already set, edit the value of this parameter during the assignment and enter the symbolic value %%HOST%%.

Alternatively, set the CI attribute PrimaryDNSName as the default value of this parameter on the aspect or management template level.

Before deploying the policy template, OMi replaces the value %%HOST%% with the list of remote servers to which the policy template is assigned.

Tip: Set %%HOST% or the CI attribute PrimaryDNSName already in the template in SiteScope before importing it to OMi. If the host instance parameter is already set at policy template level, you do not need to provide a value when assigning the policy template (aspect or management template) to a CI.

How to Combine Policy Templates into an Aspect or Management Template

To combine the SiteScope policy template and the agent-based policy template into one aspect or management template, proceed as follows:

1. *Prerequisites.* Make sure the tasks described in ["How to Set Up the SiteScope Integration" on page 30](#) are completed.
2. Using the Management Templates and Aspects manager, combine the SiteScope policy template and the agent-based policy template into one aspect or management template and assign it to the CI you want to monitor. Do not assign the template to the SiteScope server itself.

When combining two templates, consider how to group the parameters from the SiteScope policy template and the agent-based policy template, for example:

The policy `DBmonAgentBased` (type `Measurement Threshold`) has an instance parameter named `database_instance` with the dependent parameters `user`, `password` and `port=1521`. The policy `DBmonAgentLess` (type `SiteScope`) has an instance parameter `INSTANCE` with the dependent parameters `HOST=%%HOST%%`, `USER`, `PASSWORD`, `PORT=1521`. Both policies must be combined into one aspect called `DBmon` with only one instance parameter on an aspect level.

To combine the parameters:

- a. Group the `database_instance` and `INSTANCE` parameters together and name the group, for example, `DBinstance`.
- b. Group the remaining parameters: `user` and `USER` into `DBUser`, `password` and `PASSWORD` into `DBpassword`, `port` and `PORT` into `DBport`.
- c. Make a group named `DBhost` consisting of `HOST=%%HOST%%` and make it hidden, the reason for this being that displaying the combined hostname parameter can lead to cosmetic issues and therefore should not be visible to the user. Moreover, this parameter is redundant, since the `Measurement Threshold` policy template does not require it and the hostname is already defined through the assignment target.

How to Configure Drill Down to SiteScope

With drill down to SiteScope configured, OMi users can right-click a configuration item (CI) or health indicator (HI) in OMi, and then select **Go to SiteScope** to open the related monitor in SiteScope. The SiteScope UI opens in a popup browser window and displays the monitor that sends health information for the selected CI or HI.

Complete the following steps for each SiteScope server for which you want to enable drill down:

1. Make sure the SiteScope server is integrated with OMi. For details, see ["How to Set Up the SiteScope Integration" on page 30](#).
2. Make sure OMi is configured to add the user role information to the LW-SSO token:
 - a. Navigate to Infrastructure Settings:

Administration > Setup and Maintenance > Infrastructure Settings
 - b. Select **Foundations**, and use the list to set the administration context to **Single Sign-on**.
 - c. Make sure the value of **Add user roles information to LW-SSO token** is **true**.
3. Make sure the passphrase string for LW-SSO in SiteScope matches the string in OMi:
 - a. In OMi, navigate to Authentication Management:

Administration > Users > Authentication Management
 - b. Copy the value of **Token Creation Key (initString)** to the clipboard.
 - c. In the SiteScope UI, open **Preferences > General Preferences > LW SSO Settings**. Replace the value of **LW SSO Init String** with the value copied from the OMi server.
Alternatively, on the SiteScope server, edit the LW-SSO configuration file:


```
<SiteScope root directory>/conf/lwso/lwsofmconf.xml
```

 Replace the value of the attribute `initString` with the value copied from the OMi server and

save the file.

- d. Restart SiteScope.
4. In OMi, assign the user role **SiteScope Drilldown Role** to all users that should be allowed to drill down to SiteScope. The role is contained in the **OMi Content Pack** and grants the users view permission in SiteScope.

Optional. To grant OMi users additional permissions in SiteScope, create a user role with the name **SiteScope Drilldown Role** in SiteScope and define the additional permissions as required.

How to Drill Down to SiteScope

When SiteScope monitors are used to set the status of a configuration item (CI), you can drill down from the CI (or from a health indicator (HI) on the CI) to a SiteScope monitor that contributes to the HI's status.

1. Access menu commands from a CI or HI in a My Workspace page or component, for example 360° View, Top View, View Explorer, or Health Indicator. Select **Go to > SiteScope**. The SiteScope UI opens directly to the parent group of the relevant monitor.

If monitors from multiple groups contribute to the CI's or HI's status, the **Drilldown to SiteScope** dialog box opens. Select the monitor to which you want to drill down and open it in SiteScope.

The **Drilldown to SiteScope** dialog box displays the following hierarchy:

- The root level shows health indicators.
 - If you open the dialog box for a CI, one or more HIs that contribute to the CI's status are listed.
 - If you open the dialog box for an HI, this HI appears as the root.
- The level below the root shows the SiteScope systems (connected server name) that have monitors contributing to the HI.
- The lowest level shows the SiteScope monitors that contribute to the HI.

Note: In the **System Monitors** view, if you select **Go to > SiteScope** from a monitored CI, SiteScope opens to the monitor's parent group. If you select this from a group CI, SiteScope opens directly to the group.

2. Select a SiteScope monitor, and click **Drilldown**. SiteScope opens to the parent group of the selected monitor.


For details on working with SiteScope, see the Using SiteScope Guide in the SiteScope Help.

Chapter 7: How to Create a Connection to a SiteScope Server

This task describes how to create a server connection to a SiteScope server. It also lists the criteria used to determine the SiteScope server that is most suitable for deploying SiteScope monitors.

- ["How to Create a Connection to a SiteScope Server" below](#)
- ["How To Determine the Target SiteScope Server for Deployment" on the next page](#)

How to Create a Connection to a SiteScope Server

1. Open the Connected Servers manager from Administration.
2. In the **Connected Servers** pane, click  **New** and select **SiteScope**. The **Create New Server Connection** dialog box opens.
3. In the **General** page, provide the following information and make the following selections:
 - a. Enter a display name, a unique internal name (if you want to replace the automatically generated name), and optionally, a description of the connection being specified.
 - b. Select **Active** to enable the server connection immediately.
 - c. Select **Default** to set the SiteScope server as a default server.

If you are creating the first SiteScope server, this option is selected by default and disabled. If a SiteScope server already exists and this option is used when creating a new SiteScope server, the default server is changed to the newly created SiteScope server.

Click **Next** to open the **Server Properties** page.

4. In the **Server Properties** page, provide the following information:
 - a. Under **SiteScope WebService**, enter the fully qualified DNS name of the host system of the SiteScope server, as well as the user name, password, and port number. Click **Set default port** to set a default port number (8443 for secure communication or 8080 if secure communication is not used).

If you are using secure communication (default), make sure the **Use Secure HTTP** option is selected.
 - b. Under **SiteScope Installation**, enter the operating system of the host system of the SiteScope server and the version number of the SiteScope server.
 - c. Click **Test Connection** to check that the specified connection attributes are correct. If an error link is displayed, check the error message, correct the connection information, and re-test the connection.

Note: For the connection test to be successful, you need to have an event integration with SiteScope. There must be a trusted relationship between OMi servers and the SiteScope server. After SiteScope is integrated with OMi, the **Test Connection** check will return a successful result.

Click **Next** to go to the **SiteScope Settings** page.

5. In the **SiteScope Settings** page, provide the following information:
 - a. Under **OMi Credentials**, specify the user name and set the password for the specified OMi user.
 - b. Under **Proxy Server** (required if SiteScope uses a proxy to communicate to OMi), enter the fully qualified DNS name of the proxy system, as well as the proxy user name, the password associated with the proxy user and the proxy port number.
 - c. Under **Topology Settings**, enter the default routing domain from which the SiteScope topology data is collected (the default value is **DefaultDomain**).

The routing domain is a continuous region of an IP network within which routing is possible without any intervening Network Address Translation (NAT) devices. The RTSM uses the routing domain to determine the reconciliation rules and workflows that are applied to a network range.

Additionally, specify the number of days for SiteScope to synchronize topology data with OMi (the default value is **7**).

Click **Finish** to save the newly created server connection.


Note: The Health Check page is only available when health checking is globally enabled in the infrastructure settings and when you *edit* a SiteScope connected server. When you create a new connected server, as described in this task, the default settings from the infrastructure settings are applied.

How To Determine the Target SiteScope Server for Deployment

The following criteria determine the SiteScope server that is most suitable for deploying SiteScope monitors:

- **One SiteScope server.** If you have one configured SiteScope Connected Server, this server is always used as the target for deploying monitors.
- **Multiple SiteScope servers.** For environments with multiple SiteScope servers, OMi, by default, selects the SiteScope server with the most free license points as the target for deployment.

If there is more than one SiteScope server with a sufficient number of free license points, OMi chooses one server at random. To prevent OMi from randomly selecting the SiteScope server to be used for deployment, configure a Groovy server selection script:

- a. Open Infrastructure Settings from Administration.
- b. Select **Applications** and use the list to set the administration context to **Monitoring Automation**.
- c. Go to the **Monitoring Automation - Proxy Deployment Scripts** section.
- d. Open the **HP SiteScope server selection script** edit window (click the associated  button to open the **Edit Setting** dialog box).

The **Edit Setting** dialog box displays the script name and script content. Deployment script templates are located at:

```
<OMi_HOME>/opr/examples/deployment-server-selection
```

- e. Select the script that meets your needs, paste it into the script field replacing the `<XML/>` tag,

and configure it appropriately. You can choose a script to select the SiteScope manager using domain names, IP address ranges, or the one with the most available license points.

Domain Name Example

```
def domainNameMap = ["":"sis.example.com",  
".*.example.com":"test.example.com"]
```

Comma-separated list with the following regular expression format: "domain name pattern":"test.example.com"

If the node domain name of the potential SiteScope server fits the "domain name pattern", the value is taken to find the SiteScope connected server using the Display Name, Name or DNS Name values.

".*" can be used as a wildcard, for example, for ".*hp\\.com" to match "hp.com" or "internal.hp.com".

Tip: Specify an empty domain name for a default server in case no other domain names match.

IP Address Example

```
def ipMap = ["":"sis.example.com", "192\\.168\\.2\\..*":"test.example.com"]
```

The expression is specified as a string and the "." must also be escaped. Hence, "\\." is required to escape the dot.

Comma-separated list with the following format: "IP pattern":"sis server name"

If the IP address of the potential SiteScope server fits the "IP pattern", the value is taken to find the SiteScope connected server using the IP address of the system.

".*" can be used as a wildcard, for example, for "192\\.168\\.2\\..*" to match "192.168.2.10" or "192.168.204.88".

Tip: Specify an empty IP address for a default server in case no other IP addresses match.

- f. Click **Save**.

Part IV: Operations Manager i - HP Operations Manager Integration

Chapter 8: Operations Manager i - HP

Operations Manager Integration Overview

HP Operations Manager (HPOM) can be integrated into your OMi environment to become a data source for OMi. HPOM for Windows, HPOM for UNIX (HP-UX and Solaris), and HPOM for Linux are supported.

After you install both OMi and HPOM, follow the described procedures to connect OMi and HPOM. This connection enables bidirectional synchronization of events between the two systems, tool execution, and instruction text retrieval. The connection configuration requires you to establish a trust relationship between the OMi and HPOM systems, as well as to configure a message forwarding policy.

The integration between OMi and HPOM provides you with the following capabilities:

- **HPOM events > OMi.** Events from HPOM are displayed in the OMi Event Browser.
- **HPOM events > OMi health indicators.** After you set up the integration, if the HPOM events have corresponding health indicators defined, these health indicators automatically affect the status of the relevant Configuration Items (CIs) in OMi applications such as Service Health. For an introduction to health indicators, see the OMi User Guide.
- **OMi Actions, Tools, and Instructions.** You can specify tools, for example, to ping a system. These tools are launched from events or the Actions panel and run on the associated CI. The tools are designed to help users solve common problems quickly and efficiently. All available tools are launched in the context of a CI. The selection of tools a particular user sees in context menus depends on the tools that are available for the CI affected by a particular event.

Events received in the OMi Event Browser may contain event-related actions configured in HPOM. If event-related actions exist, you can run these actions from the OMi console. HPOM actions can be either operator-initiated, or can run automatically when an event occurs. For a complete overview of available actions and how to run them, see the OMi online help.

Operators working with the HPOM message browser can see additional instructions for the selected message. It is equally helpful for OMi operators to be able to access this information when using HPOM servers to forward events to OMi. This information is displayed in the Instructions tab of the Event Browser. For details, see the OMi User Guide.

- **HPOM topology > RTSM topology.** The HPOM topology can synchronize with the OMi RTSM topology. Using topology synchronization, the HPOM services are synchronized with OMi, and using corresponding mapping rules, they are transformed into CIs stored in the RTSM. For details, see the OMi Administration Guide.

Note: If the HPOM topology is not synchronized with the RTSM topology using the OMi topology synchronization mechanism, the **Monitored by** property of the OMi CIs corresponding to the HPOM services may be empty. As a consequence, these CIs are not displayed in the System Monitors only Perspective, System Hardware Monitoring, and System Software Monitoring views.

Chapter 9: Workflow: Configuring Connections Between Operations Manager i and HPOM

1. Establish a trust relationship between OMi and HPOM

For connection and communication between OMi and HPOM hosts, establish a trust relationship between all the servers.

For task details, see ["How to Establish a Trust Relationship for a Server Connection" on page 41](#).

To verify the trusted relationship, see ["How to Verify the Trusted Relationship" on page 44](#).
2. Set up the HPOM server as a connected server

Set up the HPOM server as a connected server so that you can run actions and tools from OMi, and retrieve instructions from the HPOM server.

For task details, see ["How to Create a Connection to an HPOM Server" on page 45](#).
3. Synchronize the topology

To populate the OMi database (RTSM) with the configuration item (topology) and service data from HPOM, you need to synchronize the topology. Topology synchronization is configured to update all specified servers with the topology and service data from the HPOM server.

For task details, see ["How to Run Topology Synchronization" on page 48](#).
4. Configure the HPOM forwarding policy

To enable event synchronization between HPOM and OMi, set up a message forwarding policy on the HPOM server. The policy includes the node name of the target OMi server. Alternatively, specify the load balancers, if configured, or one Gateway Server for each OMi installation, as appropriate for your high-availability arrangement.

 - **HPOM for Windows.** For task details, see ["How to Configure the HPOM for Windows Forwarding Policy" on page 53](#).
 - **HPOM for UNIX or Linux.** For task details, see ["How to Configure the HPOM for UNIX or Linux Forwarding Policy" on page 56](#).
5. Validate event synchronization

Validate event synchronization and test the connection between HPOM and OMi.

For task details, see ["How to Validate Event Synchronization" on page 59](#).

Chapter 10: How to Establish a Trust Relationship for a Server Connection

For connection and communication between OMi and HPOM hosts or other OMi hosts, you must establish a trust relationship between the systems.

In HPOM server pooling, the virtual server must have a certificate that is trusted by all HPOM hosts in the server pool and by all OMi hosts.

Note: The trust relationship must be set up on all nodes (Data Processing Servers, Gateway Servers, manager of manager configurations, load balancers, and reverse proxies). However, some load balancer technologies include a by-pass or pass-through functionality for incoming encrypted messages to its pool members. When using such technologies, the trust relationship on the load balancer node is not required if you are load balancing on the recommended OSI layer 2 or 4.

To establish a trust relationship between the Data Processing Servers and external server systems:

1. On the OMi Data Processing Server, execute the following command:

BBCTrustServer[.bat|sh] <external_server>

Replace **<external_server>** with the FQDN of the external system (for example, hpommgmt.sv).

Note: The value of **<external_server>** should be the virtual name in case of the HPOM server pooling or high-availability (HA) cluster.

When asked if to add a certificate to the trust store, enter **y**.

If the trusted certificate already exists, the tool asks you if you want to overwrite the existing certificate. To replace the existing certificate with a new one, enter **y**.

2. *HPOM servers only:*

Note:

HPOM for Windows: Starting with patches OMW_00121 (32-bit) and OMW_00122 (64-bit), the **BBCTrustServer** tool is already installed in the **%OvInstallDir%\contrib\OVOW** folder.

HPOM for UNIX or Linux: Starting with HPOM server version 9.10.220, the **BBCTrustServer** tool is already installed in the **/opt/OV/bin** directory.

If you have the appropriate HPOM patch or version, you can skip this step.

- a. Locate the following files on the OMi Data Processing Server:

<OMi_HOME>/opr/lib/cli/opr-cli.jar

<OMi_HOME>/opr/bin/BBCTrustServer.bat

<OMi_HOME>/opr/bin/BBCTrustServer.sh

- b. *HPOM for Windows only:* Copy the files to the machine that is running the HPOM for

Windows management server.

Copy **opr-cli.jar** to %OvInstallDir%\javalopr-cli.jar.

Copy **BBCTrustServer.bat** to %OvBinDir%\BBCTrustServer.bat.

- c. *HPOM for UNIX and Linux only*: Copy the files to the machine that is running the HPOM for UNIX or Linux management server.

Copy **opr-cli.jar** to /opt/OV/java/opr-cli.jar.

Copy **BBCTrustServer.sh** to /opt/OV/bin/BBCTrustServer.sh.

Change the permissions of the **BBCTrustServer** tool by entering the following command:

```
chmod 555 /opt/OV/bin/BBCTrustServer.sh
```

3. If you do not have a load balancer or a reverse proxy, or your load balancer is configured to work on **OSI layers 2 or 4** (recommended by HP), execute the following command on the external system:

```
BBCTrustServer.[bat|sh] <load_balancer_or_single_gateway_server_or_RP_or_Server_Pool_Virtual_Interface>
```

When asked if to add a certificate to the trust store, enter **y**.

If the trusted certificate already exists, the tool asks you if you want to overwrite the existing certificate. To replace the existing certificate with a new one, enter **y**.

4. If you are using a reverse proxy or your load balancer is configured to work on **OSI layer 7**, you must exchange the certificates manually:

- a. On the OMi Data Processing Server, execute the following command:

```
ovcert -exporttrusted -file <omi.cer>
```

- b. On the external system, execute the following command:

```
ovcert -exporttrusted -file <other.cer>
```

- c. Copy **<other.cer>** from the external system to the OMi Data Processing Server.

- d. Copy **<omi.cer>** from the OMi Data Processing Server to the external system.

- e. On the OMi Data Processing Server, execute the following commands:

```
ovcert -importtrusted -file <other.cer>
```

```
ovcert -importtrusted -file <other.cer> -ovrg server
```

- f. On the external system, execute the following commands:

```
ovcert -importtrusted -file <omi.cer>
```

```
ovcert -importtrusted -file <omi.cer> -ovrg server
```

5. If you are using a load balancer or a reverse proxy, where your data sources are not communicating directly with the OMi Gateway Servers, make sure that port 383 is routed through the load balancer to the OMi Gateway Servers.

If the load balancer or the reverse proxy is configured to pass through traffic directly (**OSI layers 2 or 4**), skip to the next step. If configured to work on **OSI layer 7**, perform as follows:

- o The certificate on the load balancer must be installed for port 383 (or the port that you configured for secure communication).
- o Communication between the load balancer and the gateway systems must be secured.

- The load balancer must possess a server certificate for authentication so that the external systems can connect successfully. The load balancer must also validate client certificates presented by external clients (for example, HPOM servers).
- The load balancer must possess a client certificate for authentication with OMi.
 - a. Issue a certificate for the load balancer from the OMi Data Processing Server:
ovcm -issue -file <certificate file> -name <Fully Qualified Domain Name of Virtual Interface or Reverse Proxy> [-pass <passphrase>]
 - b. Import this certificate as a server and client certificate into your load balancer.
For details on the required format, see your load balancer documentation. You can use `openssl` to convert the certificates into the required format.
- 6. Check the connection between the servers. For details, see ["How to Verify the Trusted Relationship" on page 44](#).

Chapter 11: How to Verify the Trusted Relationship

After establishing a trust relationship between the OMi Data Processing Server and external systems, check the connection between the two systems. You can do this while setting up your connected server in the **Server Properties** of the **Create New Server Connection** dialog box by selecting **Test Connection**. You can also do this by using the command-line interface:

To check the connection between the OMi server environment and an external system:

1. From the external host, verify that communication to the OMi installation is possible (the return value should be `eServiceOk`) by executing the following command on the external server system:

```
bbcutil -ping https://<load_balancer_or_single_gateway_server_or_RP_or_Server_Pool_Virtual_Interface>
```

Example of the command result:

```
https://<HP OMi servername>: status=eServiceOK  
coreID=7c66bf42-d06b-752e-0e93-e82d1644cef8 bbcV=06.10.105  
appN=ovbbccb appV=11.03.031 conn=1 time=1094 ms
```

2. From all OMi Gateway Server hosts, verify that communication with the external server host is possible (the return value should be `eServiceOk`) by executing the following command:

```
bbcutil -ping https://<external_server_hostname>
```

Example of the command result:

```
https://<external_host_server_name>: status=eServiceOK  
coreID=0c43c032-5c94-7535-064a-f7654a86f2d3 bbcV=06.10.070  
appN=ovbbccb appV=11.03.031 conn=7 time=140 ms
```

Troubleshooting:

If the **bbcutil -ping** command executes but does not return **eServiceOk**, you may need to restart the **ovc** processes on the system that is not responding by running the following commands:

- Linux: **/opt/OV/bin/ovc -kill** and **/opt/OV/bin/ovc -start**
- Windows: **ovc -kill** and **ovc -start**

Chapter 12: How to Create a Connection to an HPOM Server

OMi can forward events, run actions and tools on the HPOM server, and retrieve instructions from the HPOM server. Credentials for the HPOM web service are required for this processing.

1. In the **Connected Servers** pane, click *** New** and select **Operations Manager for Windows** or **Operations Manager for UNIX**. The **Create New Server Connection** dialog box opens.
2. In the **General** page, complete the following information:
 - a. Enter a display name, a unique internal name, if you want to replace the automatically generated name, and (optional) a description of the connection being specified.
 - b. Select **Active** if you want to enable the server connection immediately.
 - c. Click **Next** to open the **Server Properties** page.

3. In the **Server Properties** page, complete the following information:
 - a. Enter the fully qualified DNS name of the host system of the HPOM server.
If the host system is a high-availability cluster, enter the fully qualified DNS name of the cluster package where the HPOM server is installed.
If HPOM is installed in a server pooling environment, add the virtual interface as the first HPOM server. Add all physical pool servers separately as connected servers.
 - b. Enter the **Integration User** name used to log on to the HPOM server.

Note: All messages forwarded from HPOM systems are treated as allowing read and write. Any changes made to these events result in back synchronization to the originating HPOM server.

For HPOM for Windows, the selected user must have at least PowerUser rights and must be a member of the HP-OVE-Admins group and the local administrators group (for example, HP-OVE-User).

For HPOM for UNIX or Linux, the Integration User must have HPOM administrator rights (opc_adm) to be able to synchronize topology and execute tools.

- c. **Optional. Advanced Delivery Options** It is possible to customize the way events and change notifications are delivered to this server. The available options are:
 - **Serial** — Events and change notifications are delivered serially in the order that they were received.
 - **Serial per Source** — (*Default*) Each originating server is provided with a dedicated outgoing request delivery path. For each individual outgoing request delivery path, events and change notifications are delivered serially in the order that they were received. This can increase the throughput for delivery of events and change notifications when many events are received from multiple originating servers, while maintaining the incoming order.
 - **Parallel** — The configured number of outgoing request delivery paths is used when

forwarding events and change notifications. This can further increase the throughput for delivery of events and change notifications. However, because the source of the event is not considered, maintenance of the incoming order cannot be guaranteed.

- d. Specify if you want to forward dynamic topology information from the OMi instance to which you are logged on, to the HPOM instance that you are currently configuring.

Note:

If you change the status of the **Forward Dynamic Topology to this Target Server** check box, you must restart the WDE process on all gateway servers. To do so, run the following commands:

```
<OMi_HOME>/opr/support/opr-support-utils.[bat|sh] -stop wde
```

```
<OMi_HOME>/opr/support/opr-support-utils.[bat|sh] -start wde
```

- e. Click **Test Connection** to check that the specified connection attributes are correct. If an error link is displayed, check the error message, correct the connection information, and retest the connection.
 - f. Click **Next** to open the **Outgoing Connection** page.
4. **Outgoing Connection** The outgoing connection is used to receive instructions, and execute tools and actions on external nodes.

Note: If you edit outgoing connection properties (for example, integration user, password, and port), you must restart the **MercuryAS** process for the changes to take effect.

Complete the following information:

- o **If you are using this server** for receiving instructions, and executing tools and actions on external nodes, enter the password for the integration user and the port required to access the server for receiving instructions, and executing tools and actions. The default port value is automatically inserted and can be restored using **Set default port**.

Note: For HPOM for Windows, the selected user must have at least PowerUser rights and must be a member of the HP-OVE-Admins group and the local administrators group.

For HPOM for UNIX or Linux, the Integration User must have HPOM administrator rights (opc_adm) to be able to synchronize topology and execute tools.

Optional. If you are using secure communication (default), make sure that the **Use Secure HTTP** option is selected, and apply a certificate using one of the following methods:

- **Import from File** — Opens the file browser and enables you to navigate to and specify a Base64 Encoded X.509 certificate file for the server connection.
- **Retrieve from Server** — Retrieve a certificate from the host system specified in this server connection.

Note: In a clustered HPOM for Windows environment, the IIS web server on all cluster nodes must have the same certificate. If different, valid certificates are used, problems such as tools execution may be experienced after switching to a node with a different certificate.

For more details, see the HP Software Self-solve knowledge base, article number KM01211399, which can be accessed at:

<http://h20230.www2.hp.com/selfsolve/document/KM01211399>

Note: Secure communication is necessary for HPOM server pooling environments. However, do not use the Import from File or Retrieve from Server options.

Set up a trusted relationship between all HPOM and OMi servers as described in "[How to Establish a Trust Relationship for a Server Connection](#)" on page 41.

- **If you are using an alternative server** for providing instructions, and executing actions and tools, select **Use other Server**, and then select a server from the list. For the physical servers in a server pooling environment, select the virtual interface connected server.

Note: Avoid selecting an alternative action execution server that creates a loop and results in specifying the connected server as the action execution server. Select an alternative action execution server or use the **Use this Server** option.

Click **Test Connection** to check that the specified connection attributes are correct. If an error link is displayed, check the error message, correct the connection information, and retest the connection.

5. Click **Finish**.

Chapter 13: How to Run Topology Synchronization

Before configuring the forwarding of topology (node and service) data to OMi from HPOM servers, complete the following configuration steps in OMi:

- Establish a trust relationship between the Data Processing Server and the HPOM server. For details, see ["How to Establish a Trust Relationship for a Server Connection" on page 41](#).
- Add the HPOM server as a connected server to OMi. For details, see ["How to Create a Connection to an HPOM Server" on page 45](#).
- *Optional*. Import content packs. For details, see "Content Packs" in the OMi Administration Guide.
- *Optional*. Use the `opr-sdtool.[bat|sh]` command line tool to upload new or changed synchronization packages from the file system to the database. For details, see the OMi Extensibility Guide.

Note: You can also use the Content Manager to import and export the existing synchronization packages in the Content Manager format.

After ensuring that the HPOM server is added to OMi as a connected server, configure the forwarding of topology (node and service) data on the HPOM server.

The following sections describe how to configure topology synchronization:

- ["How to Configure Topology Synchronization on HPOM for Windows Systems" below](#)
- ["How to Migrate from Scheduled Synchronization on HPOM for Windows Systems" on the next page](#)
- ["How to Configure Topology Synchronization on HPOM for UNIX or Linux Systems" on page 50](#)
- ["How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems" on page 51](#)

How to Configure Topology Synchronization on HPOM for Windows Systems

This section describes how to configure topology synchronization on HPOM for Windows management servers. For further details, see the HPOM for Windows documentation.

To forward topology data to OMi, complete the following steps on the HPOM for Windows management server from which you want to receive topology information:

1. *Prerequisite*. Make sure that the minimum patch level for the HPOM for Windows management server is installed:
 - Version 8.16: Patch OMW_00121 or superseding patch
 - Version 9.00: Patch OMW_00122 or superseding patch
2. *Prerequisite*. Configure trusted certificates for multiple servers.

In an environment with multiple servers, you must configure each server to trust certificates that the other servers issued.

3. In the console tree, right-click **Operations Manager**, and then click **Configure > Server....** The Server Configuration dialog box opens.
4. Click **Namespaces**, and then click **Discovery Server**. A list of values appears.
5. Add the hostname of the server to **List of target servers to forward discovery data**. If there is more than one target server, separate the hostnames with semicolons, for example:

```
server1.example.com;server2.example.com
```

If the target server uses a port other than port 383, append the port number to the hostname, for example:

```
server1.example.com:65530;server2.example.com:65531
```

6. Make sure that the value of **Enable discovery WMI listener** is true. This is the default value.
7. Click **OK** to save your changes and close the Server Configuration dialog box.
8. Restart the `OvAutoDiscovery Server` service for your changes to take effect:

```
net stop "OvAutoDiscovery Server"  
net start "OvAutoDiscovery Server"
```
9. Start the initial synchronization of topology data:

- a. In the console tree, select **Tools > HP Operations Manager Tools**.
- b. Right-click **Synchronize Topology** and select **All Tasks > Launch Tool....**

The `startInitialSync.bat` tool is started and begins to send all the topology data to the configured target management servers.

How to Migrate from Scheduled Synchronization on HPOM for Windows Systems

This section describes how to migrate from scheduled synchronization on HPOM for Windows management servers. For further details, see the HPOM for Windows documentation.

To migrate from scheduled synchronization, complete the following steps on the HPOM for Windows management server from which you want to receive topology information:

1. *Prerequisite.* Make sure that the minimum patch level for the HPOM for Windows management server is installed:
 - Version 8.16: Patch OMW_00121 or superseding patch
 - Version 9.00: Patch OMW_00122 or superseding patch
2. Clear the agent repository cache on the HPOM management server using the following command:

```
%OvBinDir%\ovagtrep -clearall
```
3. Remove the service auto-discovery policies from the HPOM management server node:

```
%OvBinDir%\ovpolicy -remove DiscoverOM  
%OvBinDir%\ovpolicy -remove DiscoverOMTypes
```
4. Synchronize the policy inventory on the HPOM management server:

- a. In the console tree, right-click the management server.
 - b. Select **All Tasks > Synchronize inventory > Policies**.
The management server creates a deployment job to retrieve the inventory from the local agent.
5. Make sure the listener process is running:
- a. In the console tree, right-click **Operations Manager**, and select **Configure Server**.
The Server Configuration dialog box opens.
 - b. Click **Namespaces**, and select **Discovery Server**.
A list of values appears.
 - c. Set the value of **Enable discovery WMI listener** to true. This is the default value.
 - d. Click **OK** to save your changes and close the Server Configuration dialog box.
 - e. Restart the `OvAutoDiscovery Server` service for your changes to take effect:

```
net stop "OvAutoDiscovery Server"  
net start "OvAutoDiscovery Server"
```
6. Start the initial synchronization of topology data:
- a. In the console tree, select **Tools > HP Operations Manager Tools**.
 - b. Right-click **Synchronize Topology** and select **All Tasks > Launch Tool...**
The `startInitialSync.bat` tool is started and begins to send all the topology data to the configured target servers.

How to Configure Topology Synchronization on HPOM for UNIX or Linux Systems

This section describes how to configure topology synchronization on HPOM for UNIX or Linux management servers. For further details, see the HPOM for UNIX or Linux documentation.

To forward topology data to OMi, complete the following steps on the HPOM for UNIX or Linux management server from which you want to receive topology information:

1. *Prerequisite.* Make sure that the minimum patch level for the HPOM 9.10 for UNIX or Linux management server is installed:
 - HP-UX: Patch PHSS_42736 or superseding patch
 - Linux: Patch OML_00050 or superseding patch
 - Solaris: Patch IT050L_00772 or superseding patch
2. *Prerequisite.* Configure trusted certificates for multiple servers.
In an environment with multiple servers, you must configure each server to trust certificates that the other servers issued.
3. *Prerequisite.* Set up the forwarding target (OMi Gateway Server, Reverse Proxy, or Load Balancer) in the node bank as a managed node. To do so, run the following command:

```
/opt/OV/bin/OpC/utils/opcnode -add_node node_name=<node_name> net_type=NETWORK_  
IP mach_type=<machine_type> group_name=<group_name> node_label=<node_name>
```

In this instance, *<machine_type>* relates to the operating system of the OMi host system, MACH_BBC_WIN2K3_X64 (Windows) or MACH_BBC_LX26RPM_X64 (Linux), whereas *<group_name>* relates to the operating system of the HPOM server host system, hp_ux, solaris, or linux.

4. Type the following command to enable topology synchronization:

```
/opt/OV/contrib/OpC/enableToposync.sh -online -target <comma_separated_server_list>
```

Replace *<comma_separated_server_list>* with the fully qualified domain name of the target management server. If you have more than one target management server, separate each server name with a comma (.). Do not include spaces in the server list.

This command restarts the service discovery server. The source management server begins to send any topology data changes immediately.

5. Type the following command to start the initial synchronization of topology data:

```
/opt/OV/bin/OpC/startInitialSync.sh
```

How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems

This section describes how to migrate from scheduled synchronization on HPOM for UNIX or Linux management servers. For further details, see the HPOM for UNIX or Linux documentation.

To migrate from scheduled synchronization, complete the following steps on the HPOM for UNIX or Linux management server from which you want to receive topology information:

1. *Prerequisite.* Make sure that the minimum patch level for the HPOM 9.10 for UNIX or Linux management server is installed:
 - HP-UX: Patch PHSS_42736 or superseding patch
 - Linux: Patch OML_00050 or superseding patch
 - Solaris: Patch IT050L_00772 or superseding patch

2. Clear the agent repository cache on the management server using the following command:

```
/opt/OV/bin/ovagtrep -clearall
```

3. Remove the service auto-discovery policies from the management server node:

```
/opt/OV/bin/ovpolicy -remove DiscoverOM  
/opt/OV/bin/ovpolicy -remove DiscoverOMTypes
```

4. Deassign the service auto-discovery policies from the management server node:

```
/opt/OV/bin/OpC/utills/opcnode -deassign_pol node_name=<management_server> net_  
type=NETWORK_IP pol_name=DiscoverOMTypes pol_type=svcdisc  
/opt/OV/bin/OpC/utills/opcnode -deassign_pol node_name=<management_server> net_  
type=NETWORK_IP pol_name=DiscoverOM pol_type=svcdisc  
/opt/OV/bin/OpC/opcragt -dist <management_server>
```

Replace *<management_server>* with the name of the management server.

5. Type the following command to enable topology synchronization:

```
/opt/OV/contrib/OpC/enableToposync.sh -online
```

This command restarts the service discovery server. The source management server begins to send any topology data changes immediately.

6. Type the following command to start the initial synchronization of topology data:

```
/opt/0V/bin/OpC/startInitialSync.sh
```

Chapter 14: How to Configure the HPOM for Windows Forwarding Policy

To enable event synchronization between HPOM and OMi, set up a message forwarding policy on the HPOM server. The policy includes the node name of the target OMi server. Alternatively, specify the load balancers, if configured, or one Gateway Server for each OMi installation, as appropriate for your high-availability arrangement.

Before setting up a policy and to avoid overwriting the current settings, verify if a policy of the type **Server-based Flexible Management** is already active on the HPOM for Windows server. If a policy does not exist, create a new policy as described in ["Create a New Policy"](#) below. If a policy already exists and is active, adapt the policy as described in ["Adapt an Active Policy"](#) on the next page.

Create a New Policy

To set up a new policy on HPOM for Windows, complete the following steps:

1. Start the HPOM for Windows console as follows:
Start > Programs > HP > HP Operations Manager
2. In the left pane of the HPOM for Windows console, select the following:
Policy management > Policies grouped by type > Server Policies > Server-based Flexible Management
3. Verify that no Server-based Flexible Management policy exists. If such a policy does exist, go to ["Adapt an Active Policy"](#) on the next page.
4. Right-click **Server-based Flexible Management** (or a blank space in the right pane), and then select **New > Policy**.

The Server-based Flexible Management Editor dialog opens.

5. In the **General** tab text pane, insert the following policy text:

```
TIMETEMPLATES
# none
RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
SECONDARYMANAGERS
ACTIONALLOWMANAGERS
MSGTARGETRULES
  MSGTARGETRULE DESCRIPTION "Forward all messages rule"
  MSGTARGETRULECONDS
  MSGTARGETRULECOND DESCRIPTION "Forward all messages"
  MSGTARGETMANAGERS
    MSGTARGETMANAGER
    TIMETEMPLATE "$OPC_ALWAYS"
    OPCMGR IP 0.0.0.0 "<HP OMi fully qualified host name>"
```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, modify the text of the policy so that only a selected subset of messages is sent to OMi. For details, see the HPOM documentation.

6. Replace <HP OMi fully qualified host name> in the policy text with the fully qualified hostname of the Gateway server to receive HPOM messages (for example, HPGWsrv.example.com).
In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway server (for example, VirtualSrv.example.com).
7. Click **Check Syntax** to check for syntax errors in the new policy text.
8. After correcting any syntax errors, click **Save and Close**.
9. In the Save As dialog box that opens, enter a name and a description for the new policy.
10. Click **OK** to close the Save As dialog.
11. From the Policy Management folder, right-click the policy, and then select **All Tasks > Deploy on**.
12. In the Deploy server policy on dialog box that opens, select the name of your HPOM management server.
13. Click **OK** to deploy the server-based flexible management policy on the HPOM for Windows management server.

Adapt an Active Policy

If a message forwarding policy already exists on the HPOM for Windows system, complete the following steps to edit this policy and add another message target manager to it:

1. Start the HPOM for Windows console as follows:
Start > Programs > HP > HP Operations Manager
2. In the left pane of the HPOM for Windows console, select the following:
Policy management > Server policies grouped by type > Server-based Flexible Management
3. In the right pane of the HPOM for Windows console, double-click the existing policy that you want to edit. The Server-based Flexible Management Editor dialog opens.
If such a policy does not exist, go to ["Create a New Policy" on the previous page](#).
4. Add another message target manager as shown in the following example policy text:

```
TIMETEMPLATES
# none
RESPMGRCONFIGS
    RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
SECONDARYMANAGERS
ACTIONALLOWMANAGERS
MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
        MSGTARGETRULECONDS
        MSGTARGETRULECOND DESCRIPTION "Forward all messages"
```

```
MSGTARGETMANAGERS
MSGTARGETMANAGER
TIMETEMPLATE "$OPC_ALWAYS"
OPCMGR IP 0.0.0.0 "<First Target Manager>"

MSGTARGETMANAGER
TIMETEMPLATE "$OPC_ALWAYS"
OPCMGR IP 0.0.0.0 "<HP OMi fully qualified host name>"
```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, modify the text of the policy so that only a selected subset of messages is sent to OMi. For details, see the HPOM documentation.

5. Replace <HP OMi fully qualified host name> in the text with the fully qualified hostname of the Gateway server that should receive HPOM messages (for example, HPGwSrv.example.com). In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway server (for example, VirtualSrv.example.com).
6. Click **Check Syntax** to check for syntax errors in the new policy text.
7. After correcting any syntax errors, click **Save and Close**.
8. Redeploy the server-based flexible management policy on the HPOM for Windows management server.

Chapter 15: How to Configure the HPOM for UNIX or Linux Forwarding Policy

To enable event synchronization between HPOM and OMi, you must set up a message forwarding policy on each HPOM management server with the node name of the load balancer, if configured, or one Gateway Server, as appropriate for your high-availability arrangement.

Before setting up a policy, make sure that the forwarding target is set up as a node (see ["Set up a Forwarding Target in the HPOM for UNIX or Linux Node Bank"](#) below). In addition, verify if the **msgforw** policy is already active on the HPOM for UNIX or Linux server. If the **msgforw** does not exist, create a new policy as described in ["Create a New Policy"](#) below. If the **msgforw** policy already exists and is active, adapt the policy as described in ["Adapt an Active Policy"](#) on the next page.

Set up a Forwarding Target in the HPOM for UNIX or Linux Node Bank

Note: Make sure that the SNMP agent is running before adding a managed node to the HPOM database.

The forwarding target (OMi Gateway Server, Reverse Proxy, or Load Balancer) must be set up in the node bank as a managed node. You must add the managed node by using the `opcnode` command line tool:

```
/opt/OV/bin/OpC/Utils/opcnode -add_node node_name=<node_name> net_type=NETWORK_IP  
mach_type=<machine_type> group_name=<group_name> node_label=<node_name>
```

In this instance, `<machine_type>` relates to the operating system of the OMi host system, `MACH_BBC_WIN2K3_X64` (Windows) or `MACH_BBC_LX26RPM_X64` (Linux), whereas `<group_name>` relates to the operating system of the HPOM server host system, `hp_ux`, `solaris`, or `linux`.

To verify that the node was added successfully, run the following command:

```
/opt/OV/bin/OpC/Utils/opcnode -list_nodes
```

Create a New Policy

To set up a new message forwarding policy on HPOM for UNIX or Linux, complete the following steps:

1. Change to the `work_respmgrs` directory as follows:

```
cd /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs/
```

Note: Policy template files can be found in `/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`.

2. Create a new policy file using the following command:

```
vi <policy file name>
```
3. Insert the following text into the new policy file:


```

TIMETEMPLATES
# none
RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS
  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
    MSGTARGETRULECONDS
    MSGTARGETRULECOND DESCRIPTION "Forward all messages"
    MSGTARGETMANAGERS
      MSGTARGETMANAGER
      TIMETEMPLATE "$OPC_ALWAYS"
      OPCMGR IP 0.0.0.0 "<HP OMi fully qualified host name>"

```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, modify the text of the policy so that only a selected subset of messages is sent to OMi. For details, see the HPOM documentation.

4. Replace `<HP OMi fully qualified host name>` in the text with the fully qualified hostname of the Gateway server that should receive HPOM messages (for example, `HPGwSrv.example.com`). In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway server (for example, `VirtualSrv.example.com`).
5. Enter the following command to check for syntax errors in the new policy text:
`/opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>`
6. After correcting any syntax errors, copy the policy to the `msgforw` policy file in the `respmgrs` directory as follows:
`cp <policy file name> /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw`
7. Inform the server processes to reread the configuration as follows:
`/opt/OV/bin/ovconfchg`
Message forwarding from HPOM to OMi is now configured and enabled.

Adapt an Active Policy

If the message forwarding policy already exists on the HPOM for UNIX or Linux system, complete the following steps to edit this policy and add another message target manager to it:

1. Change to the `work_respmgrs` directory as follows:
`cd /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs/`

Note: Policy template files can be found in `/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs/`.

2. Edit the existing policy to which you want to add the OMi server as a target as follows:
`vi <policy file name>`

3. Add another message target manager as shown in the following policy text:

```
# none
RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS
  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
    MSGTARGETRULECONDS
    MSGTARGETRULECOND DESCRIPTION "Forward all messages"
    MSGTARGETMANAGERS
      MSGTARGETMANAGER
      TIMETEMPLATE "$OPC_ALWAYS"
      OPCMGR IP 0.0.0.0 "<First Target Manager>"

      MSGTARGETMANAGER
      TIMETEMPLATE "$OPC_ALWAYS"
      OPCMGR IP 0.0.0.0 "<HP OMi fully qualified host name>"
```

Note: This policy forwards all messages to OMi. If you want to reduce the number of messages to be sent, modify the text of the policy so that only a selected subset of messages is sent to OMi. For details, see the HPOM documentation.

4. Replace `<HP OMi fully qualified host name>` in the text with the fully qualified hostname of the Gateway Server system that should receive HPOM messages (for example, `HPGwSrv.example.com`).
In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway Server system (for example, `VirtualSrv.example.com`).
5. Enter the following command to check for syntax errors in the new policy text:
`/opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>`
6. After correcting any syntax errors, copy the policy to the `msgforw` policy file in the `respmgrs` directory as follows:
`cp <policy file name> /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw`
7. Inform the server processes to reread the configuration as follows:
`/opt/OV/bin/ovconfchg`
Message forwarding from HPOM to OMi is now configured and enabled.

Chapter 16: How to Validate Event Synchronization

This chapter provides you with instructions on how to validate event synchronization and test the connection between HPOM and OMi.

Note: Make sure that you configured HPOM to enable OMi users to use tools, actions, and instruction text. You configure this in the Connected Servers manager in OMi. For details, see ["How to Create a Connection to an HPOM Server" on page 45](#).

Verify Message Forwarding from HPOM to OMi

To check if the message forwarding policy for sending messages from HPOM to OMi is configured correctly, follow these steps:

1. Make sure the OMi servers are running.
2. Make sure at least one open message interface policy is deployed on your HPOM system. For instructions and details, see the HPOM documentation.
3. On the HPOM system, open a command or shell prompt and create a new message by executing the following command:
 - Windows:
opcmmsg a=App o=Obj msg_text="Hello"
 - UNIX or Linux:
/opt/OV/bin/OpC/opcmmsg a=App o=Obj msg_text="Hello"

If you configured the message forwarding policy correctly, the message arrives at the HPOM server and is forwarded to OMi. You can view the events with the OMi Event Browser.

Note: If the message is sent multiple times, no new message is generated by HPOM. These messages are regarded as duplicates and only the message duplicate count is increased.

To generate a new message, modify the message text. For example:

- Windows:
opcmmsg a=App o=Obj msg_text="Hello_002"
- UNIX or Linux:
/opt/OV/bin/OpC/opcmmsg a=App o=Obj msg_text="Hello_002"

Synchronize OMi Events with HPOM Messages

To check if a change to an event in OMi that is already synchronized between OMi and HPOM is

resynchronized in HPOM, change the severity of an event as follows:

1. Make sure the OMi platform is running.
2. Log on to the OMi platform management console.
3. Select **Applications > Operations Management**.
4. In the Event Browser, select the event for which you want to change the severity. Choose the event that was already synchronized in HPOM and OMi and change its severity, for example, from minor to major.
5. Access the General tab of the Event Details pane.
6. From the Severity drop-down list, choose another severity (for example, major), and then click **Save**.
7. In the HPOM event browser, verify the severity of this event and make sure it was set to the new severity value.

Chapter 17: How to Set up Operations Manager i in an Environment Managed by HPOM

To set up OMi in an environment managed by HPOM, follow these steps:

1. Before installing OMi, on all Data Processing Servers and Gateway Servers, run the following command:
ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <FQDN of primary DPS>
2. Install and configure OMi according to the OMi Installation and Upgrade Guide.
3. Integrate HPOM as described in "[Workflow: Configuring Connections Between Operations Manager i and HPOM](#)" on page 40.

Chapter 18: OMi Field Mapping

The following table shows the correspondence between the fields of an OMi event and an HPOM message.

OMi Event Attribute	HPOM Message	
	HPOM Message Attribute	HPOM Custom Message Attribute (CMA)
ID	Message ID	
Title	Message Text	
Description		Description
Lifecycle State/State (depending on space)	N/A	
Solution		Solution
Severity	Severity	
Priority		Priority
Category	Message Group	
Subcategory		SubCategory
Type	Message Type	
Related CI Hint		RelatedCiHint (incoming to OMi)
HPOM Service ID	Service Name	
Related CI	N/A	
Node	N/A	
Node Hint, DNS Name, IP Address, Core ID	node	NodeHint (incoming to OMi)
Source CI Hint, DNS Name, IP Address, Core ID	genNode	SourceCiHint (incoming to OMi)
Originating Server	origin	
Sending Server	sender	

OMi Event Attribute	HPOM Message	
	HPOM Message Attribute	HPOM Custom Message Attribute (CMA)
Assigned User	owner	
Assigned Group	N/A	
C (Event Browser) Because there is a parent event, the current event will be shown as being a symptom.		CauseEventId (synchronized back to HPOM)
C (Event Browser) Because there is at least one child event, the current event will be shown as being a cause.	N/A	
Custom Attributes	CustomMessageAttributes	
Time Created	CreationTime	
Time State Changed	N/A	
Time Received	ReceivedTime	
Duplicate Count	NumberOfDuplicates	
ETI Hint		EtiHint (incoming to OMi)
User Action	Operator Initiated Action	
Automatic Action	Automatic Action	
Application	Application	
Object	Object	
Key (only in details)	MessageKey	
Close Events with Key	Pattern of 1. MessageKeyRel	
Original Data	OriginalText	
(This field is not displayed, but events that have this attribute arrive as closed.)	logOnly	

OMi Event Attribute	HPOM Message	
	HPOM Message Attribute	HPOM Custom Message Attribute (CMA)
Match Information	policy, conditionId (unmatched)	
Original ID (only in details)	origId	
Correlation Rule	N/A	
Source CI	N/A	
No Duplicate Suppression		NoDuplicateSuppression (incoming to OMi)
Event Type Indicator/ETI	N/A	
part of CI (after :)		SubCiHint (incoming to OMi)

Chapter 19: Troubleshooting

This section contains troubleshooting information about HPOM integration-related issues.

Cleanup after switching HPOM to another OMi server

After reconnecting HPOM to another OMi server, for example after activating a disaster recovery environment, you should delete the buffered messages on the HPOM system for the old OMi server. If the messages are left in the forwarding buffer, there may be some performance degradation as the system regularly tries to deliver them without success. They also consume some disk space. It is not possible to re-direct these messages to the new OMi server, and these cannot be synchronized.

Note: All messages currently in the buffer are deleted. It is not possible to distinguish between different targets and messages for other targets are also deleted.

To delete the forwarding buffer files on HPOM for Windows:

1. Stop the server processes: `vpstat -3 -r STOP`
2. Delete all files and folders contained within the following directories:
`<OvDataDir>\shared\server\datafiles\bbc\snf\data`
`<OvDataDir>\shared\server\datafiles\bbc\snf\OvEpMessageActionServer`
3. Restart the server processes: `vpstat -3 -r START`

To delete the forwarding buffer files on HPOM for UNIX:

1. Stop the server processes: `ovc -kill`
2. Delete all files and folders contained within the following directories:
`/var/opt/OV/shared/server/datafiles/bbc/snf/data`
`/var/opt/OV/share/tmp/OpC/mgmt_sv/snf/opcforwm`
3. Restart the server processes: `ovc -start`

Specifying the URL of a Load Balancer

If the HPOM server is connected to OMi using a load balancer, the URL of the load balancer (`http://<load balancer>:80`) must be specified in the infrastructure setting:

Foundation > Platform Administration > Host Configuration > Default Virtual Gateway Server for Data Collectors URL

Note: If you omit this setting, event synchronization might get confused as it is using the wrong sender hostname (the physical gateway server in place of the virtual system name).

Part V: Operations Manager i - Service Manager Integration

Chapter 20: Operations Manager i-Service Manager Integration Overview

This section describes the integration between HP Service Manager and Operations Manager i.

If your setup uses an external UCMBD, follow the steps provided in ["OMi-SM Integration with UCMBD" on page 115](#).

If not, follow the steps provided in ["OMi-SM Integration with RTSM" on page 71](#).

Versions

In general, the information provided in this guide is for integrating OMi with SM 9.4x.

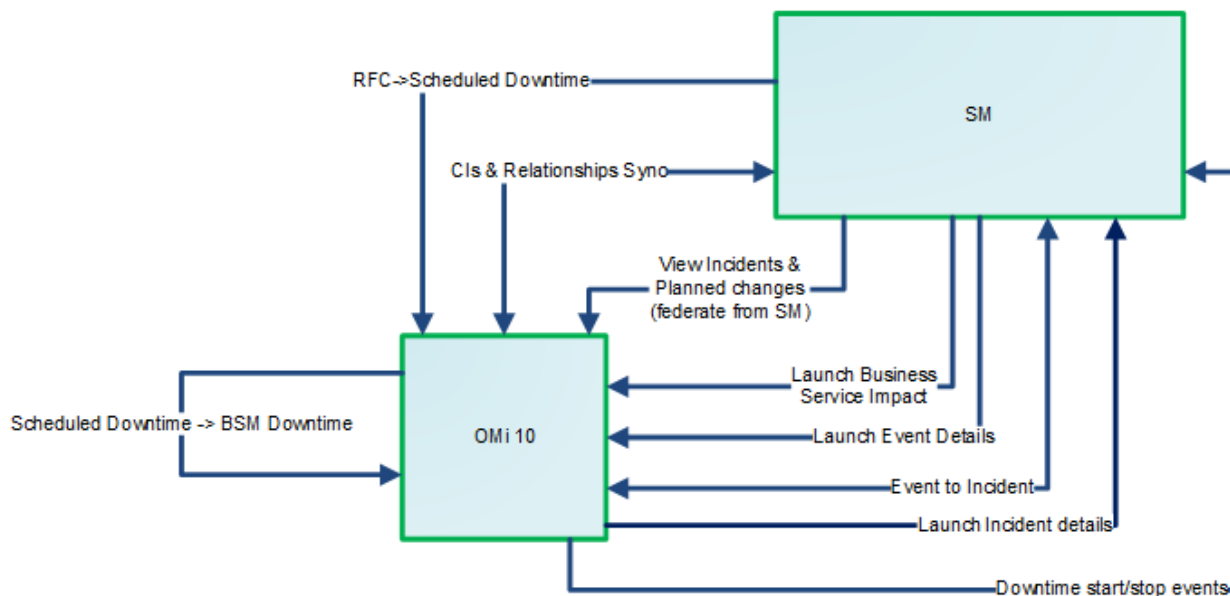
Caution: When integrating OMi with SM 9.40, make sure that one of the following patches are applied:

- 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

OMi-SM Integration Options with RTSM

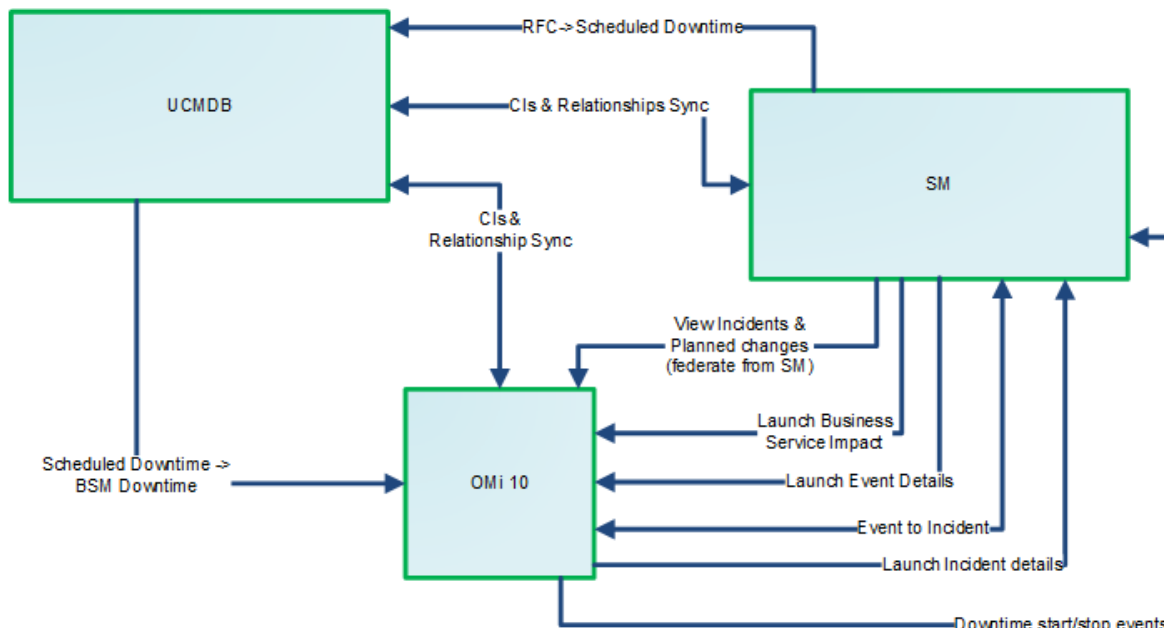
The following figure shows the options for integrating OMi and SM when using the RTSM. For detailed information, see ["OMi-SM Integration with RTSM" on page 71](#).



- **CIs synchronization between SM and OMi.** To enable operators of all systems to see the same CIs, important service, business application, and infrastructure CIs should be synchronized between all systems. Synchronized CIs are a prerequisite for all other integration features. For details, see ["RTSM-Service Manager Integration" on page 73](#).
- **Incident forwarding 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 or from SM incidents to OMi events. For details, see ["Event Forwarding from OMi to SM \(RTSM\)" on page 81](#).
- **Downtime forwarding from SM to OMi.** You can create downtimes (also known as outages) in OMi based on Requests for Changes in SM. This is done in two steps. First, scheduled downtime CIs are created in OMi based on RFCs in SM. Then, a BSM downtime CI is created based on the scheduled downtime. For details, see ["Downtime Forwarding from Service Manager to OMi \(RTSM\)" on page 98](#).
- **Downtime notification from OMi to SM.** OMi can send downtime start and end events to SM to notify operators when a downtime occurs. This provides additional information to the SM operator in case of a downtime that was not driven by an RFC. For details, see ["Sending downtime notifications from OMi to SM \(RTSM\)" on page 104](#).
- **View planned changes and incident details.** This integration enables you to view planned changes and incident details in the Changes and Incidents and Hierarchy components in OMi. For details, see ["View Changes and Incidents in OMi \(RTSM\)" on page 106](#).
- The **Business Impact Report** integration enables Service Manager operators to launch an impact report from an incident in the context of the incident's affected CI. This opens an OMi KPI over time page, displaying the affected CI and impacted CIs and services, which allows the operator to categorize and prioritize the incident accordingly. For details, see ["Business Impact Report \(BIR\) \(RTSM\)" on page 113](#).

OMi-SM Integration Options with UCMDB

The following figure shows the options for integrating OMi and SM when using a UCMDB. For detailed information, see ["OMi-SM Integration with UCMDB" on page 115](#).



- CIs synchronization between SM and UCMDB.** To enable operators of all systems to see the same CIs, important service, business application, and infrastructure CIs should be synchronized between all systems. Synchronized CIs are a prerequisite for all other integration features. With an external UCMDB, CIs are synchronized from SM to the UCMDB system and vice versa (for details, see ["UCMDB-Service Manager Integration" on page 117](#)), and from the UCMDB system to OMi and vice versa (for details, see ["OMi-UCMDB Integration" on page 117](#)). In this case, the UCMDB acts as Global ID generator.
- Incident forwarding 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 or from SM incidents to OMi events. For details, see ["Event Forwarding from OMi to SM \(UCMDB\)" on page 125](#).
- Downtime forwarding from SM to OMi.** You can create downtimes (also known as outages) in OMi based on Requests for Changes in SM. This is done in two steps. First, scheduled downtime CIs are created in UCMDB based on RFCs in SM. Then, a BSM downtime CI is created in OMi based on the scheduled downtime. For details, see ["Downtime Forwarding from Service Manager to OMi \(UCMDB\)" on page 143](#).
- Downtime notification from OMi to SM.** OMi can send downtime start and end events to SM to notify operators when a downtime occurs. This provides additional information to the SM operator in case of a downtime that was not driven by an RFC. For details, see ["Sending downtime notifications from OMi to SM \(UCMDB\)" on page 149](#).
- View planned changes and incident details.** This integration enables you to view planned changes and incident details in the Changes and Incidents and Hierarchy components in OMi. For details, see ["View Changes and Incidents in OMi \(UCMDB\)" on page 151](#).

- The **Business Impact Report** integration enables Service Manager operators to launch an impact report from an incident in the context of the incident's affected CI. This opens an OMi KPI over time page, displaying the affected CI and impacted CIs and services, which allows the operator to categorize and prioritize the incident accordingly. For details, see "[Business Impact Report \(BIR\) \(UCMDB\)](#)" on page 158.

Chapter 21: OMi-SM Integration with RTSM

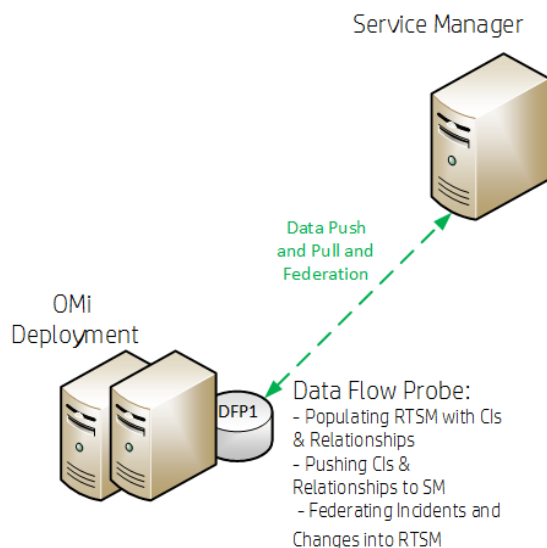
This section describes integrating OMi with Service Manager in the case where the RTSM contained in OMi is used as CMDB.

This section includes:

- ["Data Flow Probe" below](#)
- ["Create User Accounts for the OMi-SM Integration \(RTSM\)" on the next page](#)
- (prerequisite) ["RTSM-Service Manager Integration" on page 73](#)
- ["Enable LW-SSO for the OMi-SM Integration \(RTSM\)" on page 73](#)
- ["View Actual State in SM \(RTSM\)" on page 80](#)
- ["Event Forwarding from OMi to SM \(RTSM\)" on page 81](#)
- ["Downtime Forwarding from Service Manager to OMi \(RTSM\)" on page 98](#)
- ["Sending downtime notifications from OMi to SM \(RTSM\)" on page 104](#)
- ["View Changes and Incidents in OMi \(RTSM\)" on page 106](#)
- ["Business Impact Report \(BIR\) \(RTSM\)" on page 113](#)

Data Flow Probe

The OMi-SM Integration uses a Data Flow Probe to exchange data. This DFP can be installed on one of the OMi Gateway or Data Processing Server systems or on a separate system. HP recommends to install it on an OMi Gateways system as this avoids setting up an additional system.



The Data Flow Probe is necessary for

- Populating the RTSM with CIs & Relationships
- Pushing CIs & Relationships to SM
- Federating Incidents and Changes into RTSM
- Populating the RTSM with downtimes

Create User Accounts for the OMi-SM Integration (RTSM)

The OMi-SM integration requires integration accounts to be set up for the two systems to access each other.

1. In Service Manager, create an operator record with system administration privileges, and give it a descriptive name, like `OMiSMIntegrUser`.

To create a dedicated integration user account in SM:

- a. Log on to SM as a system administrator.
- b. Type **contacts** in the SM command line, and press **ENTER**.
- c. Create a new contact record for the integration user account.
 - i. In the **Full Name** field, type a full name. For example, RTSM.
 - ii. In the **Contact Name** field, type a name. For example, RTSM.
 - iii. Click **Add**, and then **OK**.
- d. Type **operator** in the SM command line, and press **ENTER**.
- e. In the **Login Name** field, type the user name of an existing system administrator account, and click **Search**.

The system administrator account displays.

- f. Create a new user account based on the existing one:
 - i. Change the **Login Name** to the integration account name you want (for example, `rtsm`).
 - ii. Type a **Full Name**. For example, RTSM.
 - iii. In the **Contact ID** field, click the **Fill** button and select the contact record you have just created.
 - iv. Click **Add**.
 - v. Select the **Security** tab, and change the password.
 - vi. Click **OK**.

This is the user account that the OMi server uses to access Service Manager. It is used to forward events, push CIs to, and retrieve incidents and RFCs from Service Manager. Remember the user name and password you specify here, as the OMi system will need them to access the Service Manager target server in later steps.

2. On each OMi server, create a user account with system administration privileges. This account is used by SM to access the OMi system to retrieve the actual state information of a CI. Give it a descriptive name, like `SMOMiIntegrUser`.

Remember the user name and password you specify here, as Service Manager will need the accounts to access the OMi server(s) in later steps.

RTSM-Service Manager Integration

Many of the integration features require that Configuration Items (CIs) exist in both Service Manager and OMi. To enable operators of both systems to see the same CIs, they should be synchronized between the two systems. For details about how to integrate OMi RTSM with Service Manager, see the UCMDB Service Manager Integration Guide in the Service Manager documentation. This integration, which synchronizes important CIs, such as services, business applications and infrastructure CIs, is a prerequisite for all other integration features.

Enable LW-SSO for the OMi-SM Integration (RTSM)

Lightweight Single Sign-On (LW-SSO) is optional but recommended for the 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 OMi-SM workflow.

LW-SSO options for the OMi-SM integration

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 or the Business Impact Report from an OMi incident

The user clicks the **View OMi Event** option or **Launch Business Impact Report** from the incident to view the event details or Business Impact Report.

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.

Required user permissions

In order to be able to view events, a user needs to be assigned a role with sufficient permission to read events. To manage permissions in OMi, select:

Administration > Users > Users, Groups, and Roles

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**.

You can optionally grant the permission to view events not assigned to each user.

When CIs are synchronized between OMi/UCMDB and SM

LW-SSO is NOT needed in this process. Dedicated users are specified in the OMi-UCMDB, UCMDB-SM and OMi-SM integration points.

Configuring LW-SSO for the OMi-SM integration

To use LW-SSO for the SM-OMi integration, LW-SSO must be enable for both products. In SM, you must enable LW-SSO in both the SM server and web tier.

Step 1: Configure LW-SSO in the SM server

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:

- LW-SSO version 2.5 is supported.
- Optionally, you can change attributes `paddingModeName`, `keySize`, `encodingMode`, `engineName`, and `cipherType`. However, you must make sure that they are same with the LW-SSO setting of the other HP product that you want to integrate with Service Manager.
- Do not change the other configurations, such as the content in tag `<restURLs>`, and the attribute of tag `<service>`.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<lwssso-config xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwssso/2.0">
  <enableLWSSO enableLWSSOFramework="true"
    enableCookieCreation="true" cookieCreationType="LWSSO" />
  <web-service>
    <inbound>
      <restURLs>
        <url>.*7/ws.*</url>
        <url>.*sc62server/ws.*</url>
        <url>.*ui.*</url>
      </restURLs>
      <service service-type="rest" >
        <in-lwssso>
          <lwsssoValidation>
            <domain>example.com</domain>
            <crypto cipherType="symmetricBlockCipher" engineName="AES"
              paddingModeName="CBC" keySize="256" encodingMode="Base64Url"
              initString="This is a shared secret passphrase"</crypto>
          </lwsssoValidation>
        </in-lwssso>
      </service>
    </inbound>
    <outbound/>
  </web-service>
</lwssso-config>
```

Step 2: Configure LW-SSO in the SM Web Tier

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.

- 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.lwssso.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, `smintegrationlwssso`. 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"
        authenticationPointServer="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>

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

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

- f. Save the lwsssofmconf.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.

- b. Uncomment bean lwSsoFilter:

```
<bean id="lwSsoFilter"  
class="com.hp.ov.sm.client.webtier.lwssso.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.

Step 3: Configure LW-SSO in OMi

- In OMi:
 - a. Navigate to Authentication Management:
Administration > Users > Authentication Management
 - b. Click the **Configure** button under the **Single Sign-On Configuration** list to open the Single Sign-On Configuration wizard.
 - c. In the **Single Sign-On** dialog, select **Lightweight**.
 - d. Paste the initString you copied above from **JMX to get Token Creation Key (initString)** to the Token Creation String.
 - e. Click **Finish** to save your configuration.

View Actual State in SM (RTSM)

To display the Actual State information in the SM configuration item form, do the following:

1. Log on to SM as a system administrator.
2. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
3. Click the **Active Integrations** tab.
4. Select the **HP Universal CMDB** option.
The form displays the UCMDB web service URL field.
5. In the UCMDB web service URL field, type the URL to the HP Universal CMDB web service API. The URL has the following format:
http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService
6. Specify the credentials for the user you created in "[Create User Accounts for the OMi-SM Integration \(RTSM\)](#)" on page 72 to access the OMi server.
7. Click **Save**. SM displays the message: **Information record updated**.
8. Log out of the SM system.
9. To verify that the setup worked, log back into the SM system with an administrator account. The **Actual State** section will be available in CI records pushed from OMi .

Event Forwarding from OMi to SM (RTSM)

OMi enables you to forward events from OMi to Service Manager, which then become incidents in Service Manager. Subsequent event/incident changes are synchronized between Service Manager and OMi. You can also drill down from OMi events to Service Manager incidents and vice versa.

Follow the steps below to set up an incident exchange between Service Manager and OMi.


This section includes:

- ["Step 1: Configure the Service Manager server as a connected server in OMi" below](#)
- ["Step 2: \(optional\) Configure an Event Forwarding Rule " on page 84](#)
- ["Step 3: Configure the OMi integration in Service Manager" on page 84](#)
- ["Step 4: Configure Launch of Service Manager Incident Details from OMi" on page 89](#)
- ["\(optional\) Step 5: Attribute Synchronization" on page 90](#)
- ["Step 6: Test the Event Forwarding and Cross Launches" on page 94](#)
- ["Advanced Configuration" on page 95](#)

Step 1: Configure the Service Manager server as a connected server in OMi

To synchronize events and event changes between OMi and Service Manager incidents, configure Service Manager as a target connected server in the OMi Connected Servers manager.

To configure the Service Manager server as a target connected server, perform the following steps:

1. Navigate to the Connected Servers manager:
Administration > Setup and Maintenance > Connected Servers
2. Click the **New**  button and select **External Event Processing**. The **Create New Server Connection - External Event Processing** dialog box opens.
3. In the General page, in the **Display Name** field, enter a name for the target Service Manager server. By default, the Name field is filled automatically. For example, if you enter *Service Manager 1* as the Display Name for the target Service Manager server, *Service_Manager_1* is automatically inserted in the Name field. You can specify your own name in the Name field, if you want to change it from the one suggested automatically.

Note: Make a note of the name of the new target server (in this example, *Service_Manager_1*). You need to provide it later as the `username` when configuring the Service Manager server to communicate with the server hosting OMi.

Optional: Enter a description for the new target server.

Make sure that you select the **Active** check box.

Click **Next** to open the Server Properties page.

4. In the **Server Properties** page, select Service Manager System in the mandatory **CI Type** field.

Then, enter the Fully Qualified DNS Name of the Service Manager target server.

Click **Next** to open the Integration Type page.

5. In the **Integration Type** page, complete the following information:
 - a. Select **Call Script Adapter** as the integration type.
 - b. From the **Script Name** menu, select the Service Manager Groovy script adapter **sm:ServiceManagerAdapter**.
 - c. Click **Next** to open the Outgoing Connection page.
6. In the **Outgoing Connection** page, enter the credentials (user name, password, and port number) required to access the Service Manager target server and to forward events to that server:
 - a. In the **User Name** field, enter the user name for the integration user you set up in Service Manager.
 - b. In the **Password** field, enter the password for the user you specified. Repeat the password entry in the **Verify Password** field.
 - c. In the **Port** field, specify the port configured on the Service Manager side for the integration with OMi.

To find the port number to enter:

- If you are using default ports in Service Manager, select or clear **Use Secure HTTP** as appropriate, and then click **Set default port**. The port is set automatically.

Note: If you do not want to use secure HTTP, make sure that the **Use secure HTTP** check box is cleared.

If the Use Secure HTTP check box is selected, download and install a copy of the target server's SSL certificate using the **Retrieve from Server** or **Import from File** link, if the certificate is available in a local file.

- If you need to find the port number, access the following file on your Service Manager system:

```
<HP Service Manager root directory>/HP/Service Manager  
<version>/Server/RUN/sm.cfg
```

In the `sm.cfg` file, check for the `sm -loadBalancer` line and add the port entry at the end of the line. The line looks similar to this:

```
sm -loadBalancer -httpPort:13080
```

Enter the appropriate value of the port used by Service Manager in the **Port** field of the Outgoing Connection page.

- d. Select the **Enable Synchronize and Transfer Control** check box.

If the Enable Synchronize and Transfer Control check box is selected, an OMi operator can transfer ownership of the event to the target connected server using the Transfer Control option in the Event Browser context menu.

If it is not selected, the Synchronize and Transfer Control option is not available from the Event Browser context menu or from the list of forwarding types for configuring forwarding rules.
- e. Test the connection by clicking the **Test Connection** link in the upper center of the dialog box.

A **Success** or **ERROR** hyperlink is displayed. Click the link to get a more detailed message.

- f. Click **Next** to open the **Event Drilldown** page.
7. If you want to drill down into Service Manager, in addition to automatically generating Service Manager incidents from OMi events, you need to specify the fully qualified DNS name and port of the Service Manager system into which you want to perform the incident drill down.

Note: To enable incident drill down to Service Manager, you must install a web tier client for your Service Manager server according to your Service Manager server installation or configuration instructions.

In the **Event Drilldown** page, configure the server where you installed the web tier client along with the configured port used.

If you do not specify a server in the Event Drilldown page, it is assumed that the web tier client is installed on the server used for forwarding events and event changes to SM, and receiving event changes back from Service Manager.

If nothing is configured in the Event Drilldown dialog box, and the web tier client is not installed on the Service Manager server machine, the web browser will not be able to find the requested URL.

Select or clear the **Use Secure HTTP** check box according to your configuration.

Click **Next** to open the Incoming Connection page.

8. To enable event changes to be synchronized back from Service Manager to OMi, you must provide credentials for the Service Manager server to access the server hosting OMi.
 - a. In the Incoming Connection page, select the **Accept event changes from external event processing server** check box, and then enter a password that the Service Manager server requires to connect to the server hosting OMi.

Note: Make a note of this password. You need to provide it later when configuring the Service Manager server to communicate with the server hosting OMi. This password is associated with the user name (*Service_Manager_1*) you configured in Service Manager. If **Enable Synchronize and Transfer Control** was previously selected, the **Accept event changes from external event processing server** option is assumed and cannot be disabled.

- b. Click **Finish**. The target Service Manager server appears in the list of Connected Servers.
9. If you have SM 9.34 or higher, perform the following additional steps:
 - a. Reopen the Service Manager connected server that you configured in the previous steps. To do so, double-click the connected server entry in the connected servers list.
 - b. Copy the ID of the connected server (displayed in the lower right corner of the General tab) and save it. You need to specify this ID as `omi.mgr.id` on the Service Manager system.

An example of a connected server ID is as follows:


ID: 22f42836-fd36-473e-afc9-a81290f4f73b

Step 2: (optional) Configure an Event Forwarding Rule

Once you have configured the Service Manager server as a connected server in OMi, you can forward events manually using **Transfer Control To** from the Context Menu. If you want to automatically forward events, you can configure an Event Forwarding Rule for the OMi server.


1. Open the Event Forwarding manager:

Administration > Event Processing > Automation > Event Forwarding

2. In the **Event Forwarding Rules** pane, click the  **New Item** button to open the **Create New Event Forwarding Rules** dialog box.
3. Enter a display name, and (optional) a description of the event forwarding rule being specified.
4. Select **Active**. A rule must be active in order for its status to be available in Service Manager.
5. Select an event filter for the event forwarding rule from the **Events Filter** list. The filter determines which events to consider for forwarding.

Filters for Event Forwarding Rules can screen events based on the following date-related event attributes which, for example, help you to ignore outdated events:

- o Time Created
- o Time Received
- o Time Lifecycle State Changed

4. If no appropriate filter is already configured, create a new filter as follows:
 - a. Click the  **New Item** button to open the **Filter Configuration** dialog box. You can choose between New Simple Filter or New Advanced Filter.
 - b. In the **Display Name** field, enter a name for the new filter, in this example, FilterCritical. Clear the check boxes for all severity levels except for the severity Critical. Click **OK**.
 - c. You should see your new filter in the Select an Event Filter dialog box (select it, if it is not already highlighted). Click **OK**.
6. Under **Target Servers**, select the target server you configured in the previous step on connecting servers. Click the **Add** button next to the target servers selection field. You can now see the connected server's details. In the **Forwarding Type** field, select the **Synchronize and Transfer Control** forwarding type. Although other selections are technically possible, only Synchronize and Transfer Control is supported by Service Manager.

Step 3: Configure the OMi integration in Service Manager

Service Manager can integrate with more than one OMi server. To configure more than one server, first complete ["Configure the Instance Count in the Service Manager-OMi integration template" on the next page](#) before adding integration instances. To proceed with the default of one server, skip to ["Add an SMOMi integration instance for each OMi server" on the next page](#).

Configure the Instance Count in the Service Manager-OMi integration template

To integrate Service Manager with more than one OMi server, 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 SMOMi integration instance for each OMi server

Once you have completed configuration in OMi, you are ready to add and enable a separate integration instance in Service Manager for each OMi server.

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 OMi server host. For example: my_OMi_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 value is 30 (seconds), and 15 (seconds) is used if this field is empty.

Field	Sample Value	Description
sm.mgr.id	55436DBE-F81E-4799-BA05-65DE9404343B	<p>The Universally Unique Identifier (UUID) automatically generated for this instance of Service Manager.</p> <p>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.</p>
omi.reference.prefix	um:x-hp:2009:opr:	<p>The prefix of the BDM External Process Reference field, which will be present in incoming synchronization requests from the OMi server.</p> <p>Note: This field is automatically completed and has a fixed value. Do not change it.</p>
sm.reference.prefix	um:x-hp:2009:sm:	<p>The prefix of the BDM External Process Reference field, which will be present in outgoing synchronization requests from Service Manager.</p> <p>Note: This field is automatically completed and has a fixed value. Do not change it.</p>
omi.eventdetail.baseurl	http://<servername>/opr-console/opr-evt-details.jsp?eventId=	<p>The basic URL address of the event detail page in OMi. Replace <servername> with the fully qualified domain name of your OMi server.</p>

- 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 OMi. The following table lists the parameters, whose values you can copy from your OMi server.
 To copy the parameter values from OMi, follow these steps:

- a. Log on to OMi 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.
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.

Step 4: Configure Launch of Service Manager Incident Details from 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.

1. Navigate to Connected Servers in OMi:

Administration > Setup and Maintenance > Connected Servers

Click the **Manage Scripts** icon.

2. Select the **sm:ServiceManagerAdapter** script, and click the **Edit Item** button.
3. Click the **Script** tab and locate the following text in the Groovy script:

```
private static final String SM_WEB_TIER_NAME = 'webtier-9.30'
```

4. Change the value of `webtier-9.30` to the value required to access the Service Manager web tier client.

The drill-down URL is made up like this:

```
http://<FQDN of HP Service Manager web tier server>/<web path to HP Service Manager>/<URL query parameters>
```

In this instance, *<FQDN of HP Service Manager web tier server>* is the fully qualified DNS name of the Service Manager server where the web tier client is installed. This part of the URL is added automatically (together with `http://` or `https://`) according to the values that you provided when you configured Service Manager as a target connected server in the Connected Servers manager. The address of the Event Drilldown page of the Connected Server makes up the rest of the URL. For details, see the previous step on connecting servers.

An example of a drill-down URL:

```
http://smsserver.example.com/SM930/index.do?ctx=docEngine&file=probsummary&query=number%3D%22IM10216%22&queryHash=bf52f465
```

In this example, you need to replace `webtier-9.30` with `SM930`. All the other parts of the URL are configured automatically.

5. When finished editing, save the new version of the script. Note that the script can always be reverted to its original version.

For details, see the OMi Administration Guide.

6. If you are using SM 9.34 or lower, set the value of the `querySecurity` parameter from the default value (`true`) to `false` in the SM web tier configuration file `web.xml`.

For more details, see the HP Service Manager online help:

Guides and reference > System Configuration Parameters > Security parameters >

Parameter: `querysecurity`

and

Guides and reference > System Configuration Parameters > Client parameters for Web clients > Web parameter: `querySecurity`

(optional) Step 5: Attribute Synchronization

Attribute Synchronization using Groovy Scripts

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. 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.

Bidirectional Synchronization of Attributes

Individual OMi event attributes can be synchronized from an OMi event to the corresponding SM incident, whenever the event is changed in OMi. Similarly, individual SM incident attributes can be synchronized from an SM incident to the corresponding event in OMi, every time the event is changed in SM. To change the attributes that are synchronized from an OMi event to a corresponding SM incident, change the attributes included in the `SyncOPRPropertiesToSM` list in the Groovy script. To change the attributes that are synchronized from an SM incident to an OMi event, change the attributes included in the `SyncSMPPropertiesToOPR` list in the Groovy script. By default, the `state`, `solution`, and `cause` attributes are synchronized from OMi events to their corresponding SM incidents, and the `incident_status` and `solution` attributes are synchronized from an SM incident to the corresponding OMi event.

To enable synchronization of all attributes in both directions, you can set the `SyncAllAttributes` variable to true. In this case, all other variables will be ignored.

Example:

- `private static final Set SyncOPRPropertiesToSM = ["state", "solution", "cause"]`
- `private static final Set SyncSMPPropertiesToOPR = ["incident_status", "solution"]`

The following table lists the OMi event attributes that can be synchronized with an SM incident, and the matching SM incident attributes that can be synchronized with an OMi event:

OMi event attribute	SM incident attribute
title	name
description	description
state	incident_status
severity	urgency
priority	priority
solution	solution

Unidirectional Synchronization of Attributes

The `assigned_user`, `assigned_group`, and `cause` event properties can be synchronized from an OMi event to a corresponding SM incident. To synchronize these attributes, add them to the `SyncOPRPropertiesToSM` list in the groovy script.

Example:

- ```
private static final Set SyncOPRPropertiesToSM = ["assigned_user", "assigned_group", "cause"]
```

Individual OMi event properties can be synchronized to a corresponding SM incident Activity Log. Updates are not synchronized back from the SM incident Activity Log to the corresponding OMi event. To change the properties that are synchronized, add the desired properties to the `SyncOPRPropertiesToSMActivityLog` list in the Groovy script. By default, the `title`, `description`, `state`, `severity`, `priority`, `annotation`, `duplicate_count`, `cause`, `symptom`, `assigned_user`, and `assigned_group` properties are synchronized.

Example:

- ```
private static final Set SyncOPRPropertiesToSMActivityLog = ["title", "description", "priority"]
```

The following list includes all properties that can be synchronized from OMi events to the SM incident Activity Log:

- `title`
- `description`
- `state`
- `severity`
- `priority`
- `solution`
- `annotation`
- `duplicate_count`
- `assigned_user`
- `assigned_group`
- `cause`
- `symptom`
- `control_transferred_to`
- `time_state_changed`

Custom Mappings for Custom Attributes

You can define your own mappings for custom attributes between OMi and SM. These mapping can be either unidirectional, if the attributes are only contained in one map, or bidirectional, if the attributes are contained in both maps. To create custom mappings for custom attributes, you can edit the `MapSM2OPRCustomAttribute` and `MapOPR2SMCustomAttribute` lists in the Groovy script. These maps are empty by default.

Example:

- `private static final Map <String, String> MapSM2OPRCustomAttribute =
["MySMAttribute" : "MyOMiCustomAttribute"]`
- `private static final Map <String, String> MapOPR2SMCustomAttribute = [
"MyOtherOMiCustomAttribute" : "MyOtherSMAttribute", "MyThirdOMiCA", "activity_
log"]`

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"]`

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:

```
//  
// *BEGIN Configuration: Customization of properties for synchronization*  
//  
...  
...  
//  
// *END Configuration: Customization of properties for synchronization*  
//
```

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.

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

The `ServiceManagerAdapter` Groovy script uses the Apache Wink client to communicate with HP Service Manager. It therefore will throw a `ClientWebException` when there is an HTTP error status returned by HP Service Manager.

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`

Step 6: Test the Event Forwarding and Cross Launches

To test the event forwarding, forward an event manually to SM and then verify that the event is forwarded to SM as expected, and that the cross launches work in both directions.

1. Open an OMi **Event Browser**.
2. Select an event and select **Transfer Control To** in the Context Menu. Select the SM target system.
3. Select the **Forwarding** tab.
4. In the External Id field, you should see a valid SM incident ID after a few seconds.
5. Verify that the incident appears in the Incident Details in HP Service Manager by using the cross launch (see next step).

If the event drill-down connection is not configured, verify the forwarding using 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.
6. Test the cross launch from OMi to SM:
Click the hyperlink created with the incident ID. A browser window opens, which takes you directly to the incident in the Incident Details in HP Service Manager.
 7. Test the cross launch from SM to OMi:

In the Incident Details in HP Service Manager, click **More** and then select **View OMi Event**. A browser window opens, which takes you directly to the event in the Event Browser in OMi.

Note: The **View OMi Event** option displays only when the **omi.mgr.id** parameter in the corresponding SM-OMi integration instance is set correctly.

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 Closed Event Browser.

Advanced Configuration

Configure automatic closure for OMi incidents in SM

Incidents created from OMi events will be automatically closed when the corresponding OMi event is closed. You can also configure SM incidents created from OMi events to 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. <ul style="list-style-type: none"> ■ 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. Click **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 OMiAuto-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: <code>jscall("SMOMi.isAutoCloseAndResolved")</code> . An incident is scheduled for automatic closure when the following conditions are met. <ul style="list-style-type: none"> ■ 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.

Field	Value
Alert Condition	<p>This expression is evaluated when an incident is about to be automatically closed. If it evaluates to true, the incident is closed. Default: <code>jscall("SMOMi.isAutoCloseEnabled")</code>.</p> <p>An incident is closed when the following conditions are met.</p> <ul style="list-style-type: none"> ■ 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	<p>This expression is used to determine how much time will elapse before an incident is automatically closed. Default: <code>\$.alert.time=update.time in \$.file+'7 00:00:00'</code>.</p> <p>The default value means the amount of time elapsed is equal to seven days since the incident was last updated.</p>

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 $.file="incident" and not null(1 in external.process.reference in $.file)`.

Configure SSL for the Incident Exchange integration

When 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>
```

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.

Downtime Forwarding from Service Manager to OMi (RTSM)

You can create downtimes (also known as outages) in OMi based on Requests for Changes (RFCs) in SM. This is done in two steps. First, scheduled downtime CIs are created in OMi based on RFCs in SM. Then, a BSM downtime CI is created based on the scheduled downtime.

You can also send downtime start and end information from OMi to SM to notify operators of when a downtime occurs, especially if the downtime was not driven by an RFC in SM. For more information on this integration, see ["Sending downtime notifications from OMi to SM \(RTSM\)" on page 104](#)

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.
4. The SLA scheduler needs to be started in the **System Status** form.

Step 1: Add an SMBSM_DOWNTIME integration instance in SM

To set up the integration from Service Manager to OMi, you must add an instance of this integration in the Service Manager Integration Suite (SMIS). Note that additional setup is required on the OMi side for integration from OMi to Service Manager.

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 OMi 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	<p>Set this value to <code>true</code>: 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.</p> <p>Set this value to <code>false</code>: The pop-up window is disabled. This operation may cause some unapproved planned downtimes be synchronized to OMi.</p> <p>By default, this value is set to <code>true</code>.</p>
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.

Name	Category	Value	Description
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.

Step 2: Tailor Service Manager to handle phase change

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 the RTSM. The changes or tasks need to be approved again to synchronize with the RTSM 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 OMi.

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.

Step 3: Set up downtime sync jobs in OMi

As part of CI synchronization, you have already set up an integration point between SM and OMi. In this step, you add downtime synchronization jobs, so that scheduled downtime CIs are created in OMi based on Requests for Change in SM.

To add the downtime synchronization jobs:

1. Log in to your OMi system as an administrator.
2. Edit the existing integration point that connects to your Service Manager server.
3. Click **Administration > RTSM Administration > Data Flow Management > Integration Studio**. OMi displays a list of integration points.
4. Select the existing SM integration point. Make sure that CIs have already been synchronized between SM and OMi.
5. Create two integration jobs in the integration point on the **Population** tab:
 - a. Create a new job including the SM **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. Create another new job including the **SM CI Connection Downtime CI** 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 first. You can set the two jobs as schedule-based and set the schedule interval according to your needs.

Note: If no related CIs exist in RTSM 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 RTSM.

Step 4: Set up creation of BSM Downtime CIs

In this step, BSM Downtime CIs are created based on Scheduled Downtime CIs.

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.

To create BSM Downtime CIs:

1. Create a new Integration Point or, if existing, edit the **Scheduled Downtime to BSM Downtime** Integration Point:
 - a. Do the following on your OMi system.
Go to:
Administration > RTSM Administration > Data Flow Management > Integration Studio
 - b. Click **New Integration Point** or **Edit**, enter a name and description of your choice, and select the adapter: **BSM Downtime Adapter**.
 - c. Enter the following information for the adapter: OMi DPS Hostname and port 21212, communication protocol, and the context root (if you have a non-default context root).
 - d. Specify the credentials for the OMi system. The specified user must have administrative rights in the RTSM. Choose generic protocol as protocol.
 - e. Click **OK**, then click the **Save** button above the list of the integration points.
2. 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.

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

Step 5: Verify the SM-OMi downtime synchronization setup

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, choose a CI that has been 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 BSM (RTSM).

External Status values	Description
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.

Task 6. Test if BSM Downtime CIs have been created

1. In OMi, got to **Administration > Service Health > Downtime Management**.
2. Check if a corresponding Downtime was created.

Sending downtime notifications from OMi to SM (RTSM)

OMi can send downtime start and end events to SM to notify operators of when a downtime occurs. This provides additional information to the SM operator in case of a downtime that was not driven by an RFC.

To create downtimes in OMi based on RFCs in SM, see ["Downtime Forwarding from Service Manager to OMi \(RTSM\)" on page 98](#).

Step 1: Send OMi Downtime Events to SM

To enable OMi to send downtime start and end events 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 *the OMi Administration Guide*.

Downtime events use the following formats:

- **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
CloseKeyPattern	<OMi Downtime ID>:<Affected CI ID>:downtime-start
EtiHint	downtime:end
LogOnly	true

View Changes and Incidents in OMi (RTSM)

This integration enables you to view planned changes and incident details in the Changes and Incidents and Hierarchy components in OMi.

This chapter includes the following:

- ["Prerequisite" below](#)
- ["Step 1: Configure the Service Manager Adapter Time Zone" below](#)
- ["Step 2: Create an Integration Point in OMi" on page 108](#)
- ["Step 3: Edit Integration TQLs " on page 109](#)
- ["Step 4: Verify View changes and incidents" on page 110](#)
- ["How to Customize the Changes and Incidents Component" on page 110](#)

Prerequisite

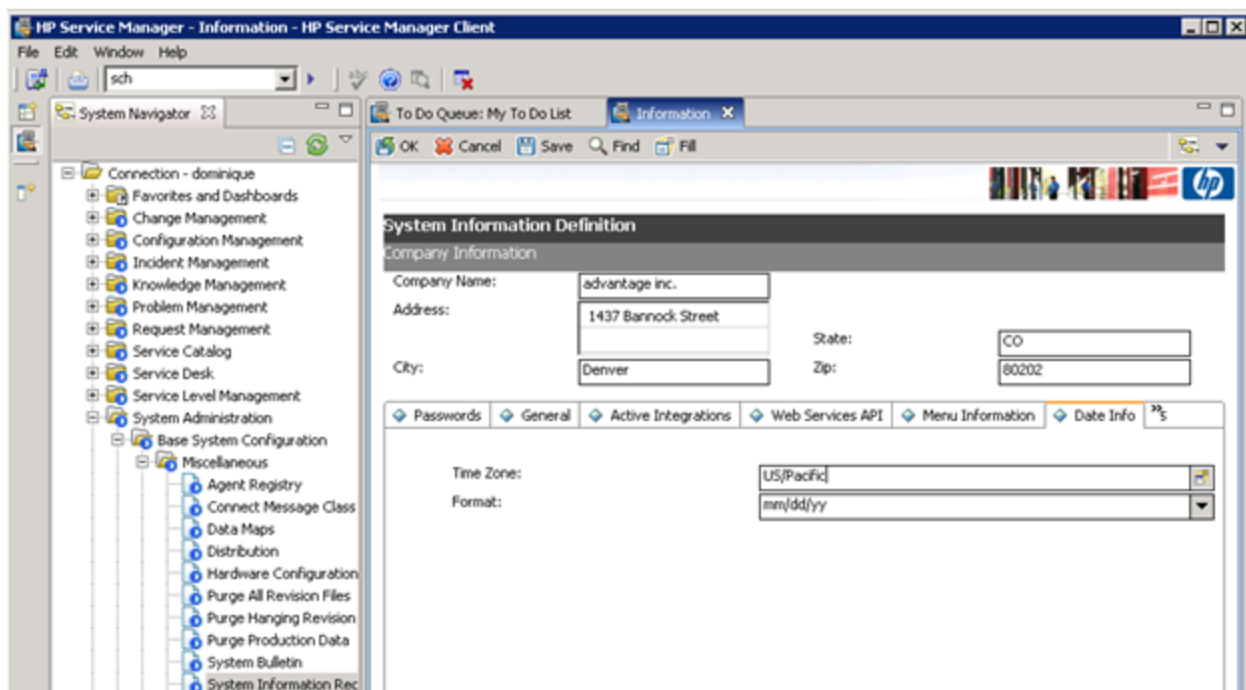
This integration requires that CIs are synchronized between the RTSM and SM. For information on CI synchronization, see ["Operations Manager i-Service Manager Integration Overview" on page 67](#)

This integration requires an administrator user account for OMi to connect to SM. This user account must already exist in both OMi and SM. For details on creating required user accounts, see ["Create User Accounts for the OMi-SM Integration \(RTSM\)" on page 72](#)

Step 1: Configure the Service Manager Adapter Time Zone

Configure the time zone so Incidents and Planned Changes have the correct time definitions:

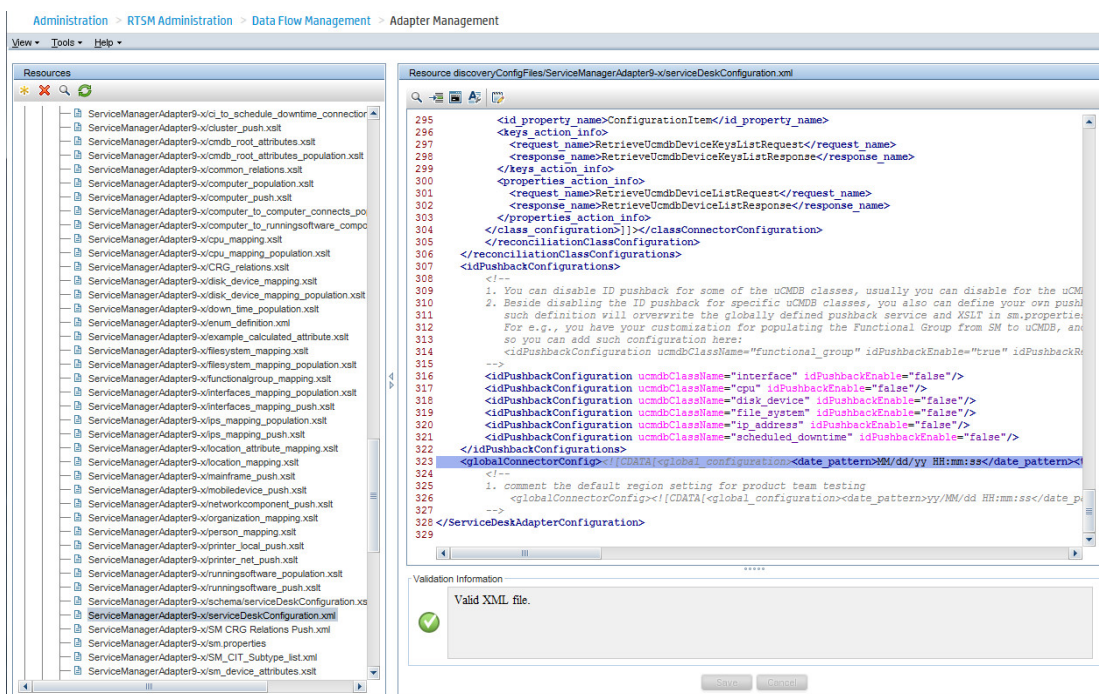
1. In SM, select **Navigation pane > Menu navigation > System Administration > Base System Configuration > Miscellaneous > System Information Record**. Open the **Data Info** tab.
2. In the **Date Info** tab, look up the value for the Timezone.



3. In OMi, select **Administration > RTSM Administration > Data Flow Management > Adapter Management**.
4. In the **Resources** window, open **ServiceManagerAdapter9-x > Configuration Files > ServiceManagerAdapter9-x/serviceDeskConfiguration.xml**

Find the row that includes the following string:

```
<globalConnectorConfig><![CDATA[<global_configuration><date_pattern>MM/dd/yy  
HH:mm:ss</date_pattern><time_zone>US/MOUNTAIN</time_zone>
```



Check the date and time format, as well as a time zone. Note that the date is case-sensitive. Change either SM or the xml file so that they both match each other's settings.

Note: Specify a time zone from the Java time zone list that matches the time zone used in SM (for example, America/New York).

5. If you changed the time zone on SM, restart the SM server; if you changed the time zone on OMi, you do not need to restart the OMi server.)

Step 2: Create an Integration Point in OMi

You edTo create an integration point, follow these steps:

1. In OMi, select **Administration > RTSM Administration > Data Flow Management > Integration Studio**.
2. In the Integration Point pane, select **Create New Integration Point** or choose an existing integration point to edit. The Create New Integration Point dialog box opens. Enter the following:

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

Name	Recommended Value	Description
Adapter	<user defined>	Select HP Software Products > Service Manager > Service Manager 9.xx . This adapter, which supports CI/ relationship Data Push from RTSM to Service Manager, and Population and Federation from Service Manager to RTSM.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the SM server.
Port	<user defined>	The port through which you access SM.
Credentials	<user defined>	Click Generic Protocol , click the Add button to add the integration user account you created in " Create User Accounts for the OMi-SM Integration (RTSM) " on page 72 and then select it.
Probe Name (for ServiceManagerAdapter9-x only)	<user defined>	Select the probe that you installed for this integration.

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

3. In the **Integration Point** pane, click the Integration Point you just created, and click the **Federation** tab in the right pane.
4. In the **Supported and Selected CI Types** area, verify that **Incident** and **RequestForChange** are selected.

Step 3: Edit Integration TQLs

In this step, edit the integration TQLs so that they use the Integration Point created in the previous step.

1. In OMi, select **Administration > RTSM Administration > Modeling > Modeling Studio**.
2. On the **Resources** tab, select Resource Type: Queries. Open the **Console** folder.
3. Open the TQL: `CollectRequestForChangeWithImpacts`.
4. In the **Query Definition** pane, right click one of the objects of CI Type: RequestForChange.
5. From its Context Menu, select **Set Integration Points**. Choose the Integration Point that you configured in the previous step.
6. Repeat steps 4 and 5 for all objects of CI Type: RequestForChange.
7. Open the TQL: `CollectRequestForChangeWithoutImpacts`.
8. Repeat steps 4 and 5 for all objects of CI Type: RequestForChange.

9. Open the TQL: `CollectTicketsWithImpacts`.
10. In the **Query Definition** pane, right click one of the objects of CI Type: Incident.
11. From its Context Menu, select **Set Integration Points**. Choose the Integration Point that you configured in the previous step.
12. Repeat steps 10 and 11 for all objects of CI Type: Incident.
13. Open the TQL: `CollectTicketsWithoutImpacts`.
14. Repeat steps 10 and 11 for all objects of CI Type: Incident.
15. Save all TQLs.

Step 4: Verify View changes and incidents

To verify that you can view changes and incidents in OMi, make sure that you have an incident in SM that is related to a CI in the OMi RTSM. To do so, send a test event related to a CI that has been synchronized between OMi and SM.

1. Send an event, for example, using the following command:

```
submitEvent-t testViewIncidents -rch <hintForExistingCI>
```
2. Select the event in the OMi Event Browser and select **Transfer Control To** in the Context Menu. Select the SM target system.
3. Open the 360° View and select a view containing the related CI.
4. Select the CI, and verify that the **Incident Count** is at least 1. Click **Incidents** to show the Changes in Incidents window, and verify that the incident is displayed in the Incidents section.

By default, the Changes and Incidents component displays data for the previous week. You can change this setting to previous week, day, or hour (up to the current time) using the Configure Component button.

How to Customize the Changes and Incidents Component

By default, incidents and requests for change are displayed for the following CI types: Business Service, Siebel Application, Business Application, and Node. If you want to view change and incident information for other CITs, perform the following procedure:

1. Open the Modeling Studio:
Administration > RTSM Administration > Modeling > Modeling Studio

Copy one of the TQLs within the **Console** folder, and save your copy with a new name. These default TQLs perform the following:

TQL name	Description
<code>CollectTicketsWithImpacts</code>	Retrieves SM incidents for the selected CI, and for its child CIs which have an Impact relationship.
<code>CollectTicketsWithoutImpacts</code>	Retrieves SM incidents for the selected CI.

TQL name	Description
CollectRequestForChangeWithImpacts	Retrieves SM requests for change, for the selected CI, and for its child CIs which have an Impact relationship.
CollectRequestForChangeWithoutImpacts	Retrieves SM requests for change, for the selected CI.

2. Edit the new TQL as needed. You can add CITs as described in ["Naming Constraints for New Request for Change TQLs" below](#).
3. Open Infrastructure Settings:
Administration > Setup and Maintenance > Infrastructure Settings
 - a. Select **Applications**.
 - b. Select **Service Health Application**.
 - c. In the **Service Health Application - Hierarchy (360) properties** area, enter the name of the new TQL you created in the corresponding infrastructure setting.

Note: By default, these infrastructure settings contain the default TQL names. If you enter a TQL name that does not exist, the default value will be used instead.

After you modify the infrastructure setting, the new TQL will be used, and the Changes and Incidents component will show this information for the CITs you defined.

Naming Constraints for New Request for Change TQLs

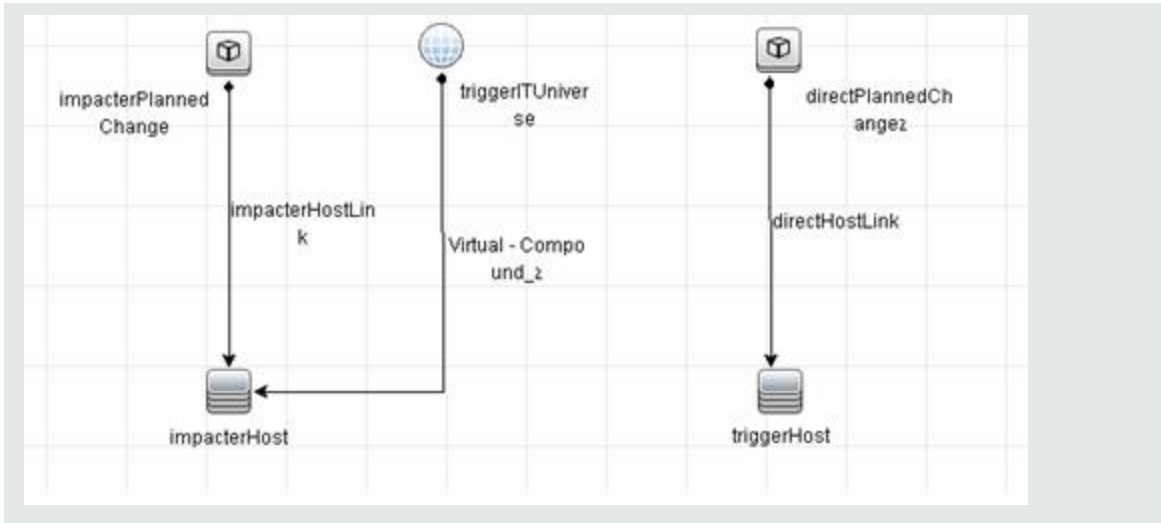
The following naming constraints must be followed in the request for change *without* impact TQL (see the TQL example below, on the right side of the image):

- The request for change CI type must start with **directPlannedChange**.
- The CI type related to the request for change must start with **trigger**.

The following naming constraints must be followed in the request for change *with* impact TQL (see the TQL example below, on the left side of the image):

- **impacterPlannedChange** represents the request for change CI type.
- The CI type related to the request for change must start with **impacter**.
- **trigger!TUniverse** represents the "impacted" child CIs.

Examples of request for change TQLs:



Naming Constraints for New Incident TQLs

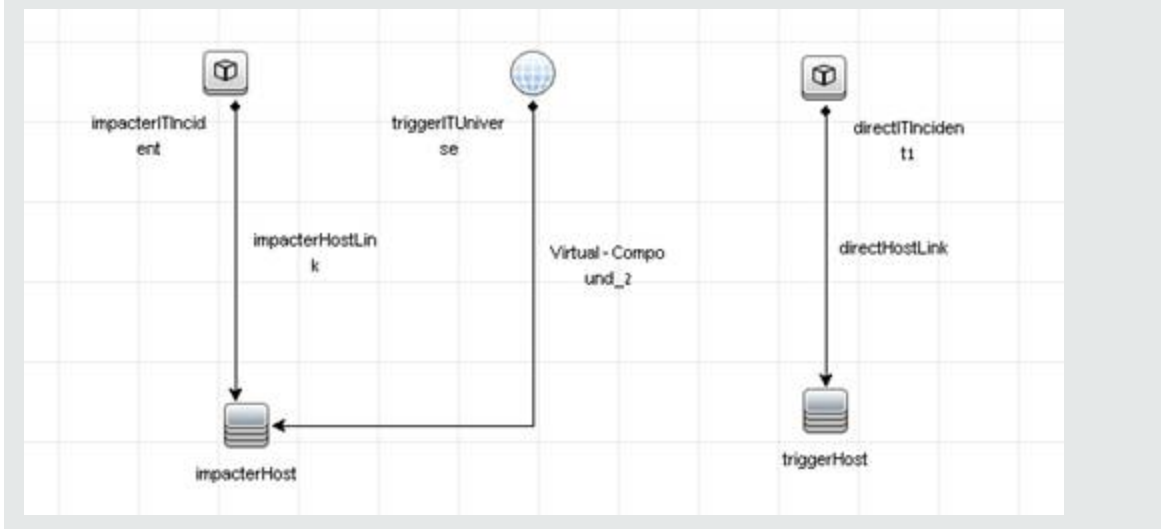
The following naming constraints must be followed in the incidents *without* impact TQL (see the TQL example below, on the right side of the image):

- The incident CI type must start with **directTIncident**.
- The CI type related to the incident must start with **trigger**.

The following naming constraints must be followed in the incidents *with* impact TQL (see the TQL example below, on the left side of the image):

- **impacterTIncident** represents the incident CI type.
- The CI type related to the incident must start with **impacter**.
- **triggerTUUniverse** represents the "impacted" child CIs.

Examples of incident TQLs:



Business Impact Report (BIR) (RTSM)

OMi includes a report that you can use to help evaluate the impact of incidents on your business. 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.

Note:

- This integration requires that CIs are synchronized between both Service Manager and OMi.
- Only one instance of this integration is allowed.

Step 1: Add a Business Impact Report Integration in SM

To use the Service Manager to BIR integration, you must add and enable an instance of this integration in Integration Manager.

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.

Field	Value
Endpoint Server	The name of the OMi 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 OMi 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.

Step 2: Launch a Business Impact Report from an Incident

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**. The OMi Business Impact window opens, showing the KPI over time data for the related CI and related business services.

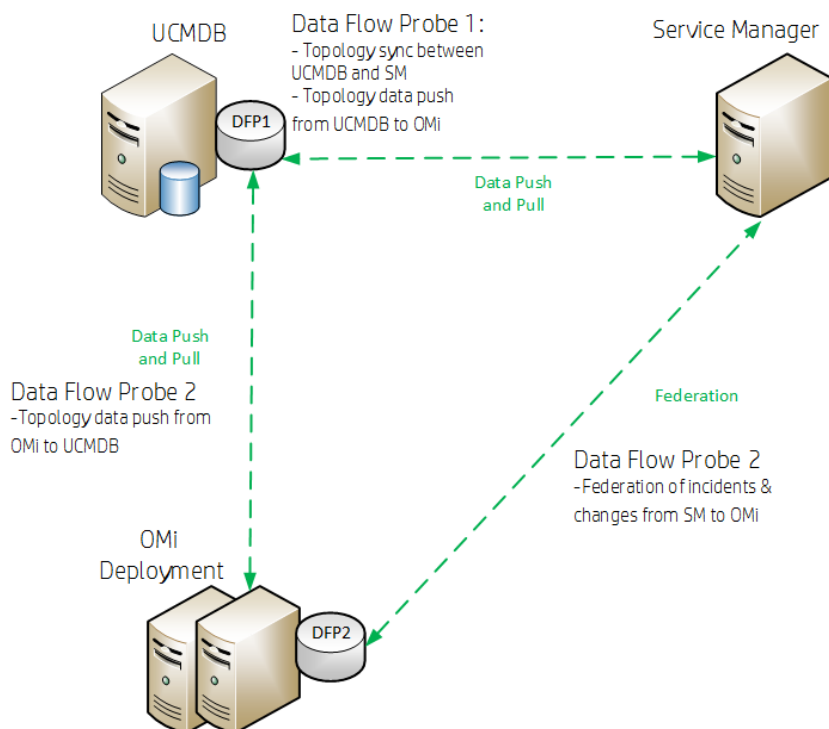
Chapter 22: OMi-SM Integration with UCMDB

This section describes the integration of Service Manager with OMi in the case of an external UCMDB.

This section includes:

- "Data Flow Probes" below
- "Create User Accounts for the OMi-SM Integration (UCMDB)" on the next page
- "UCMDB-Service Manager Integration" on page 117 (prerequisite for all other integration options)
- "OMi-UCMDB Integration" on page 117 (prerequisite for all other integration options)
- "Enable LW-SSO for the OMi-SM Integration (UCMDB)" on page 117
- "View Actual State in SM (UCMDB)" on page 125
- "Event Forwarding from OMi to SM (UCMDB)" on page 125
- "Downtime Forwarding from Service Manager to OMi (UCMDB)" on page 143
- "Sending downtime notifications from OMi to SM (UCMDB)" on page 149
- "View Changes and Incidents in OMi (UCMDB)" on page 151
- "Business Impact Report (BIR) (UCMDB)" on page 158

Data Flow Probes



The DFP1 is necessary for

- Topology synchronization (CIs) between UCMDB and OMi
- Topology synchronization (CIs) between UCMDB and Service Manager

DFP2 is necessary for

- Topology data push from OMi to UCMDB
- Federation of incidents and changes from SM into OMi

Figure: Setup OMi with a UCMDB and two Data Flow Probes

Create User Accounts for the OMi-SM Integration (UCMDB)

The OMi-SM integration requires integration accounts to be set up for the three systems to access each other.

1. In Service Manager, create an operator record with system administration privileges, and give it a descriptive name, like UCMDBSMIntegrUser.

To create a dedicated integration user account in SM:

- a. Log on to SM as a system administrator.
- b. Type **contacts** in the SM command line, and press **ENTER**.
- c. Create a new contact record for the integration user account.
 - i. In the **Full Name** field, type a full name. For example, UCMDB.
 - ii. In the **Contact Name** field, type a name. For example, UCMDB.
 - iii. Click **Add**, and then **OK**.
- d. Type **operator** in the SM command line, and press **ENTER**.
- e. In the **Login Name** field, type the user name of an existing system administrator account, and click **Search**.

The system administrator account displays.

- f. Create a new user account based on the existing one:
 - i. Change the **Login Name** to the integration account name you want (for example, UCMDB).
 - ii. Type a **Full Name**. For example, RTSM.
 - iii. In the **Contact ID** field, click the **Fill** button and select the contact record you have just created.
 - iv. Click **Add**.
 - v. Select the **Security** tab, and change the password.
 - vi. Click **OK**.

This is the user account that the OMi server uses to access Service Manager. It is used to forward events and retrieve incidents and RFCs from Service Manager. Remember the user name and password you specify here, as the UCMDB system will need them to access the Service Manager target server in later steps.

2. On each OMi server, create a user account with system administration privileges. This account is used by SM to access the OMi system to retrieve the actual state information of a CI. Give it a descriptive name, like `SMOMiIntegrUser`.

Remember the user name and password you specify here, as Service Manager will need the accounts to access the OMi server(s) in later steps.

3. In OMi, create a user account with the system administration privileges for the UCMDB-OMi integration. Give it a descriptive name, like `UCMDBOMiIntegrUser`. Remember the user name and password you specify here, as the UCMDB system will need the account details to access the OMi server in later steps.
4. In UCMDB, create a user account with system administration privileges for the OMi-UCMDB integration. Give it a descriptive name, like `OMiUCMDBIntegrUser`. Remember the user name and password you specify here, as OMi will need the account details to access the UCMDB server in later steps.
5. In UCMDB, create a user account with system administration privileges for the SM-UCMDB integration. Give it a descriptive name, like `SMUCMDBIntegrUser`. Remember the user name and password you specify here, as SM will need the account to access the UCMDB server in later steps.

UCMDB-Service Manager Integration

For details about how to integrate UCMDB with Service Manager, see the UCMDB Service Manager Integration Guide. This integration, and the OMi-UCMDB integration, which synchronize important CIs, such as services, business applications and infrastructure CIs, are prerequisites for all other integration features.

OMi-UCMDB Integration

For details about how to integrate UCMDB with OMi, see the UCMDB online help (**Data Flow Management**> **Integrations**> **Integrating Multiple CMDBs**) and the RTSM Best Practices Guide.

Enable LW-SSO for the OMi-SM Integration (UCMDB)

Lightweight Single Sign-On (LW-SSO) is optional but recommended for the 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 OMi-SM workflow.

LW-SSO options for the OMi-SM integration

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 or the Business Impact Report from an OMi incident

The user clicks the **View OMi Event** option or **Launch Business Impact Report** from the incident to view the event details or Business Impact Report.

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.

Required user permissions

In order to be able to view events, a user needs to be assigned a role with sufficient permission to read events. To manage permissions in OMi, select:

Administration > Users > Users, Groups, and Roles

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**.

You can optionally grant the permission to view events not assigned to each user.

When CIs are synchronized between OMi/UCMDB and SM

LW-SSO is NOT needed in this process. Dedicated users are specified in the OMi-UCMDB, UCMDB-SM and OMi-SM integration points.

Configuring LW-SSO for the OMi-SM integration

To use LW-SSO for the SM-OMi integration, LW-SSO must be enable for both products. In SM, you must enable LW-SSO in both the SM server and web tier.

Step 1: Configure LW-SSO in the SM server

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:

- LW-SSO version 2.5 is supported.
- Optionally, you can change attributes `paddingModeName`, `keySize`, `encodingMode`, `engineName`, and `cipherType`. However, you must make sure that they are same with the LW-SSO setting of the other HP product that you want to integrate with Service Manager.
- Do not change the other configurations, such as the content in tag `<restURLs>`, and the attribute of tag `<service>`.

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>
```

Step 2: Configure LW-SSO in the SM Web Tier

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.

- 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.lwssso.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, `smintegrationlwssso`. 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"?>  
<lwso-config  
  xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwso/2.0">  
  <enableLWSSO  
    enableLWSSOFramework="true"  
    enableCookieCreation="true"  
    cookieCreationType="LWSSO"/>  
  
  <webui>  
    <validation>  
      <in-ui-lwso>  
        <lwsoValidation id="ID000001">  
          <domain>example.com</domain>  
          <crypto cipherType="symmetricBlockCipher"  
            engineName="AES" paddingModeName="CBC" keySize="256"
```

```
        encodingMode="Base64Url"
        initString="This is a shared secret passphrase"/>
    </lwsoValidation>
</in-ui-lwso>

<validationPoint
    enabled="false"
    refid="ID000001"
    authenticationPointServer="http://server1.example.com:8080/bsf"/>
</validation>

<creation>
    <lwsoCreationRef useHTTPOnly="true" secureHTTPCookie="true">
        <lwsoValidationRef refid="ID000001"/>
        <expirationPeriod>50</expirationPeriod>
    </lwsoCreationRef>
</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>

<lwso-plugin type="Acegi">
    <roleIntegration
```

```
        rolePrefix="ROLE_"
        fromLWSSO2Plugin="external"
        fromPlugin2LWSSO="enabled"
        caseConversion="upperCase"/>

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

- f. Save the lwsssofmconf.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.

- b. Uncomment bean lwSsoFilter:

```
<bean id="lwSsoFilter"
class="com.hp.ov.sm.client.webtier.lwssso.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.

Step 3: Configure LW-SSO in OMi

- In OMi:
 - a. Navigate to Authentication Management:
Administration > Users > Authentication Management
 - b. Click the **Configure** button under the **Single Sign-On Configuration** list to open the Single Sign-On Configuration wizard.
 - c. In the **Single Sign-On** dialog, select **Lightweight**.
 - d. Paste the initString you copied above from **JMX to get Token Creation Key (initString)** to the

Token Creation String.

- e. Click **Finish** to save your configuration.

View Actual State in SM (UCMDB)

To display the Actual State information in the SM configuration item form, do the following:

1. Log on to SM as a system administrator.
2. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
3. Click the **Active Integrations** tab.
4. Select the **HP Universal CMDB** option.
The form displays the UCMDB web service URL field.
5. In the UCMDB web service URL field, type the URL to the HP Universal CMDB web service API. The URL has the following format:
http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService
6. Specify the credentials for the user you created in ["Create User Accounts for the OMi-SM Integration \(UCMDB\)" on page 116](#) to access the UCMDB server.
Replace <UCMDB server name> with the host name of your UCMDB server, and replace <port> with the port used by your UCMDB server web service.
7. Click **Save**. SM displays the message: **Information record updated**.
8. Log out of the SM system.
9. To verify that the setup worked, log back into the SM system with an administrator account. The **Actual State** section will be available in CI records pushed from UCMDB.

Event Forwarding from OMi to SM (UCMDB)

OMi enables you to forward events from OMi to Service Manager, which then become incidents in Service Manager. Subsequent event/incident changes are synchronized between Service Manager and OMi. You can also drill down from OMi events to Service Manager incidents and vice versa.

Follow the steps below to set up an incident exchange between Service Manager and OMi.


This section includes:

- ["Step 1: Configure the Service Manager server as a connected server in OMi" on the next page](#)
- ["Step 2: \(optional\) Configure an Event Forwarding Rule " on page 128](#)
- ["Step 3: Configure the OMi integration in Service Manager" on page 129](#)
- ["Step 4: Configure Launch of Service Manager Incident Details from OMi" on page 133](#)
- ["\(optional\) Step 5: Attribute Synchronization" on page 134](#)
- ["Step 6: Test the Event Forwarding and Cross Launches" on page 139](#)
- ["Advanced Configuration" on page 140](#)

Step 1: Configure the Service Manager server as a connected server in OMi

To synchronize events and event changes between OMi and Service Manager incidents, configure Service Manager as a target connected server in the OMi Connected Servers manager.

To configure the Service Manager server as a target connected server, perform the following steps:

1. Navigate to the Connected Servers manager:
Administration > Setup and Maintenance > Connected Servers
2. Click the **New**  button and select **External Event Processing**. The **Create New Server Connection - External Event Processing** dialog box opens.
3. In the General page, in the **Display Name** field, enter a name for the target Service Manager server. By default, the Name field is filled automatically. For example, if you enter *Service Manager 1* as the Display Name for the target Service Manager server, *Service_Manager_1* is automatically inserted in the Name field. You can specify your own name in the Name field, if you want to change it from the one suggested automatically.

Note: Make a note of the name of the new target server (in this example, *Service_Manager_1*). You need to provide it later as the `username` when configuring the Service Manager server to communicate with the server hosting OMi.

Optional: Enter a description for the new target server.

Make sure that you select the **Active** check box.

Click **Next** to open the Server Properties page.

4. In the **Server Properties** page, select Service Manager System in the mandatory **CI Type** field. Then, enter the Fully Qualified DNS Name of the Service Manager target server.

Click **Next** to open the Integration Type page.

5. In the **Integration Type** page, complete the following information:
 - a. Select **Call Script Adapter** as the integration type.
 - b. From the **Script Name** menu, select the Service Manager Groovy script adapter **sm:ServiceManagerAdapter**.
 - c. Click **Next** to open the Outgoing Connection page.
6. In the **Outgoing Connection** page, enter the credentials (user name, password, and port number) required to access the Service Manager target server and to forward events to that server:
 - a. In the **User Name** field, enter the user name for the integration user you set up in Service Manager.
 - b. In the **Password** field, enter the password for the user you specified. Repeat the password entry in the **Verify Password** field.
 - c. In the **Port** field, specify the port configured on the Service Manager side for the integration with OMi.

To find the port number to enter:

- If you are using default ports in Service Manager, select or clear **Use Secure HTTP** as appropriate, and then click **Set default port**. The port is set automatically.

Note: If you do not want to use secure HTTP, make sure that the **Use secure HTTP** check box is cleared.

If the Use Secure HTTP check box is selected, download and install a copy of the target server's SSL certificate using the **Retrieve from Server** or **Import from File** link, if the certificate is available in a local file.

- If you need to find the port number, access the following file on your Service Manager system:

```
<HP Service Manager root directory>/HP/Service Manager  
<version>/Server/RUN/sm.cfg
```

In the `sm.cfg` file, check for the `sm -loadBalancer` line and add the port entry at the end of the line. The line looks similar to this:

```
sm -loadBalancer -httpPort:13080
```

Enter the appropriate value of the port used by Service Manager in the **Port** field of the Outgoing Connection page.

- d. Select the **Enable Synchronize and Transfer Control** check box.
If the Enable Synchronize and Transfer Control check box is selected, an OMi operator can transfer ownership of the event to the target connected server using the Transfer Control option in the Event Browser context menu.
If it is not selected, the Synchronize and Transfer Control option is not available from the Event Browser context menu or from the list of forwarding types for configuring forwarding rules.
 - e. Test the connection by clicking the **Test Connection** link in the upper center of the dialog box. A **Success** or **ERROR** hyperlink is displayed. Click the link to get a more detailed message.
 - f. Click **Next** to open the **Event Drilldown** page.
7. If you want to drill down into Service Manager, in addition to automatically generating Service Manager incidents from OMi events, you need to specify the fully qualified DNS name and port of the Service Manager system into which you want to perform the incident drill down.

Note: To enable incident drill down to Service Manager, you must install a web tier client for your Service Manager server according to your Service Manager server installation or configuration instructions.

In the **Event Drilldown** page, configure the server where you installed the web tier client along with the configured port used.

If you do not specify a server in the Event Drilldown page, it is assumed that the web tier client is installed on the server used for forwarding events and event changes to SM, and receiving event changes back from Service Manager.

If nothing is configured in the Event Drilldown dialog box, and the web tier client is not installed on the Service Manager server machine, the web browser will not be able to find the requested URL.

Select or clear the **Use Secure HTTP** check box according to your configuration.

Click **Next** to open the Incoming Connection page.

8. To enable event changes to be synchronized back from Service Manager to OMi, you must provide credentials for the Service Manager server to access the server hosting OMi.
 - a. In the Incoming Connection page, select the **Accept event changes from external event processing server** check box, and then enter a password that the Service Manager server requires to connect to the server hosting OMi.

Note: Make a note of this password. You need to provide it later when configuring the Service Manager server to communicate with the server hosting OMi. This password is associated with the user name (*Service_Manager_1*) you configured in Service Manager. If **Enable Synchronize and Transfer Control** was previously selected, the **Accept event changes from external event processing server** option is assumed and cannot be disabled.


- b. Click **Finish**. The target Service Manager server appears in the list of Connected Servers.
9. If you have SM 9.34 or higher, perform the following additional steps:
 - a. Reopen the Service Manager connected server that you configured in the previous steps. To do so, double-click the connected server entry in the connected servers list.
 - b. Copy the ID of the connected server (displayed in the lower right corner of the General tab) and save it. You need to specify this ID as `omi.mgr.id` on the Service Manager system.

An example of a connected server ID is as follows:

ID: 22f42836-fd36-473e-afc9-a81290f4f73b


Step 2: (optional) Configure an Event Forwarding Rule

Once you have configured the Service Manager server as a connected server in OMi, you can forward events manually using **Transfer Control To** from the Context Menu. If you want to automatically forward events, you can configure an Event Forwarding Rule for the OMi server.

1. Open the Event Forwarding manager:
Administration > Event Processing > Automation > Event Forwarding
2. In the **Event Forwarding Rules** pane, click the  **New Item** button to open the **Create New Event Forwarding Rules** dialog box.
3. Enter a display name, and (optional) a description of the event forwarding rule being specified.
4. Select **Active**. A rule must be active in order for its status to be available in Service Manager.
5. Select an event filter for the event forwarding rule from the **Events Filter** list. The filter determines which events to consider for forwarding.

Filters for Event Forwarding Rules can screen events based on the following date-related event attributes which, for example, help you to ignore outdated events:

- o Time Created
- o Time Received

- Time Lifecycle State Changed
4. If no appropriate filter is already configured, create a new filter as follows:
 - a. Click the  **New Item** button to open the **Filter Configuration** dialog box. You can choose between New Simple Filter or New Advanced Filter.
 - b. In the **Display Name** field, enter a name for the new filter, in this example, FilterCritical. Clear the check boxes for all severity levels except for the severity Critical. Click **OK**.
 - c. You should see your new filter in the Select an Event Filter dialog box (select it, if it is not already highlighted). Click **OK**.
 6. Under **Target Servers**, select the target server you configured in the previous step on connecting servers. Click the **Add** button next to the target servers selection field. You can now see the connected server's details. In the **Forwarding Type** field, select the **Synchronize and Transfer Control** forwarding type. Although other selections are technically possible, only Synchronize and Transfer Control is supported by Service Manager.

Step 3: Configure the OMi integration in Service Manager

Service Manager can integrate with more than one OMi server. To configure more than one server, first complete "[Configure the Instance Count in the Service Manager-OMi integration template](#)" below before adding integration instances. To proceed with the default of one server, skip to "[Add an SMOMi integration instance for each OMi server](#)" below.

Configure the Instance Count in the Service Manager-OMi integration template

To integrate Service Manager with more than one OMi server, 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 SMOMi integration instance for each OMi server

Once you have completed configuration in OMi, you are ready to add and enable a separate integration instance in Service Manager for each OMi server.

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 OMi server host. For example: my_OMi_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	<p>The HTTP connection timeout setting in seconds.</p> <p>Note: The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.</p>
http.rec.timeout	30	<p>The HTTP receive timeout setting in seconds.</p> <p>Note: The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.</p>
http.send.timeout	30	<p>The HTTP send timeout setting in seconds.</p> <p>Note: The out-of-box value is 30 (seconds), and 15 (seconds) is used if this field is empty.</p>
sm.mgr.id	55436DBE-F81E-4799-BA05-65DE9404343B	<p>The Universally Unique Identifier (UUID) automatically generated for this instance of Service Manager.</p> <p>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.</p>

Field	Sample Value	Description
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 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 OMi. The following table lists the parameters, whose values you can copy from your OMi server.

To copy the parameter values from OMi, follow these steps:

- a. Log on to OMi 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.
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.

- 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.

- Enable the integration instance.
- If you have multiple OMi servers, repeat the steps above for the rest of your OMi servers.

Step 4: Configure Launch of Service Manager Incident Details from 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.

1. Navigate to Connected Servers in OMi:
Administration > Setup and Maintenance > Connected Servers
Click the **Manage Scripts** icon.
2. Select the **sm:ServiceManagerAdapter** script, and click the **Edit Item** button.
3. Click the **Script** tab and locate the following text in the Groovy script:

```
private static final String SM_WEB_TIER_NAME = 'webtier-9.30'
```
4. Change the value of `webtier-9.30` to the value required to access the Service Manager web tier client.

The drill-down URL is made up like this:

```
http://<FQDN of HP Service Manager web tier server>/<web path to HP Service Manager>/<URL query parameters>
```

In this instance, `<FQDN of HP Service Manager web tier server>` is the fully qualified DNS name of the Service Manager server where the web tier client is installed. This part of the URL is added automatically (together with `http://` or `https://`) according to the values that you provided when you configured Service Manager as a target connected server in the Connected Servers manager. The address of the Event Drilldown page of the Connected Server makes up the rest of the URL. For details, see the previous step on connecting servers.

An example of a drill-down URL:

```
http://smsserver.example.com/SM930/index.do?ctx=docEngine&file=probsummary&query=number%3D%22IM10216%22&queryHash=bf52f465
```

In this example, you need to replace `webtier-9.30` with `SM930`. All the other parts of the URL are configured automatically.

5. When finished editing, save the new version of the script. Note that the script can always be reverted to its original version.
For details, see the OMi Administration Guide.
6. If you are using SM 9.34 or lower, set the value of the `querySecurity` parameter from the default value (`true`) to `false` in the SM web tier configuration file `web.xml`.

For more details, see the HP Service Manager online help:

Guides and reference > System Configuration Parameters > Security parameters >

Parameter: `querysecurity`

and

Guides and reference > System Configuration Parameters > Client parameters for Web clients > Web parameter: `querySecurity`

(optional) Step 5: Attribute Synchronization

Attribute Synchronization using Groovy Scripts

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. 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.

Bidirectional Synchronization of Attributes

Individual OMi event attributes can be synchronized from an OMi event to the corresponding SM incident, whenever the event is changed in OMi. Similarly, individual SM incident attributes can be synchronized from an SM incident to the corresponding event in OMi, every time the event is changed in SM. To change the attributes that are synchronized from an OMi event to a corresponding SM incident, change the attributes included in the `SyncOPRPropertiesToSM` list in the Groovy script. To change the attributes that are synchronized from an SM incident to an OMi event, change the attributes included in the `SyncSMPPropertiesToOPR` list in the Groovy script. By default, the `state`, `solution`, and `cause` attributes are synchronized from OMi events to their corresponding SM incidents, and the `incident_status` and `solution` attributes are synchronized from an SM incident to the corresponding OMi event.

To enable synchronization of all attributes in both directions, you can set the `SyncAllAttributes` variable to `true`. In this case, all other variables will be ignored.

Example:

- `private static final Set SyncOPRPropertiesToSM = ["state", "solution", "cause"]`
- `private static final Set SyncSMPPropertiesToOPR = ["incident_status", "solution"]`

The following table lists the OMi event attributes that can be synchronized with an SM incident, and the matching SM incident attributes that can be synchronized with an OMi event:

OMi event attribute	SM incident attribute
title	name
description	description
state	incident_status
severity	urgency
priority	priority
solution	solution

Unidirectional Synchronization of Attributes

The `assigned_user`, `assigned_group`, and `cause` event properties can be synchronized from an OMi event to a corresponding SM incident. To synchronize these attributes, add them to the `SyncOPRPropertiesToSM` list in the groovy script.

Example:

- `private static final Set SyncOPRPropertiesToSM = ["assigned_user", "assigned_group", "cause"]`

Individual OMi event properties can be synchronized to a corresponding SM incident Activity Log. Updates are not synchronized back from the SM incident Activity Log to the corresponding OMi event. To change the properties that are synchronized, add the desired properties to the `SyncOPRPropertiesToSMActivityLog` list in the Groovy script. By default, the `title`, `description`, `state`, `severity`, `priority`, `annotation`, `duplicate_count`, `cause`, `symptom`, `assigned_user`, and `assigned_group` properties are synchronized.

Example:

- ```
private static final Set SyncOPRPropertiesToSMActivityLog = ["title",
"description", "priority"]
```

The following list includes all properties that can be synchronized from OMi events to the SM incident Activity Log:

- `title`
- `description`
- `state`
- `severity`
- `priority`
- `solution`
- `annotation`
- `duplicate_count`
- `assigned_user`
- `assigned_group`
- `cause`
- `symptom`
- `control_transferred_to`
- `time_state_changed`

### Custom Mappings for Custom Attributes

You can define your own mappings for custom attributes between OMi and SM. These mappings can be either unidirectional, if the attributes are only contained in one map, or bidirectional, if the attributes are contained in both maps. To create custom mappings for custom attributes, you can edit the `MapSM2OPRCustomAttribute` and `MapOPR2SMCustomAttribute` lists in the Groovy script. These maps are empty by default.

Example:

- ```
private static final Map <String, String> MapSM2OPRCustomAttribute =  
["MySMAttribute" : "MyOMiCustomAttribute"]
```
- ```
private static final Map <String, String> MapOPR2SMCustomAttribute = [
"MyOtherOMiCustomAttribute" : "MyOtherSMAttribute", "MyThirdOMiCA", "activity_
log"]
```



## 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"]
```

## 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:

```
//
// *BEGIN Configuration: Customization of properties for synchronization*
//
...
...
//
// *END Configuration: Customization of properties for synchronization*
//
```

**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.

### 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

The `ServiceManagerAdapter` Groovy script uses the Apache Wink client to communicate with HP Service Manager. It therefore will throw a `ClientWebException` when there is an HTTP error status returned by HP Service Manager.

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
```

## Step 6: Test the Event Forwarding and Cross Launches

To test the event forwarding, forward an event manually to SM and then verify that the event is forwarded to SM as expected, and that the cross launches work in both directions.

1. Open an OMi **Event Browser**.
2. Select an event and select **Transfer Control To** in the Context Menu. Select the SM target system.
3. Select the **Forwarding** tab.
4. In the External Id field, you should see a valid SM incident ID after a few seconds.
5. Verify that the incident appears in the Incident Details in HP Service Manager by using the cross launch (see next step).

If the event drill-down connection is not configured, verify the forwarding using 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.
6. Test the cross launch from OMi to SM:  
Click the hyperlink created with the incident ID. A browser window opens, which takes you directly to the incident in the Incident Details in HP Service Manager.
  7. Test the cross launch from SM to OMi:

In the Incident Details in HP Service Manager, click **More** and then select **View OMi Event**. A browser window opens, which takes you directly to the event in the Event Browser in OMi.

**Note:** The **View OMi Event** option displays only when the `omi.mgr.id` parameter in the corresponding SM-OMi integration instance is set correctly.

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 Closed Event Browser.

## Advanced Configuration

Configure automatic closure for OMi incidents in SM

Incidents created from OMi events will be automatically closed when the corresponding OMi event is closed. You can also configure SM incidents created from OMi events to 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. <ul style="list-style-type: none"> <li>■ If this option is not selected, no incidents will be automatically closed.</li> <li>■ If this option is selected, incidents will be automatically closed under specified conditions.</li> </ul> Default: Not selected |
| Closure Code                  | This value will be copied to the <b>Closure Code</b> field of incidents when they are automatically closed.<br>Default: Automatically Closed                                                                                                                                                                                                               |
| Solution                      | This description will be appended to the end of the <b>Solution</b> field of incidents when they are automatically closed.<br>Default: This incident which belongs to OMi has been closed automatically.                                                                                                                                                   |

- c. Click **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 OMiAuto-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 | <p>This expression is used to determine if an incident should be scheduled for automatic closure.<br/>                     Default: <code>jscall("SMOMi.isAutoCloseAndResolved")</code>.</p> <p>An incident is scheduled for automatic closure when the following conditions are met.</p> <ul style="list-style-type: none"> <li>■ The <b>Close Incident Automatically?</b> option in the Incident Management Environment record is selected.</li> <li>■ In the incident record, the <b>Do not close this incident automatically</b> option is not selected.</li> <li>■ The incident has a status of <b>Resolved</b>.</li> </ul> |
| Alert Condition    | <p>This expression is evaluated when an incident is about to be automatically closed. If it evaluates to true, the incident is closed.<br/>                     Default: <code>jscall("SMOMi.isAutoCloseEnabled")</code>.</p> <p>An incident is closed when the following conditions are met.</p> <ul style="list-style-type: none"> <li>■ The <b>Close Incident Automatically?</b> option in the Incident Management Environment record is selected.</li> <li>■ In the incident record, the <b>Do not close this incident automatically</b> option is not selected.</li> </ul>                                                  |

| Field           | Value                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Calc Expression | <p>This expression is used to determine how much time will elapse before an incident is automatically closed.</p> <p>Default: <code>\$L.alert.time=update.time in \$L.file+'7 00:00:00'</code>.</p> <p>The default value means the amount of time elapsed is equal to seven days since the incident was last updated.</p> |

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)`.

### Configure SSL for the Incident Exchange integration

When 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>
```

**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.

## Downtime Forwarding from Service Manager to OMi (UCMDB)

You can create downtimes (also known as outages) in OMi based on Requests for Changes (RFCs) in SM. This is done in two steps. First, scheduled downtime CIs are created in the UCMDB based on RFCs in SM. Then, a BSM downtime CI is created in OMi based on the scheduled downtime.

You can also send downtime start and end information from OMi to SM to notify operators of when a downtime occurs, especially if the downtime was not driven by an RFC in SM. For more information on this integration, see ["Sending downtime notifications from OMi to SM \(UCMDB\)" on page 149](#)

### 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.
4. The SLA scheduler needs to be started in the **System Status** form.

## Step 1: Add an SMBSM\_DOWNTIME integration instance in SM

To set up the integration from Service Manager to OMi, you must add an instance of this integration in the Service Manager Integration Suite (SMIS). Note that additional setup is required on the OMi side for integration from OMi to Service Manager.

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:
  - o Modify the **Name** and **Version** fields to the exact values you need.
  - o 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.
  - o 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 OMi 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                           | <p>Set this value to <code>true</code>: 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.</p> <p>Set this value to <code>false</code>: The pop-up window is disabled. This operation may cause some unapproved planned downtimes be synchronized to OMi.</p> <p>By default, this value is set to <code>true</code>.</p> |
| 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.                                                                                                                                                                                                                                                                                                                                          |
| sm.host                                                 | General  | <sm server name >                    | <p>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.</p> <p><b>Note:</b> Do not include a colon in this field. Otherwise, the logic will be broken.</p>                                                                                                                                                                           |



| Name                | Category | Value            | Description                                                                                                                                                     |
|---------------------|----------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sm.reference.prefix | General  | urn:x-hp:2009:sm | Set the prefix to compose the External Process Reference of Scheduled Downtime CI in UCMDB.<br><br><b>Note:</b> 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.

## Step 2: Tailor Service Manager to handle phase change

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 OMi.

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.

## Step 3: Set up downtime sync jobs in UCMDB

As part of CI synchronization, you have already set up an integration point between SM and UCMDB. In this step, you add downtime synchronization jobs, so that scheduled downtime CIs are created in UCMDB based on Requests for Change in SM.

To add the downtime synchronization jobs:

1. Log in to your UCMDB system as an administrator.
2. Edit the existing integration point that connects to your Service Manager server.
3. Click **Managers > Data Flow Management > Integration Studio**. UCMDB displays a list of integration points.
4. Select the existing SM integration point. Make sure that CIs have already been synchronized between SM and UCMDB.
5. Create two integration jobs in the integration point on the **Population** tab:
  - a. Create a new job including the `SM 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. Create another new job including the `SM CI Connection Downtime CI` 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 first. You can set the two jobs as schedule-based and set the schedule interval according to your needs.

**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.

## Step 4: Set up creation of BSM Downtime CIs

In this step, BSM Downtime CIs are created based on Scheduled Downtime CIs.

To enable downtimes defined in SM to be sent to OMi, you need to install the DFP2 in the OMi deployment.

### 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.

To create BSM Downtime CIs:

1. Create a new Integration Point or, if existing, edit the **Scheduled Downtime to BSM Downtime** Integration Point:
  - a. Do the following on your UCMDB:  
Go to:  
**Managers > Data Flow Management > Integration Studio**
  - b. Click **New Integration Point** or **Edit**, enter a name and description of your choice, and select the adapter: **BSM Downtime Adapter**.
  - c. Enter the following information for the adapter: OMi DPS Hostname and port 21212, communication protocol, and the context root (if you have a non-default context root).
  - d. Specify the credentials for the user you created in "[Create User Accounts for the OMi-SM Integration \(UCMDB\)](#)" on page 116 to access the OMi system. Choose generic protocol as protocol.
  - e. Click **OK**, then click the **Save** button above the list of the integration points.
2. 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.

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

## Step 5: Verify the SM-OMi downtime synchronization setup

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, choose a CI that has been 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 BSM (RTSM).          |

| External Status values | Description                                                                      |
|------------------------|----------------------------------------------------------------------------------|
| 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.

## Task 6. Test if BSM Downtime CIs have been created

1. In OMi, got to **Administration > Service Health > Downtime Management**.
2. Check if a corresponding Downtime was created.

## Sending downtime notifications from OMi to SM (UCMDB)

OMi can send downtime start and end events to SM to notify operators of when a downtime occurs. This provides additional information to the SM operator in case of a downtime that was not driven by an RFC.

To create downtimes in OMi based on RFCs in SM, see "[Downtime Forwarding from Service Manager to OMi \(UCMDB\)](#)" on page 143.

### Step 1: Send OMi Downtime Events to SM

To enable OMi to send downtime start and end events 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 *the OMi Administration Guide*.

Downtime events use the following formats:

- **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                                                                   |
| CloseKeyPattern | <OMi Downtime ID>:<Affected CI ID>:downtime-start                      |
| EtiHint         | downtime:end                                                           |
| LogOnly         | true                                                                   |

## View Changes and Incidents in OMi (UCMDB)

This integration enables you to view planned changes and incident details in the Changes and Incidents and Hierarchy components in OMi.

This chapter includes the following:

- ["Prerequisite" below](#)
- ["Step 1: Configure the Service Manager Adapter Time Zone" below](#)
- ["Step 2: Create an Integration Point in OMi" on page 153](#)
- ["Step 3: Edit Integration TQLs " on page 154](#)
- ["Step 4: Verify View changes and incidents" on page 155](#)
- ["How to Customize the Changes and Incidents Component" on page 155](#)

### Prerequisite

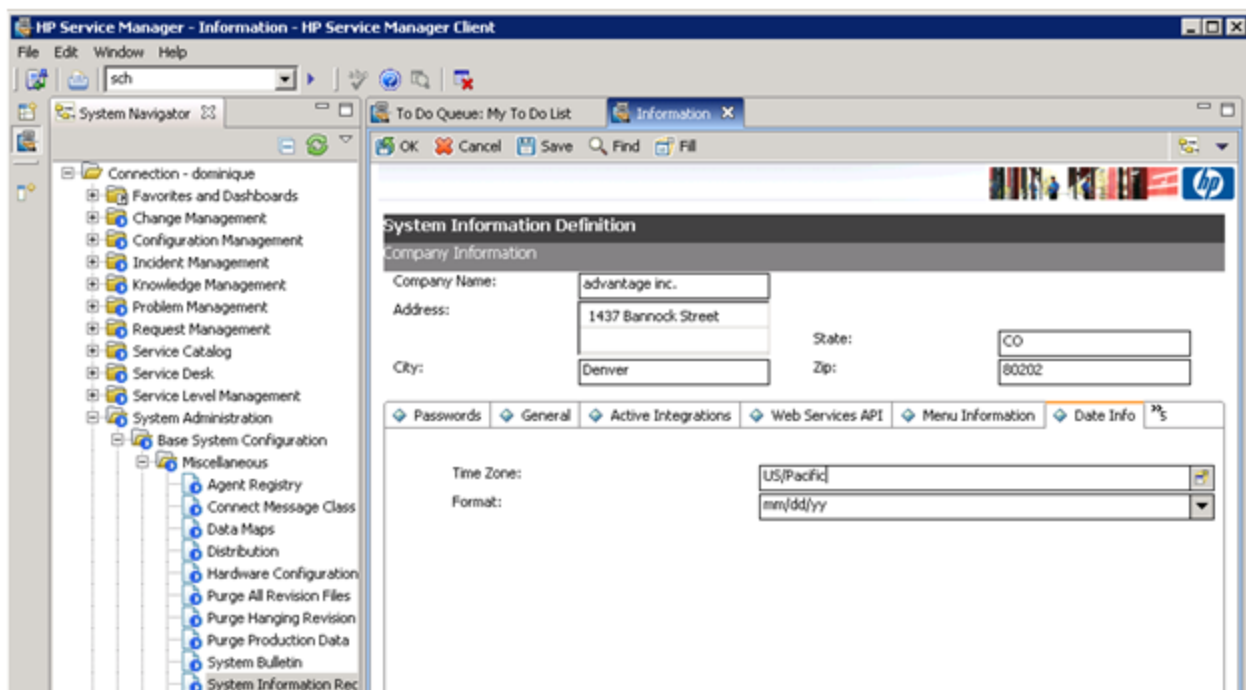
This integration requires that CIs are synchronized between UCMDB and SM. For information on CI synchronization, see ["Operations Manager i-Service Manager Integration Overview" on page 67](#)

This integration requires an administrator user account for OMi to connect to SM. This user account must already exist in both OMi and SM. For details on creating required user accounts, see ["Create User Accounts for the OMi-SM Integration \(UCMDB\)" on page 116](#)

### Step 1: Configure the Service Manager Adapter Time Zone

Configure the time zone so Incidents and Planned Changes have the correct time definitions:

1. In SM, select **Navigation pane > Menu navigation > System Administration > Base System Configuration > Miscellaneous > System Information Record**. Open the **Data Info** tab.
2. In the **Date Info** tab, look up the value for the Timezone.

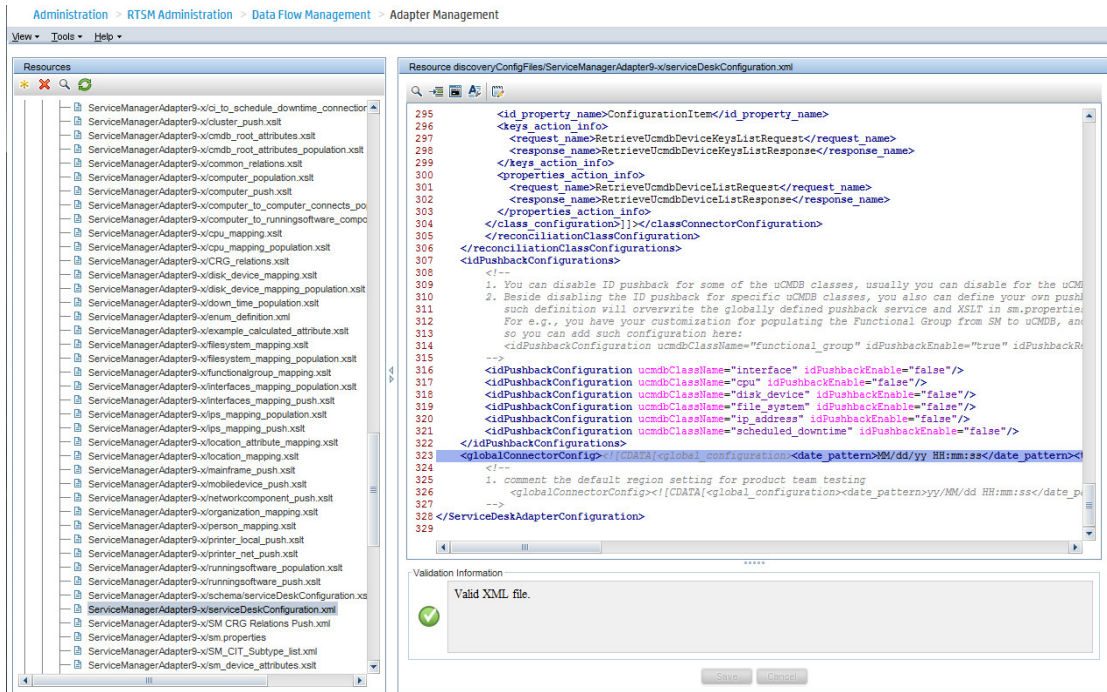


3. In OMi, select **Administration > RTSM Administration > Data Flow Management > Adapter Management**.
4. In the **Resources** window, open **ServiceManagerAdapter9-x > Configuration Files > ServiceManagerAdapter9-x/serviceDeskConfiguration.xml**

Find the row that includes the following string:

```
<globalConnectorConfig><![CDATA[<global_configuration><date_pattern>MM/dd/yy
HH:mm:ss</date_pattern><time_zone>US/MOUNTAIN</time_zone>
```





Check the date and time format, as well as a time zone. Note that the date is case-sensitive. Change either SM or the xml file so that they both match each other's settings.

**Note:** Specify a time zone from the Java time zone list that matches the time zone used in SM (for example, America/New York).

5. If you changed the time zone on SM, restart the SM server; if you changed the time zone on OMi, you do not need to restart the OMi server.)

## Step 2: Create an Integration Point in OMi

You edTo create an integration point, follow these steps:

1. In OMi, select **Administration > RTSM Administration > Data Flow Management > Integration Studio**.
2. In the Integration Point pane, select **Create New Integration Point** or choose an existing integration point to edit. The Create New Integration Point dialog box opens. Enter the following:

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

| Name                                                  | Recommended Value | Description                                                                                                                                                                                                                            |
|-------------------------------------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Adapter</b>                                        | <user defined>    | Select HP Software Products > Service Manager > <b>Service Manager 9.xx</b> .<br><br>This adapter, which supports CI/ relationship Data Push from RTSM to Service Manager, and Population and Federation from Service Manager to RTSM. |
| <b>Is Integration Activated</b>                       | <b>selected</b>   | Select this check box to create an active integration point.                                                                                                                                                                           |
| <b>Hostname/IP</b>                                    | <user defined>    | The name of the SM server.                                                                                                                                                                                                             |
| <b>Port</b>                                           | <user defined>    | The port through which you access SM.                                                                                                                                                                                                  |
| <b>Credentials</b>                                    | <user defined>    | Click <b>Generic Protocol</b> , click the <b>Add</b> button to add the integration user account you created in " <a href="#">Create User Accounts for the OMi-SM Integration (UCMDB)</a> " on page 116 and then select it.             |
| <b>Probe Name</b> (for ServiceManagerAdapter9-x only) | <user defined>    | Select the probe that you installed for this integration.                                                                                                                                                                              |

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

3. In the **Integration Point** pane, click the Integration Point you just created, and click the **Federation** tab in the right pane.
4. In the **Supported and Selected CI Types** area, verify that **Incident** and **RequestForChange** are selected.

### Step 3: Edit Integration TQLs

In this step, edit the integration TQLs so that they use the Integration Point created in the previous step.

1. In OMi, select **Administration > RTSM Administration > Modeling > Modeling Studio**.
2. On the **Resources** tab, select Resource Type: Queries. Open the **Console** folder.
3. Open the TQL: `CollectRequestForChangeWithImpacts`.
4. In the **Query Definition** pane, right click one of the objects of CI Type: RequestForChange.
5. From its Context Menu, select **Set Integration Points**. Choose the Integration Point that you configured in the previous step.
6. Repeat steps 4 and 5 for all objects of CI Type: RequestForChange.
7. Open the TQL: `CollectRequestForChangeWithoutImpacts`.
8. Repeat steps 4 and 5 for all objects of CI Type: RequestForChange.

9. Open the TQL: `CollectTicketsWithImpacts`.
10. In the **Query Definition** pane, right click one of the objects of CI Type: Incident.
11. From its Context Menu, select **Set Integration Points**. Choose the Integration Point that you configured in the previous step.
12. Repeat steps 10 and 11 for all objects of CI Type: Incident.
13. Open the TQL: `CollectTicketsWithoutImpacts`.
14. Repeat steps 10 and 11 for all objects of CI Type: Incident.
15. Save all TQLs.

## Step 4: Verify View changes and incidents

To verify that you can view changes and incidents in OMi, make sure that you have an incident in SM that is related to a CI in the OMi RTSM. To do so, send a test event related to a CI that has been synchronized between OMi and SM.

1. Send an event, for example, using the following command:  

```
submitEvent-t testViewIncidents -rch <hintForExistingCI>
```
2. Select the event in the OMi Event Browser and select **Transfer Control To** in the Context Menu. Select the SM target system.
3. Open the 360° View and select a view containing the related CI.
4. Select the CI, and verify that the **Incident Count** is at least 1. Click **Incidents** to show the Changes in Incidents window, and verify that the incident is displayed in the Incidents section.

By default, the Changes and Incidents component displays data for the previous week. You can change this setting to previous week, day, or hour (up to the current time) using the Configure Component button.

## How to Customize the Changes and Incidents Component

By default, incidents and requests for change are displayed for the following CI types: Business Service, Siebel Application, Business Application, and Node. If you want to view change and incident information for other CITs, perform the following procedure:

1. Open the Modeling Studio:  
**Administration > RTSM Administration > Modeling > Modeling Studio**

Copy one of the TQLs within the **Console** folder, and save your copy with a new name. These default TQLs perform the following:

| TQL name                                  | Description                                                                                          |
|-------------------------------------------|------------------------------------------------------------------------------------------------------|
| <code>CollectTicketsWithImpacts</code>    | Retrieves SM incidents for the selected CI, and for its child CIs which have an Impact relationship. |
| <code>CollectTicketsWithoutImpacts</code> | Retrieves SM incidents for the selected CI.                                                          |

| TQL name                              | Description                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| CollectRequestForChangeWithImpacts    | Retrieves SM requests for change, for the selected CI, and for its child CIs which have an Impact relationship. |
| CollectRequestForChangeWithoutImpacts | Retrieves SM requests for change, for the selected CI.                                                          |

2. Edit the new TQL as needed. You can add CITs as described in ["Naming Constraints for New Request for Change TQLs"](#) below.

3. Open Infrastructure Settings:

**Administration > Setup and Maintenance > Infrastructure Settings**

- a. Select **Applications**.
- b. Select **Service Health Application**.
- c. In the **Service Health Application - Hierarchy (360) properties** area, enter the name of the new TQL you created in the corresponding infrastructure setting.

**Note:** By default, these infrastructure settings contain the default TQL names. If you enter a TQL name that does not exist, the default value will be used instead.

After you modify the infrastructure setting, the new TQL will be used, and the Changes and Incidents component will show this information for the CITs you defined.

## Naming Constraints for New Request for Change TQLs

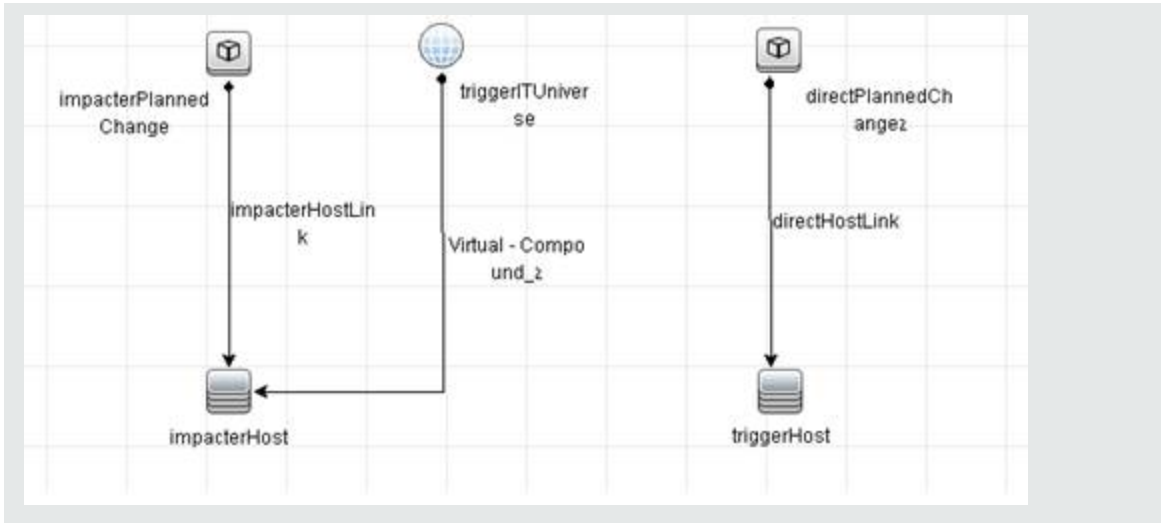
The following naming constraints must be followed in the request for change *without* impact TQL (see the TQL example below, on the right side of the image):

- The request for change CI type must start with **directPlannedChange**.
- The CI type related to the request for change must start with **trigger**.

The following naming constraints must be followed in the request for change *with* impact TQL (see the TQL example below, on the left side of the image):

- **impacterPlannedChange** represents the request for change CI type.
- The CI type related to the request for change must start with **impacter**.
- **triggerITUniverse** represents the "impacted" child CIs.

Examples of request for change TQLs:



## Naming Constraints for New Incident TQLs

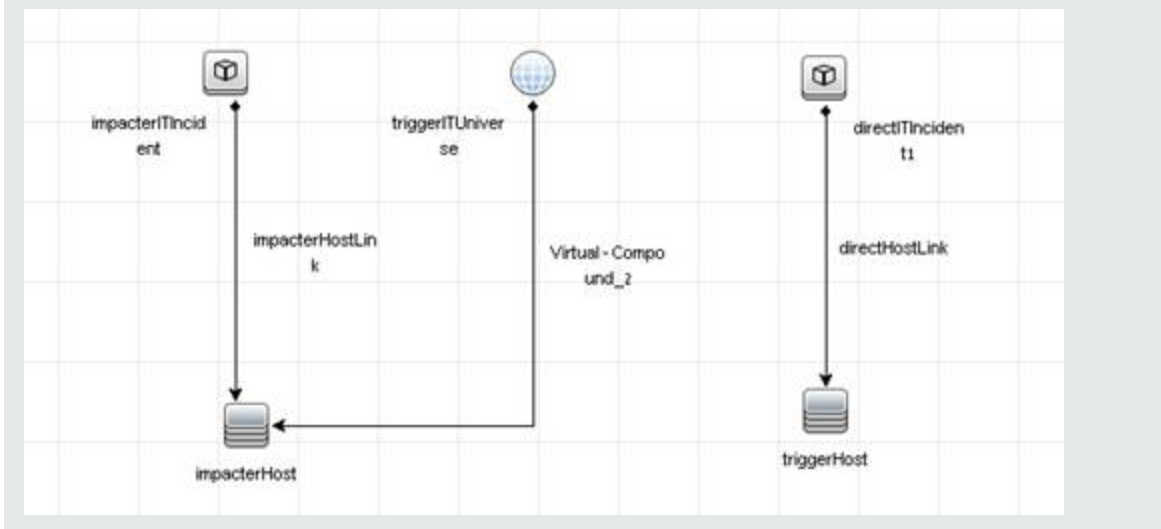
The following naming constraints must be followed in the incidents *without* impact TQL (see the TQL example below, on the right side of the image):

- The incident CI type must start with **directTIncident**.
- The CI type related to the incident must start with **trigger**.

The following naming constraints must be followed in the incidents *with* impact TQL (see the TQL example below, on the left side of the image):

- **impacterTIncident** represents the incident CI type.
- The CI type related to the incident must start with **impacter**.
- **triggerTUUniverse** represents the "impacted" child CIs.

Examples of incident TQLs:



## Business Impact Report (BIR) (UCMDB)

OMi includes a report that you can use to help evaluate the impact of incidents on your business. 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.

**Note:**

- This integration requires that CIs are synchronized between both Service Manager and OMi.
- Only one instance of this integration is allowed.

### Step 1: Add a Business Impact Report Integration in SM

To use the Service Manager to BIR integration, you must add and enable an instance of this integration in Integration Manager.

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.<br>Default: SMBIR  |
| Version   | (Required) The version of the integration template.<br>Default: 1.0 |
| SM Server | The name of the Service Manager server machine.                     |

| Field                 | Value                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------|
| Endpoint Server       | The name of the OMi 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 OMi 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.

## Step 2: Launch a Business Impact Report from an Incident

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**. The OMi Business Impact window opens, showing the KPI over time data for the related CI and related business services.





# Part VI: Operations Manager i - Network Node Manager i Integration

# Chapter 23: Operations Manager i - Network Node Manager i Integration Overview

**Tip:** The following is a high-level overview of the Operations Manager i - Network Node Manager i (NNMi) integration. You can find comprehensive details on NNMi integrations in the *HP Network Node Manager i Software—HP Business Service Management/Universal CMDB Topology Integration Guide*.

You can integrate NNMi with OMi to provide the following capabilities:

- **NNMi topology > OMi RTSM topology.** The topology integration populates the OMi RTSM with the NNMi network topology. OMi stores each device, interface, IP address, and a few other artifacts in the NNMi network topology as a CI and includes it in the relevant views.
- **NNMi events > OMi events.** NNMi events are displayed in the Event Browser in OMi. You can also access the NNMi console from the OMi Event Browser. The NNMi events are sent to OMi using the BSM Connector.

This integration has item ID 344 in the Integrations Catalog at the following location:

<http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=344>

- **NNMi events > OMi health indicators.** After you have set up the integration, if the NNMi events have corresponding health indicators defined, these health indicators affect the status of relevant CIs in OMi applications, such as Service Health.
- **OMi > NNMi drill down.** In OMi, you can configure a link to the NNMi management server that enables you to drill down from My Workspace and other locations to NNMi, to view trace route information between the client and the destination machine. You can also use URL tools to launch a browser that enables you to connect to the NNMi management server and further analyze incoming events in NNMi.

In addition, certain NNMi user interface components (network maps, items, detailed information dialogs, and so on) can be displayed directly in **Workspaces > My Workspace**.

**Note:** If the NNMi topology is not synchronized with the OMi RTSM topology, the **Monitored by** property of the OMi CIs corresponding to the NNMi CIs is empty, and these CIs are not displayed in the System Monitors only Perspective, System Hardware Monitoring, and System Software Monitoring views.

# Chapter 24: How to Integrate Network Node Manager i with Operations Manager i

This chapter describes how to integrate NNMi with OMi.

## 1. Prerequisite

Make sure you have the OMi and NNMi licenses installed. For details, see the OMi Administration Guide.

## 2. Perform the integration in NNMi

Perform the steps needed to integrate NNMi with OMi in the NNMi application.

For details, see the *HP Network Node Manager i Software—HP Business Service Management/Universal CMDB Topology Integration Guide*.

## 3. Configure LW-SSO in both OMi and NNMi (Optional)

To be able to seamlessly switch between NNMi and OMi, it is recommended to use LW-SSO. Make sure that LW-SSO is configured in both OMi and NNMi with the same `initString`. For details on how to configure the `initString` in OMi, see the OMi Administration Guide. For details on how to configure the `initString` in NNMi, see the *NNMi Deployment Reference*.

It is also possible to integrate NNMi with OMi without using LW-SSO. In this case, you are prompted for a password every time you switch to an NNMi component.

## 4. Connect NNMi to more than one OMi instance

After connecting the first OMi instance to NNMi, NNMi stores in its own database the CI IDs gained from the topology synchronization of the OMi's RTSM. When another OMi instance is connected, another topology synchronization is carried out. As the OMi instances might contain some of the same CI IDs, the IDs need to be reconciled in the NNMi database. This reconciliation works only partially and the NNMi log files still include several reconciliation errors that are caused by the non-existing RTSM IDs. To fix the problem, perform the following steps:

- a. Change the integration to the new OMi system.
- b. Log on to the NNMi JMX console `http://<NNMi_fqdn_and_port>/jmx-console` using the system account and password.
- c. Go to **mbean NnmBsmModule**.
- d. Run **`java.lang.String resetNnmBsmIds()`**.  
You should see a list of devices from which the RTSM ID was removed.
- e. Disable and enable the topology integration to get the CIs into RTSM.

## 5. Configure OMi to display NNMi data

To display NNMi data in OMi and to access the NNMi components in **Workspaces > My**

**Workspace:**

- a. Open Infrastructure Settings:

**Administration > Setup and Maintenance > Infrastructure Settings**

- b. Select **Foundations**.

- c. Select **Integrations with other applications**.

- d. In the **Integrations with other applications - HP NNM** table, locate and modify the following parameters:

- **HP NNM Integration URL**. The NNMi host and port number (protocol://host:port/nnm).
- **HP NNM User name**. The user name that is used for logging on to NNMi.
- **HP NNM User password**. The user password that is used for logging on to NNMi.

6. Results

You can view NNMi data in **Workspaces > My Workspace**, as described in "[NNMi Components in My Workspace](#)" on page 165.

# Chapter 25: NNMi Components in My Workspace

If you set up an integration between NNMi and OMi, you can view the NNMi components described below in **Workspaces > My Workspace** as follows:

1. Click the **New Page** icon.
2. Click **Add Component**. The Component Gallery window opens.
3. In All Categories, select the **NNMi** check box.

To access the NNMi components, you must have the appropriate licenses installed. NNMi components are only displayed if you configured a connection to an NNMi server in Infrastructure Settings:

**Administration > Setup and Maintenance > Infrastructure Settings**

Select **Foundations > Integrations with other applications > HP NNM**.

| Component Name                                      | Description                                                                                                                                                                                                |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Layer 2 Neighbor View</b>                        | Shows a map view of a selected device and its connector devices within a specified number of hops from the selected device. This view is useful for understanding the switch connectivity between devices. |
| <b>Layer 3 Neighbor View</b>                        | Shows a map view of a selected device and its connector devices within a specified number of hops from the selected device. This view is useful for understanding the router connectivity between devices. |
| <b>MPLS VPN Inventory</b>                           | This is an enterprise customer view of how their sites are connected via service provided MPLS networks.                                                                                                   |
| <b>Open Key Incidents</b>                           | Shows the incidents that are most important to network operators and that often require more immediate action.                                                                                             |
| <b>Overall Network Health (Node Group Overview)</b> | Displays a map containing all (top-level) Node Groups that do not have parent Node Groups.                                                                                                                 |
| <b>Overall Network Health - Routers</b>             | Displays a Node Group Map of the Router connectivity in your network.                                                                                                                                      |
| <b>Overall Network Health - Switches</b>            | Displays a Node Group map of the Switches connectivity in your network.                                                                                                                                    |

| <b>Component Name</b>                     | <b>Description</b>                                                                                                                                                                                                                                               |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Router Redundancy Groups Inventory</b> | Shows the available Router Redundancy Groups created by the NNMi administrator. Each Router Redundancy Group is a set of two or more routers that use one or more virtual IP addresses to help ensure that information packets reach their intended destination. |

# Part VII: Operations Manager i - Operations Orchestration Integration

# Chapter 26: Operations Manager i - Operations Orchestration Integration Overview

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

OO run books can be launched from the Service Health and Event Browser applications.

The integration of OMi and OO provides the capability of mapping CI types to OO run books.

After you create such mappings, you can run the mapped OO run books:

- **On CIs, using the Invoke Run Books context menu option in Service Health.** The OO run book parameters are populated using the map to the CI attributes defined in the Run Book Mapping Configuration wizard. For detailed information about the wizard, see the OMi Administration Guide.
- **At the event level.** OMi opens an event and checks if the CI for this event has a run book assigned to it, and if the run book is set to run automatically. The OO run book parameters are populated using the map to the CI or event attributes defined in the Run Book Mapping Configuration wizard. For detailed information about the wizard, see the OMi Administration Guide.



# Chapter 27: How to Integrate Operations Manager i and Operations Orchestration

This chapter describes how to integrate OMi and OO.

## 1. Prerequisites

Before you configure the integration, the OO administrator needs to perform the following:

- a. Enable user authentication and create an integration user with the **Administrator** role:
  - **OO version 10.02 or higher:** The user must be **internal**.
  - **OO 9.xx:** The user must be **external**.

Users must have the following capabilities in OO: AUTHOR, SCHEDULE, MANAGE\_RUNS, RUN\_REPORTS, and HEADLESS\_FLOWS. You can either add users to groups with these capabilities (for example, the administrator group has these capabilities) or you can create such a group.

- b. Deploy the following OO Content Packs (CPs) on the OO server: **Base**, **Middleware**, and **Operating Systems**.

First deploy the **Base** CP, and then the other CPs.

For details how to deploy CPs in OO, see the OO documentation.

- c. If you want to configure run book automation in a set up with a load balancer and a firewall, ensure that port 8443 is open. If port 8443 is not open, the automatic run book execution will fail. The **Automatic Run Book Execution** is triggered from the data processing server.

## 2. Configure the link between OMi and OO

To configure the integration between OMi and OO, in OMi:

- a. Open Infrastructure Settings:
  - Administration > Setup and Maintenance > Infrastructure Settings**
- b. Select **Foundations**.
- c. Select **Integrations with other applications**.
- d. In the **HP Operations Orchestration** table, locate **Operations Orchestration application URL**, and modify the setting to the URL used to access the OO application.

When connecting an OMi instance that employs Lightweight Single Sign-On (LW-SSO) to **OO version 10.02 or higher**, you must specify the connection URL of OO using the following format: **<protocol>://<FQDN>:<portNumber>** (for example, http://lab.lab:8080). The port can be 8080 for HTTP or 8443 for HTTPS, according to your needs. For **OO 9.xx**, use: https://<fully qualified server name>:8443.

If you want to enable run books to be invoked automatically, you must enter a User Name and Password in the same table. In this case, the user should be defined as **internal** in OO.

- e. **OO 9.xx only:** To be able to invoke run books automatically, the user must be **internal**.

### 3. Configure LW-SSO authentication

Configure LW-SSO authentication between OMi and OO. You must configure LW-SSO in both OMi and OO. Proceed to the relevant section depending on your version of OO.

#### For OO version 9.05 or lower:

- a. In OMi, open Authentication Management:

##### **Administration > Users > Authentication Management**

Copy the **Token Creation Key (initString)** to OO, and replace, in OO, all the initStrings in the **lwssofmconf.xml** file located in the **<OO installation directory>\Program Files\Hewlett-Packard\Operations Orchestration\Central\conf\** directory.

- b. In OO, in the **web.xml** and **applicationContext.xml** files located in the **<OO installation directory>\Program Files\Hewlett-Packard\Operations Orchestration\Central\WEB-INF\** directory, enable all filters and mappings between **LWSSO\_SECTION\_BEGIN** and **LWSSO\_SECTION\_END**.
- c. If OO and OMi are in different domains in the Windows operating system, you must make sure that the **Trusted Hosts/Domains** parameter is the same in OO and OMi. To set the parameter in OMi, open Authentication Management:

##### **Administration > Users > Authentication Management**

Configure the **Trusted Hosts/Domains** parameter.

- d. Restart the following OO services:
  - For OO version 9.02 or lower: **RSCentral**, **RSJRAS**, and **RSScheduler**.
  - For OO version 9.03, 9.04, or 9.05: **RSCentral** and **RSJRAS**.

**Note:** If you need to enable logging for debugging LW-SSO: In OO, in the **<OO installation directory>\jetty\resources\log4j.properties** file, uncomment the line that appears under the LW-SSO comment.

#### For OO version 9.06 or higher:

- a. In OMi, open Authentication Management:

##### **Administration > Users > Authentication Management**

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

- b. In OO, access the following:
  - For OO version 10.20, select **System Configuration > Security > SSO**.
  - For OO version 10.02 or higher (except version 10.20), select **System Workspace > Security > SSO**.
  - For OO version 9.xx, select **Administration > System Configuration > Authentication**.
- c. In the **LW SSO Settings** area, select the **Enable Authentication** check box.
- d. Replace the value of the **LW SSO** passphrase or the **InitString** parameter with the Token Creation Key you copied from OMi. (This must have the same value on all OMi instances that are integrated using LW-SSO.)
- e. Define domain-related parameters in the **LW SSO Settings** area:

- **Domain.** The domain of the OO server.
- **Protected Domains.** List of comma-separated domains used by the OMi instances that employ LW-SSO.

**Note:** If OO and OMi are in different domains in the Windows operating system, make sure that the **Trusted Hosts/Domains** parameter is the same in OO and OMi.

In OMi, open Authentication Management:

**Administration > Users > Authentication Management**

Configure the **Trusted Hosts/Domains** parameter.

**Note: Limitation with OO 10.02 or higher and OMi**

The integration of OO 10.02 or higher with OMi is currently only supported if OO and OMi are in the same domain. If they are in different domains, the integration fails.

For further details on configuring LW-SSO in OO, see the OO documentation.

For further details on configuring LW-SSO in OMi, see the OMi Administration Guide.

#### 4. Export server certificates from OO

To export server certificates from OO and import them into OMi in a Windows or Linux environment, use the **keytool** utility, which is included in JRE.

**For OO 9.xx:**

- a. On the OO server, enter:
  - **Windows:**  
`[OO install folder]\jre1.6\bin\keytool -keystore "[OO install folder]\Central\conf\rc_keystore" -export -alias pas -file "<path>\<Operations Orchestration fully qualified host name>.cer"`
  - **Linux:**  
`keytool -keystore "$ICONCLUDE_HOME/Central/conf/rc_keystore" -export -alias pas -file "<path>/<Operations Orchestration fully qualified host name>.cer"`
- b. When prompted for a password, enter `bran507025`.

**For OO version 10.02 or higher**

- a. On the OO server, enter:
  - **Windows:**  
`[OO install folder]\java\bin\keytool.exe -keystore "[OO install folder]\central\var\security\key.store" -export -alias tomcat -file "<path>\<Operations Orchestration fully qualified host name>.cer"`
  - **Linux:**  
`keytool -keystore "$ICONCLUDE_HOME/central/var/security/key.store" -export -alias tomcat -file "<path>/<Operations Orchestration fully qualified host name>.cer"`
- b. When prompted for a password, enter `changeit`.

## 5. Import OO server certificates to OMi

Import the server certificate from the OO server to the OMi Gateway Server so that the two systems can communicate with each other securely.

- a. **Import the Server Certificate to OMi.** To import the server certificate you exported from OO to the OMi cacerts keystores, on the OMi Gateway Server and Data Processing Server:

■ **Windows:**

Enter the following commands:

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

■ **Linux:**

Enter the following command:

```
$TOPAZ_HOME/JRE/bin/keytool -keystore "$TOPAZ_HOME/JRE/lib/security/cacerts" -import -alias "<Operations Orchestration fully qualified host name>" -file "<path>/<Operations Orchestration fully qualified host name>.cer"
```

**Note:** If TOPAZ\_HOME is not set, use the following script:  
`./opt/HP/BSM/scripts/topaz_env.sh`

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

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

- i. Click **Tools > Internet Options > Content > Certificates**.
  - ii. In the Trusted Root Certification Authorities tab, click the **Import...** button.
  - iii. Click **Next** to start the Certificate Import Wizard.
  - iv. Specify the file you want to import, and then click **Next**.
  - v. Select the **Place all certificates in the following store** radio button, and then click **Browse**.
  - vi. Select **Trusted Root Certification Authorities**, and then click **Next**.
  - vii. Click **Finish**.
- d. Restart OMi on the Gateway server.

**Note:** Repeat the above steps on the Data Processing Server as well.

## 6. Grant permissions

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

To integrate with OO, you must set up users with specific permissions. Select

**Administration > Users > Users, Groups, and Roles**

Select the user or create a new user and grant them a role with **Operations Orchestration Integration** permissions.

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

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

**7. Map run books to CI Types**

You can map OO run book parameters to:

- CI type attributes. For details on the user interface, see the OMi Administration Guide.  
The child CIs of a CI, for which you configure a run book, are also assigned to that run book.

**Note:** To be able to map run books to CI types, either create a run book flow in OO, or import a content pack in OO with the Content Workspace.

- The event attributes are predefined in OMi.

For details, see the OMi Administration Guide.

**8. Use OO functionality from OMi**

You can trigger a run book:

- From Service Health using the **Invoke Run Books** context menu option.
- From the Event Browser using the context menu or from the Action Panel.

# Chapter 28: Troubleshooting Integration Problems

## Connection Errors

If you receive a connection error when you select run books in the **Available Run Books** pane (**Library > Operations**), change the **run.book.timeout** and **service.center.ws.timeout** settings from 10000 to 60000 (1 minute):

1. Open a JMX console on the OMi server: **http://localhost:29000**.
2. Select **Foundations > service=Infrastructure Settings Manager**.
3. To set the values, use **setSettingValuePerCustomerId()** with **contextName: integrations** and **settingName: settings.pm.settings.run.book.timeout** or **settings.pm.settings.service.center.ws.timeout**. Change to **newValue: 60000**.

**Note:** Restarting OMi is not required.

## Different Domains

If OMi and OO 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**).

# Chapter 29: Examples of Operations Manager i and Operations Orchestration Integrations

This section describes two possible scenarios to integrate OMi and OO.

## Use Case Scenario in Service Health

In OO, the **Restart a Node** run book is associated with a Node CI Type. The parameters of the run book are mapped to the relevant CI attributes of the Node CI.

In Service Health, the operator detects that a host has a system problem. The operator right-clicks the CI to get a list of the run books relevant to the CI. One of the run books is **Restart a Node**. The run book can execute automatically because the values of the parameters such as the host name or the IP address are automatically populated by data taken from the CI context.

## Use Case Scenario in the Event Browser

In the OMi Event Browser, the operator is going through the assigned events. The operator detects an event related to a lack of disk space that causes a database performance issue. From the event context, the operator can get a list of relevant run books. The operator can launch the appropriate run book manually. The run book continues running without further input from the operator as all run book parameters are extracted from the event or related CI.

**Tip:** If you set up the integration between OO and OMi, you can also use **Automatic Run Book Execution** to run an OO flow as an automatic action. For details, see the OMi Administration Guide.

Although OO flows are not set up as an automatic action in the policy, you can run OO flows automatically when the event comes into OMi, or as a result of time-based event automation.

# Part VIII: BSM Connector Integrations



# Chapter 30: BSM Connector Integration Administration

BSM Connector captures data such as events, metrics, and topology from third-party systems. Events and topology data are forwarded to OMi; metrics data is stored locally on the BSM Connector system and can be viewed in OMi using the embedded Performance Graphing component. Service Health Reporter, a high-capacity performance reporting solution also enables you to generate reports on data collected by BSM Connector.

To access

In OMi, select:

**Administration > Setup and Maintenance > Connected Servers**

For details on configuring a BSM Connector server in OMi, see the *BSM Connector User Guide*.

## BSM Connector Integrations Overview

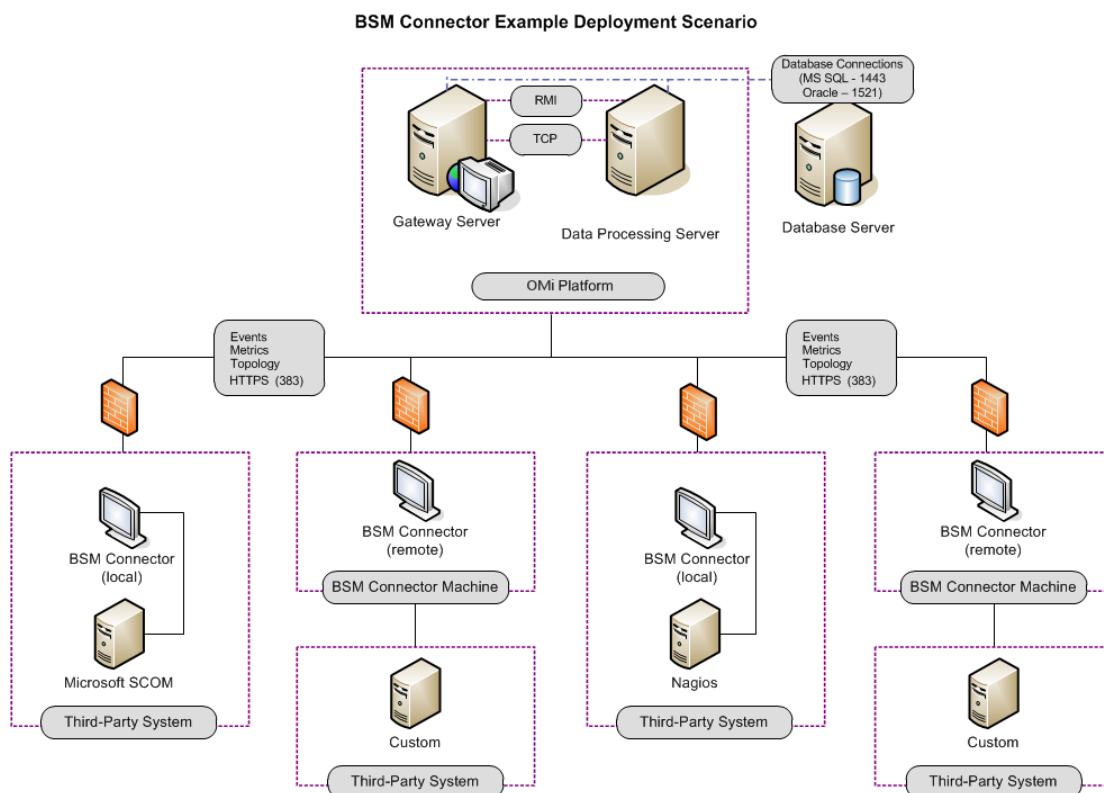
From the **Connected Servers** page, you can access and maintain all BSM Connectors in the OMi deployment environment, regardless of the operating system or host location on which the BSM Connector is installed.

The **Connected Servers** page enables you to add, modify, or remove BSM Connector integrations from the OMi deployment environment.

Before you can add a BSM Connector integration, BSM Connector must be installed in the OMi deployment environment. That is, the BSM Connector host must have access to at least one OMi Gateway Server in the OMi deployment environment to which it sends the collected data. Additionally, BSM Connector must have access to the third-party system from which it is collecting data.

For some types of data sources, BSM Connector must be installed and run locally on the host of the third-party system with which it is integrating. Examples for local data sources are XML files, open message interface messages, and scheduled tasks. For other types of data sources, BSM Connector can be installed on the host of the third-party system or on a remote system. For more information on supported data sources, see the *BSM Connector online help*.

The following diagram shows an example of an OMi deployment environment with four BSM Connector integrations.



For information about installing BSM Connector, see the *BSM Connector Installation and Upgrade Guide*.

### Controlling data transfer with policies


The data transfer is controlled by policies that you define in BSM Connector. Policies monitor the data sources and, if certain conditions apply, forward the data in the form of events or metrics to OMi. The policies can optionally also map the data to topology and create configuration items (CIs) and CI relationships in BSM Connector. This enables OMi to associate the events and metrics it receives with CIs.

### Out-of-the box integrations

You can use one of the out-of-the box integrations that are available for BSM Connector. Alternatively, if you do not find the integration that you are looking for, you can develop your own custom integration.

HP is continually updating the list of the integrations with third-party products. For details and for download information, see the HP Live Network site: <https://hpln.hp.com/group/bsm-integrations>.

### More information

For complete information about the features, capabilities, and usage of BSM Connector, see the BSM Connector online help after you install BSM Connector. To access the help, click **Help**  in the toolbar of the BSM Connector user interface.

# 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 OMi Integrations Guide (Operations Manager i 10.01)**

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-asm@hp.com](mailto:ovdoc-asm@hp.com).

We appreciate your feedback!



Go OMi!