



HP Operations Manager i

Software Version: 10.00

OMi Integrations Guide

Document Release Date: January 2015
Software Release Date: March 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 U.S. registered trademarks of Microsoft Corporation.

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=>.

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
Chapter 4: How to Display APM Data in OMi	26
Part III: Operations Manager i - HP SiteScope Integration	27
Chapter 5: SiteScope Integration - Overview	28
Chapter 6: SiteScope Integration - Tasks	30
Chapter 7: How to Create a Connection to a SiteScope Server	36
Part IV: Operations Manager i - HP Operations Manager Integration	40
Chapter 8: Operations Manager i - HP Operations Manager Integration Overview	41
Chapter 9: Workflow: Configuring Connections Between Operations Manager i and HPOM ...	43
Chapter 10: How to Establish a Trust Relationship for a Server Connection	44
Chapter 11: How to Verify the Trusted Relationship	48
Chapter 12: How to Create a Connection to an HPOM Server	49
Chapter 13: How to Run Dynamic Topology Synchronization	53
Chapter 14: How to Configure the HPOM for Windows Forwarding Policy	58
Chapter 15: How to Configure the HPOM for UNIX or Linux Forwarding Policy	61
Chapter 16: How to Set up a Forwarding Target in the HPOM for UNIX or Linux Node Bank ...	64
Chapter 17: How to Validate Event Synchronization	65
Chapter 18: How to Set up Operations Manager i in an Environment Managed by HPOM	67
Chapter 19: OMi Field Mapping	68
Chapter 20: Troubleshooting	71
Part V: Operations Manager i - Service Manager Integration	72
Chapter 21: Operations Manager i - Service Manager Integration Overview	73
Point to Point Integration	73

Integration Using a Universal Configuration Management Database (uCMDB)	74
Data Flow Probes	74
Chapter 22: Downtime Exchange Between Operations Manager i and Service Manager	77
Integration Overview	77
Step 1: Send OMi Downtime Events to SM	78
Step 2: Integrate SM Downtimes with OMi	80
Chapter 23: Incident Exchange Between Service Manager and Operations Manager i	82
Step 1: Configure the SM Server as a Connected Server	82
Step 2: Configure an Event Forwarding Rule	86
Step 3: Configure a URL Launch of the Event Browser from SM	87
Step 4: Configure a URL Launch of SM from the Event Browser	88
Step 5: Configure the SM Server	89
Step 6: Mapping and Customization	90
Step 7: Test the Connection	91
Step 8: Synchronize Attributes	92
Tips for Customizing Groovy Scripts	93
Chapter 24: View Changes and Incidents in Service Health Using Standalone HP Universal CMDB	96
Prerequisite	97
Step 1: Load the .unl File to Provide External Access to Service Manager	97
Step 2: Configure the Service Manager Adapter Time Zone	98
Step 3: Configure UCMDB to Generate Global IDs	99
Step 4 (for SM 9.2x only): Add a Domain	100
Step 5: Configure SM Adapter in UCMDB	101
Step 6: Configure the SM-UCMDB Integration: Create an Integration Point	101
Step 7: Configure the SM-UCMDB Integration: Set Up Data Push Jobs	102
Step 8: Configure the SM-UCMDB Integration: Run Data Push Jobs	103
Step 9: Configure the SM-UCMDB Integration: Add UCMDB Connection Information to SM	104
Step 10: Configure the OMi-UCMDB Integration: Deploy CMS_to_RTSM_Sync.zip on UCMDB	104
Step 11: Configure the OMi-UCMDB Integration: Create an Integration Point on OMi	105
Step 12: Configure the OMi-UCMDB Integration: Create an Integration Point on the CMS	107
Step 13 (Optional): Add CI Types to the Service Health Changes and Incidents Component	109
Result	110
Troubleshooting	110
Chapter 25: View Changes and Incidents in Service Health Using RTSM	111
Prerequisite	111

Step 1: Configure the Service Manager Adapter Time Zone	111
Step 2: Create an Integration User Account in Service Manager	113
Step 3: Add the OMi Connection Information in SM	114
Step 4: Create an Integration Point in OMi	114
Step 5: Create New Jobs to Synchronize Between OMi and SM	116
Step 6: Run the Job	116
Step 7: Test the Configuration	116
Step 8 (Optional): Add CI Types to the Service Health Changes and Incidents Component	119
Troubleshooting	119
Chapter 26: How to Customize the Changes and Incidents Component	120
Naming Constraints for New Request for Change TQLs	121
Naming Constraints for New Incident TQLs	121
Customizing the Service Manager 9.2 Integration	122
Mapping Table: OMi Event to BDM Incident Property	131
Part VI: Operations Manager i - Network Node Manager i Integration	138
Chapter 27: Operations Manager i - Network Node Manager i Integration Overview	139
Chapter 28: How to Integrate Network Node Manager i with Operations Manager i	140
Chapter 29: NNMi Components in My Workspace	142
Part VII: Operations Manager i - Operations Orchestration Integration	144
Chapter 30: Operations Manager i - Operations Orchestration Integration Overview	145
Chapter 31: How to Integrate Operations Manager i and Operations Orchestration	146
Chapter 32: Troubleshooting Integration Problems	153
Chapter 33: Examples of Operations Manager i and Operations Orchestration Integrations ..	154
Part VIII: BSM Connector Integrations	155
Chapter 34: BSM Connector Integration Administration	156
Send Documentation Feedback	158

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 OMIs enable the exchange of events between OMIs, using event synchronization and topology synchronization between the OMIs.

For more information on working with multiple OMIs, 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 sync.

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 allows you to:

- Design a dashboard in which you see OMi and APM data displayed side by side. It is possible to drill down into the APM data from this dashboard.
- Integrate user interface components from separately deployed APM systems directly into the OMiuser interface workspaces. In this way, relevant information is shown directly within the OMiuser interface, although this data comes from the APM system.
- Use OMi's 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 APMuser interface. For this purpose, OMi provides drill down operations that allow to launch the APMuser 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 10.00
- BSM - APM 9.25
- 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 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" below](#)

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

1. Make sure the Data Flow Probe is installed. For details, see ["Install the UCMDB Data Flow Probe" on page 16](#).
2. 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 20](#).
3. Create the integration user. For details, see ["Create the Integration User" on page 20](#)
4. 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](#).
5. Verify the Topology Synchronization. For details, see ["Verify the Topology Synchronization " on page 22](#)
6. 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 rulesFor details, see [" Continue the Setup of APM in OMi and Start the Integration" on page 23](#)
7. Configure the initial KPI Status and Downtime Synchronization. For details, see [" Configure Initial KPI Status and Downtime Synchronization" on page 24](#)
8. Deleting a connected server. For details, see ["Deleting a Connected Server" on page 25](#)

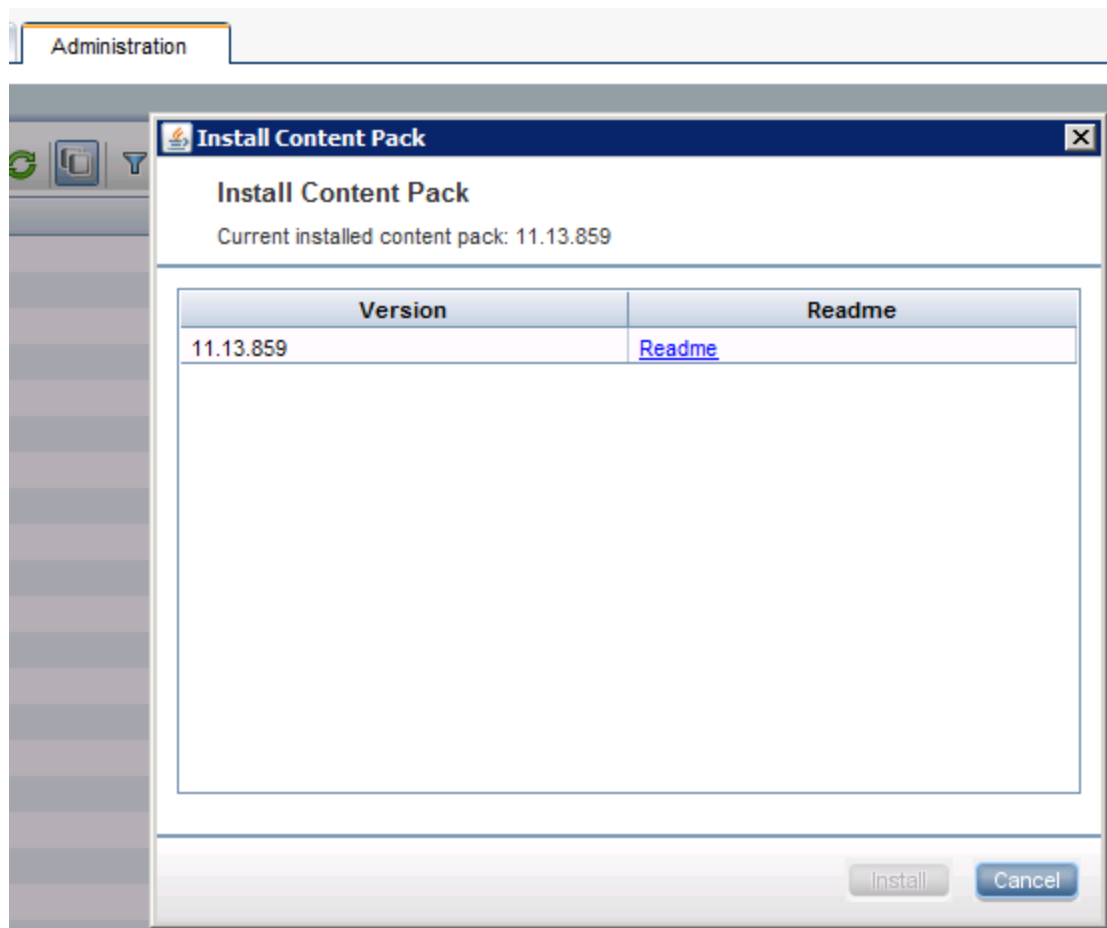
Integrate a BSM - APM deployment updated from a running BSM 9.24 or earlier to BSM 9.25 or later

1. On your APM server, check if uCMDB content pack 11.13.859 is installed. On the BSM 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





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 `<OMi_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 `<OMi_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 `<OMi_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 `tql - 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 `<OMi_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 `tql - 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 `<OMi_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 `tql - OMi_Sync_SIS` and `tql - 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_BLE  
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%3DInfrastructure+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%3A  
service%3DInfrast  
ructure+Settings+Manager
```


- e. Find the method **java.lang.String 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 starting the UCMDB Data Flow Probe was successful, check the 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. Exclude the CI types that should not be synchronized by adding these entries between `<excludeFilter>` and `</excludeFilter>`:

```
<vector>
<object class="sitedscope_group"></object>
<object class="sitedscope_measurement"></object>
<object class="sitedscope_measurement_group"></object>
<object class="sitedscope_monitor"></object>
<object class="sitedscope_profile"></object>
<object class="sitedscope_profile_monitor"></object>
<object class="sitedscope_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>
```

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

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

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 **setSettingsValue**.

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 Secure Socket Layer (SSL)

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

1. Enable SSL 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
```

Import Certificates

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>/JRE64/bin/keytool.[exe, sh]-import -trustcacerts -file <Root  
Certificate of your Certificate Authority> -alias <any name> -keystore <APM_  
HOME>/JRE64/lib/security/cacerts
```

2. On the APM gateway and data processing servers, run the following command:

```
<APM_HOME>/JRE64/bin/keytool.[exe, sh]-import -trustcacerts -file <Root  
Certificate of your Certificate Authority> -alias <any name> -keystore <OMi_  
HOME>/JRE64/lib/security/cacerts
```

If you are working with a High Availability deployment, you need to import the root certificate from your certification authority to all the servers in your HA set up.

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:

1. In your APM deployment:
 - a. Open **Administration > Platform > Platform Authentication Management**.
 - b. Click **Configure** to open the **Authentication Management** wizard.
 - c. Click **Next** to open the **Single Sign-On Configuration** wizard.
 - d. Copy the `initString` from **JMX to get Token Creation Key (initString)**
 - e. Click **Finish** to save your configuration.
2. In OMi:
 - a. Navigate to Authentication Management:
Administration > Users > Authentication Management
 - b. Double-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 **Platform > User and Permissions > User Management**.
7. Select **Operations Management** from the **Context** drop-down list
8. Select **Create New Users** with the same user name as the integration user created previously
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, depending on the Refresh interval defined in the following setting:

Applications > Operations Management > Operations Management - Topaz Authorization Service Settings > Refresh Interval

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

After completing this step, you will have synchronized configuration items (CIs) that exist in APM to OMi.

1. On the OMi deployment, navigate to
Administration > Setup and Maintenance > Connected Servers
2. Click  **New** and select **APM** from the drop-down list. The **General** page of the **Create New Server Connection - APM** wizard opens.
3. Enter a **Display Name** (the **Name** is entered automatically) and click **Next**. The **Server Properties** page opens.
4. Enter the FQDN of the **Application User**. This is especially important in case of an High Availability configuration.
5. Enter the user name and password of the integration user.
6. *Optional:* if the URL Path has changed, you need to add the new URL

If you press **Test Connection** now, you will receive an error, because no synchronization has happened at this point.

7. Click **Next** to go to the Synchronization pane of the **Create New Server Connection - APM** wizard.
8. 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.
9. Select the name of your Data Flow Probe from the drop-down list. The **Domain Name** is inserted automatically.
10. Click **Finish** 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 underneath 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.

Adjust KPI Assignments

BSM will create Improved/Worsened CI Status events that are forwarded to **OMi**:

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

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.

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 on the desired APM

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

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 30](#)

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 36](#)

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 page 32](#)
- ["How to Import Templates from a SiteScope Server" on page 33](#)
- ["How to Assign SiteScope Policy Templates to Remote Servers" on page 34](#)
- ["How to Combine Policy Templates into an Aspect or Management Template" 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, the new systems are migrated as inactive connected servers that do not get registered by OMi until they get activated.

To activate a migrated SiteScope connected server:

1. Open the Connected Servers manager from Administration.
2. Select the SiteScope connected server you want to activate and click the  button.

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

To finish the upgrade, you need to manually import the Health Indicator and CI Type Mapping content from the BSM version you are upgrading from. Proceed as follows:

1. On the SiteScope system, copy the files `ciSubTypes.xml`, `indicators.xml`, `meas2eti.xml`, and `userDefinedCiType.xml` located in `<SiteScope_installation_dir>/config/integration/bsm` and add them to a temporary directory on the OMi system.
2. Run the following command:

```
<OMi_HOME>/bin/opr-import-xml-files.[bat|sh] -folder <path_temporary_dir>
```

As a result, the updated files are uploaded to the `<OMi_HOME>/conf/sis/content` directory.

Note: The imported content overrides the default Health Indicator and CI Type Mapping content provided in the `<OMi_HOME>/conf/sis/content` directory.

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

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 36](#).
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>\JRE64\bin\keytool -importcert -alias <yourCA> -file
<CAcertificateFile> -keystore <OMi_HOME>\JRE64\lib\security\cacerts
```

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

- d. *Windows only.* 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>\JRE64\bin\keytool -importcert -file <certificateFile> -keystore
<OMi_HOME>\JRE64\lib\security\cacerts
```

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

- e. *Windows only.* 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 31](#) 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 31](#) 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.

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**) and 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 dynamic 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 44.](#)

To verify the trusted relationship, see ["How to Verify the Trusted Relationship" on page 48.](#)

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 49.](#)

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 Dynamic Topology Synchronization" on page 53.](#)

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 58.](#)

- **HPOM for UNIX or Linux.** For task details, see ["How to Configure the HPOM for UNIX or Linux Forwarding Policy" on page 61.](#)

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 65.](#)

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, hpommgmtsv).

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%\javaopr-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:

- The certificate on the load balancer must be installed for port 383 (or the port that you configured for secure communication).
- 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 48](#).

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 (for example, 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:

- **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 (for example, 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 44.

- **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**.
6. 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).

Chapter 13: How to Run Dynamic 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 44](#).
- Add the HPOM server as a connected server to OMi. For details, see ["How to Create a Connection to an HPOM Server" on page 49](#).
- *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 Dynamic 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 Dynamic Topology Synchronization on HPOM for UNIX or Linux Systems" on page 56](#)
- ["How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems" on page 56](#)

How to Configure Dynamic Topology Synchronization on HPOM for Windows Systems

This section describes how to configure dynamic 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 Dynamic Topology Synchronization on HPOM for UNIX or Linux Systems

This section describes how to configure dynamic 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 your HPOM server version is 9.10.220 or higher.
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.
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 your HPOM server version is 9.10.220 or higher.
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/Utils/opcnode -deassign_pol node_name=<management_server> net_type=NETWORK_IP pol_name=DiscoverOMTypes pol_type=svcdisc
```

```
/opt/OV/bin/OpC/Utils/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/OV/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 page 58](#).

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 ["How to Set up a Forwarding Target in the HPOM for UNIX or Linux Node Bank" on page 64](#)). 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](#).

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 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, for example:

```
/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
```

Chapter 17: 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 49](#).

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 18: 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 43.

Chapter 19: 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 20: 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`

Part V: Operations Manager i – Service Manager Integration

Chapter 21: Operations Manager i - Service Manager Integration Overview

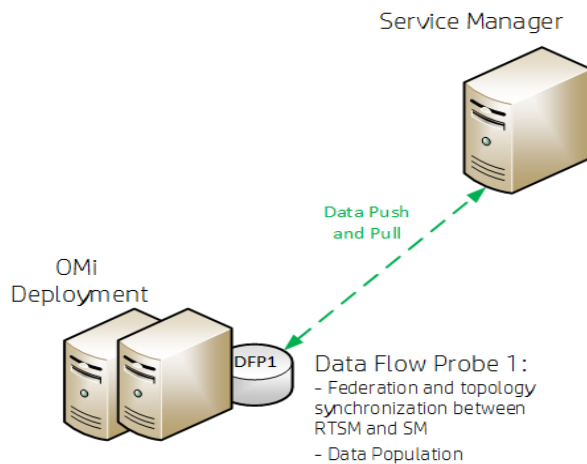
Two variations of integrating Service Manager (SM) with OMi are described below. **Point to point integration** describes the case where the RTSM contained in OMi is used as CMDB. In this case, only one data flow probe is needed (DFP1) which is installed in the OMi deployment.

Integration Using a Universal Configuration Management Database (uCMDB) describes the case where a uCMDB is used. In this case, two data flow probes are needed: the DFP1 is installed on the uCMDB server and the DFP2 in the OMi deployment.

Point to Point Integration

OMi is integrated with Service Manager directly, using OMi's Run Time Service Model (RTSM) as CMDB:

Figure: Point to Point Integration

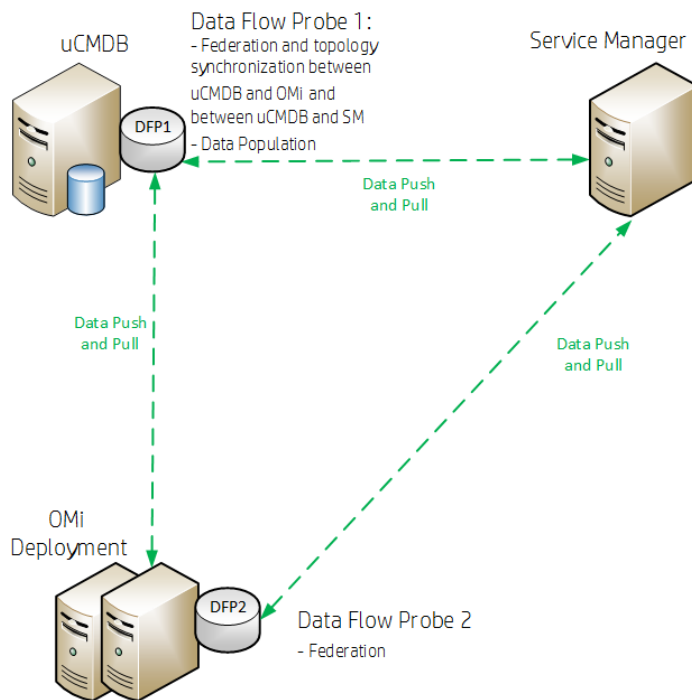


HP recommends to install the Data Flow Probe 1 (DFP1) in the OMi deployment.

Integration Using a Universal Configuration Management Database (uCMDB)

OMi is set up using an external uCMDB:

Figure: Setup OMi with a uCMDB



HP recommends to install the Data Flow Probe 1 (DFP1) on the uCMDB server and the Data Flow Probe 2 (DFP2) in the OMi deployment.

Data Flow Probes

Two different data flow probes need to be installed. Each of the two has a different task:

The DFP1 is necessary for

- Populating the RTSM with CIs (Data Population)
- Federation
- Topology synchronization (CIs) between RTSM and SM in the case of a point to point integration
- *OR*

- Topology synchronization (CIs) between uCMDB and OMi and between uCMDB and SM in case of using an external uCMDB

DFP2 is necessary for federation only.

Note: In general, the information provided in this guide is for integrating OMi with SM 9.3x.

For instructions on integrating OMi with earlier versions of SM, see http://support.openview.hp.com/selfsolve/document/KM1303768/binary/BSM9.12_SM_Integration_Interactive_Docs.html. Download and extract the zip file contents, and then open the **SM_interactive_document.htm** file and follow the guidelines.

The options are as follows:

- **Downtime exchange between OMi and SM.** OMi enables you to forward downtimes (also known as outages) from OMi to SM, and from SM to OMi. The downtime defined in OMi is directed to SM as an incident, and vice versa. For details, see "[Downtime Exchange Between Operations Manager i and Service Manager](#)" on page 77.
- **Incident exchange between SM and OMi.** OMi enables you to forward events from OMi to SM. Forwarded events and subsequent event changes are synchronized back from SM to OMi. You can also drill down from OMi events to SM incidents. For details, see "[Incident Exchange Between Service Manager and Operations Manager i](#)" on page 82.
- **View planned changes and incident details in Service Health.** This integration enables you to view planned changes and incident details in the Changes and Incidents tab in the 360° View page in Service Health. For details, see "[View Changes and Incidents in Service Health Using Standalone HP Universal CMDB](#)" on page 96 and "[View Changes and Incidents in Service Health Using RTSM](#)" on page 111.
- The **Business Impact Report** integration is described in the *Closed Loop Incident Process (CLIP) Guide*. When deployed as part of the OMi solution, Incident Management users can launch an impact report from an incident in context with the incident's affected CI. Service desk agents can validate the updated status of the business impact to categorize and prioritize the incident accordingly. For details, see the CLIP page in the Solutions Portal at:

<http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab1>

Note:

- **Service Manager Query Security.** If you have set up an integration from OMi to SM, there is a CI context menu that enables you to access SM from OMi Service Health. This drill-down option is not available if you have enabled Service Manager query security.
- **Troubleshooting Multiple Domains.** If OMi and SM are in different domains, and you are

using Internet Explorer as your browser, you may need to add the domains to the list of allowed domains in the Privacy tab (**Internet Options > Privacy > Sites**).

Chapter 22: Downtime Exchange Between Operations Manager i and Service Manager

OMi enables you to forward downtimes (also known as outages) from OMi to SM, and from SM to OMi. The downtime defined in OMi is converted to an incident in SM, and vice versa.

This chapter includes the following:

- ["Integration Overview" below](#)
- ["Prerequisites" on the next page](#)
- ["Step 1: Send OMi Downtime Events to SM" on the next page](#)
- ["Step 2: Integrate SM Downtimes with OMi" on page 80](#)

Integration Overview

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

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

In this scenario, you install a data flow probe on the CMDB:

- If you use OMi's RTSM as CMDB, install the data flow probe provided on the OMi installation media.
 - If you use uCMDB as CMDB, install the data flow probe as described in the uCMDB documentation. In this case, the synchronization must also be done from UCMDB to OMi, additionally to synchronizing SM with UCMDB. The RfC creates a planned downtime CI in the CMDB, and the data flow probe DFP1 sends the planned downtime CI to OMi to create a downtime.
- **OMi > SM.** When you define downtimes using OMi, the help desk should be aware of such operational downtimes: After you set up the integration, downtimes in OMi trigger events, which create corresponding incidents in SM.

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

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

Prerequisites

Supported Platforms

To set up the downtime integration, you must meet the following prerequisites:

- Service Manager 9.31 and higher.
- uCMDB (CMS) 9.05 CUP 5 and higher with content pack 11 update 2, or
uCMDB 10.01 or higher with content pack 12 or higher.
- Before deploying the adapter, verify that CP11 or higher is installed. If it is not, install the content pack.
- If the adapter is installed on the RTSM, and the adapter is working behind a reverse proxy, the DPS must have the correct certificates installed to send requests to the reverse proxy.

If you are using a uCMDB as a CMS, make sure that the CMS integration is set up. When it is set up, it serves as the global ID generator.

Global ID Generator

If you are using OMi's RTSM you need to configure the RTSM to be the global ID generator, to enable the downtime integration:

1. Access the following location with your browser: <http://<DPS name>:21212/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Multiple CMDB Instances Services>
2. In the **setAsGlobalIdGenerator()** method, fill the **customerID** parameter with the value of **1**, and click **Invoke**.

Step 1: Send OMi Downtime Events to SM

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

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.

A corresponding forwarding rule that configures forwarding downtime start and end events from OMi to SM must be configured in the Event Forwarding Rule dialog box. The forwarding rule must be based on the ETI Hint, as follows:

- ETI Hint equals ignore case “downtime:start”
- ETI Hint equals ignore case “downtime:end”

For details on how to use the event forwarding mechanism to generate incidents in SM, 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>
Cild	<Affected CI Global ID>
CiHint	GUCMDB:<Affected CI Global ID> UCMDB:<Affected CI ID>
HostHint	GUCMDB:<Related Host Global ID> UCMDB:<Related Host ID>
EtiHint	downtime:start

- **Downtime End**

Event field	OMi Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name> ended at < Downtime End Time>
Key	<OMi Downtime ID>:<Affected CI ID>:downtime-stop
SubmitCloseKey	true
CloseKeyPattern	<OMi Downtime ID>:<Affected CI ID>:downtime-start
EtiHint	downtime:end
LogOnly	true

Step 2: Integrate SM Downtimes with OMi

To enable downtimes defined in SM to be sent to OMi, again, you need to distinguish between the two cases of where the CMDB is:

If you are using OMi's RTSM as CMDB, no further steps are required. See also ["Point to Point Integration" on page 73](#).

If you are using an external uCMDB, you need to install the DFP2 in the OMi deployment. See also ["Integration Using a Universal Configuration Management Database \(uCMDB\)" on page 74](#)

Important:

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

Note:

- The following procedure does not describe the SM > CMS/RTSM connection setup. SM should be configured to create its CIs in the CMS. This procedure connects the adapter between the CMS/RTSM and OMi.
- The default job synch frequency is one minute.

Create a new integration point as follows:

1. Create the integration point credentials:

- a. If you use OMi's RTSM, do the following on your OMi. If you use a CMS, do the following on the uCMDB that fulfills the role of your CMS: Access the Data Flow Probe Setup:

Administration > RTSM Administration > Data Flow Management > Data Flow Probe Setup

Note: You do not need a probe to perform this integration. Nevertheless you create credentials using the Data Flow Probe Setup tab.

- b. Click **Add domain or probe**, and enter a name and description of your choice.
- c. Expand the submenus and select **HTTP protocol**.
- d. Click the **+** sign (**Add new connection details**) and enter the OMi Gateway host name, Port 80, and the OMi username and password. Leave the **Trust** fields blank. When you are done, click **OK** to save the credentials.

2. Create a new integration point:

- a. If you have OMi, do the following on your OMi. If you use a CMS, do the following on your CMS: Access the Integration Studio:

Administration > RTSM Administration > Data Flow Management > Integration Studio

- b. Click **New Integration Point**, enter a name and description of your choice, and select **BSMDowntimeAdapter/SM scheduled Downtime Integration into BSM**.
- c. Enter the following information for the adapter: OMi Gateway hostname and port, the integration point credentials you just created, communication protocol, and the context root (if you have a non-default context root).
- d. Click **OK**, then click the **Save** button above the list of the integration points.

3. You can use the **Statistics** tab in the lower pane to track the number of downtimes that are created or updated. By default, the integration job runs every minute. If a job has failed, you can open the **Query Status** tab and double-click the failed job to see more details on the error.

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

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

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

Chapter 23: Incident Exchange Between Service Manager and Operations Manager i

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.

Note: HP recommends this integration option for new integrations with SM. However, existing integrations that use other integration options are still supported.

This chapter includes the following:

- ["Step 1: Configure the SM Server as a Connected Server" below](#)
- ["Step 2: Configure an Event Forwarding Rule" on page 86](#)
- ["Step 3: Configure a URL Launch of the Event Browser from SM" on page 87](#)
- ["Step 4: Configure a URL Launch of SM from the Event Browser" on page 88](#)
- ["Step 5: Configure the SM Server" on page 89](#)
- ["Step 6: Mapping and Customization" on page 90](#)
- ["Step 7: Test the Connection" on page 91](#)
- ["Step 8: Synchronize Attributes" on page 92](#)
- ["Tips for Customizing Groovy Scripts" on page 93](#)

Step 1: Configure the SM Server as a Connected Server

Synchronizing events and event changes between OMi and SM incidents requires configuring a connected server within OMi to correctly identify the target SM instance. The first step to achieve this is to configure HP Service Manager as a target connected server in the Connected Servers manager.

For full details about how to configure a connected server, see the OMi Administration Guide.

Note: Before you continue with the below procedure, set up an integration user with a user name and password in SM. This is the user name and password needed by OMi to access the SM target server.

To configure the SM 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 SM server. By default, the Name field is filled automatically. For example, if you enter *Service Manager 1* as the Display Name for the target SM 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 SM 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, enter the Fully Qualified DNS Name of the SM 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 SM Groovy script adapter **sm:ServiceManagerAdapter**.

Note: In case the **Test Connection** fails and the error indicates that there could be a problem with timeout, increase the timeout value. Otherwise, you can leave the default timeout value.

- 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 SM 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 SM.
 - 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 SM side for the integration with OMi.

To find the port number to enter:

- If you are using default ports in SM, 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 SM 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 SM 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 SM, in addition to automatically generating SM incidents from OMi events, you need to specify the fully qualified DNS name and port of the SM system into which you want to perform the incident drilldown.

Note: To enable incident drilldown to SM, you must install a web tier client for your SM server according to your SM 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 SM.

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

Select or clear the **Use Secure HTTP** check box according to your configuration. In case the SM server is configured for SSL access, click the **Retrieve from Server** link to import the certificate from the SM server to allow SSL encryption.

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

8. To enable event changes to be synchronized back from SM to OMi, you must provide credentials for the SM 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 SM 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 SM server to communicate with the server hosting OMi. This password is associated with the server name (`Service_Manager_1`) you configured in SM.

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 SM 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 SM 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 SM system.

An example of a connected server ID is as follows:

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

Step 2: Configure an Event Forwarding Rule

The next step is to configure an event forwarding rule that determines which events are forwarded automatically to SM.

For details about configuring filters, see the OMi Administration Guide.

To configure a forwarding rule, follow these steps:

1. Navigate to the Forwarding Rules manager:

Administration > Event Processing > Automation > Event Forwarding

2. Click the **New Item** button to open the Create New Event Forwarding Rule dialog box.
3. Under General, in the **Display Name** field, enter a name for the forwarding rule, in this example `Forward Critical (Sync and Transfer Control)`.

Optional. Enter a description for the forwarding rule you are creating.

4. Under Condition, click the browse button next to the Event Filter field. The Select an Event Filter dialog box opens.

In the Select an Event Filter dialog box, do one of the following:

- Select an existing filter
- Create a new filter as follows:
 - i. Click the **New** button to open the Filter Configuration dialog box. You can choose between **New Simple Filter** or **New Advanced Filter**.
 - ii. 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**.
 - iii. You should see your new filter in the Select an Event Filter dialog box (select it, if it is not already highlighted).

Click **OK**.

5. Under Target Servers, select the target connected server you configured in "[Step 1: Configure the](#)

[SM Server as a Connected Server" on page 82](#). In this example, this is Service Manager 1.

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 SM.

Click **OK**.

6. Make sure the **Activate Rule after creation** check box is selected. A rule must be active in order for its status to be available in SM.

Step 3: Configure a URL Launch of the Event Browser from SM

Before operators are able to perform event drill-down from SM into the OMi user interface using a URL launch of the Event Browser, the operators must be set up as valid users with appropriate permissions in OMi:

User account requirements

- If Single Sign-On (SSO) authentication is configured, set up each user in OMi with the *same* user name that is used by the SM operator to log on to SM and to perform the URL call. (The password of each OMi user can be any string, but not empty.) After successfully logging on to SM, the OMi users can launch the OMi Event Browser without further authentication.

For details on setting up SSO, see **System Administration > Integrations > Service Manager integration methods and tools > Integration Manager > Using LW-SSO with integrations** in the SM documentation library.

- If SM is not configured to use SSO authentication, set up each user with the *same* user name that is used by the SM operator and specify a valid password. The users are required to enter their user name and password when launching the OMi Event Browser.

Required user permissions

You must grant the permission `Events assigned to user` including the required actions to each OMi user. To do so, 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.

Note: Without valid user names, or if a user does not have the required viewing permissions, any attempt to perform a URL launch of the OMi Event Browser from SM results in an empty browser window.

Step 4: Configure a URL Launch of SM from the Event Browser

To be able to perform a URL launch of SM from the OMi Event Browser using the web tier client, perform the following:

1. Navigate to Connected Servers:

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 SM 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 SM 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 SM as a target connected server in the Connected Servers manager. For details, see ["Step 1: Configure the SM Server as a Connected Server" on page 82](#).

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

Step 5: Configure the SM Server

The next step describes how to configure the SM server to integrate with OMi.

Note: If you want to configure more than one OMi server, you need to increase the connection count on the SM side:

System Administration > Integrations > HP Business Service Management (BSM) > Incident Exchange (OMi - SM) integration > Incident Exchange (OMi - SM) integration setup > Configure the Instance Count setting in the SM-OMi integration template.

This functionality is only available for SM 9.34 and higher.

To configure the SM server, complete the following steps in the HP Service Manager user interface:

1. From the left hand pane, navigate to:

Tailoring > Integration Manager

2. Click **Add** to add a new configuration.
3. Select the **SMOMi** integration template from the Integration Template field. Click **Next**.
4. *Optional.* Change the log level to the desired value.

Optional. Change the description, for example, to *This is for SMOMi integration.*

Specify **Interval Time (s)** and **Max Retry Times**, and then click **Next**.

5. In the General Parameters tab, replace the existing entries with the following values:

Name	Value	Category
omi.server.url	http://<OMi_gateway_FQDN>:<port>/opr-gateway/rest/synchronization/event/	General

Name	Value	Category
username	Service_Manager_1 (This is the name of the SM target server you configured in " Step 1: Configure the SM Server as a Connected Server " on page 82).	Header
omi.eventdetail.baseurl	http://<OMi_gateway_FQDN>:<port>/opr-web/opr-evt-details.jsp?eventId=	General
omi.mgr.id	The ID obtained when reentering the Connected Servers window.	General

6. In the Secure Parameters tab, set the password to the one you specified in the Incoming Connection page when configuring the target connected server in "[Step 1: Configure the SM Server as a Connected Server](#)" on page 82. In our example, this is HPqwer1_.

Click **Next**.

7. In the Integration Instance Fields dialog box, click **Next**.
8. In the Integration Instance Mapping dialog box, click **Finish**.

Note: Ensure that the rule is active. To make the rule active, select the rule and click **Enable**.

Step 6: Mapping and Customization

You can add your own custom attributes in the Groovy script selected for the SM server in the Connected Servers pane, and then map these custom attributes to the appropriate field in SM. For details about groovy scripting, see the OMi Extensibility Guide.

You can also change how attributes are mapped from OMi to SM. The mapping is done in the BDM Mapping Manager in SM:

System Administration > Ongoing Maintenance > BDM Mapping Management

For details about mapping attributes, see the HP Service Manager online help:

System Administration > Integrations > Service Manager integration methods and tools > BDM Mapping Management

Step 7: Test the Connection

To test the connection, send an event to the server hosting OMi that matches the filter you defined (in our example filter, the severity value is `Critical`), and then verify that the event is forwarded to SM as expected.

To test the connection, do the following:

1. On the Gateway Server system running OMi, open an Event Browser.
2. On the system running OMi, open a command prompt and change to the following directory:

```
<OMi_HOME>\opr\support
```

3. Send an event using the following command:

```
sendevent -s critical -t test111-1
```

4. Verify that the event appears in the OMi Event Browser.
5. Select the **Forwarding** tab.
6. In the External Id field, you should see a valid SM incident ID.
7. Verify that the incident appears in the Incident Details in HP Service Manager:

If the event drill-down connection is configured correctly, click the hyperlink created with the incident ID. A browser window opens, which takes you directly to the incident in the Incident Details in HP Service Manager.

If the event drill-down connection is not configured, do the following:

- a. In the Forwarding tab in the OMi Event Browser, copy or note the incident ID from the External Id field.

- b. In the HP Service Manager user interface, navigate to:

Incident Management > Search Incidents

- c. Paste or enter the incident ID in the Incident Id field.
- d. Click the **Search** button. This takes you to the incident in the Incident Details.

8. Close the incident in HP Service Manager.
9. Verify that the change in the state of the incident (it is now `closed`) is synchronized back to OMi. You should not be able to see the event that was closed in SM in the active Event Browser, but it should now be in the History Browser.

Step 8: Synchronize Attributes

Not all attributes are synchronized back from SM to OMi by default. When the SM incident is initially created from an OMi event, event attributes are mapped to the corresponding SM incident attribute. Out of the box, after the initial incident creation, whenever the incident or event subsequently changes, only a subset of the changed event and incident attributes are synchronized. The following describes how to customize the list of attributes to synchronize upon change.

Unidirectional Synchronization: OMi to SM

The following attributes are transferred to SM from OMi on a one-time basis, that is, when the event was initially created, and the transfer of control of the event was configured in the Connected Servers manager.

These attributes support bidirectional synchronization, but are disabled out-of-the-box:

- Title
- Severity
- Priority
- Operator: the operator assigned to the event who forwarded the event
- Category
- Subcategory
- Related CI

For the above attributes, there is no back synchronization from SM to OMi.

Bidirectional Synchronization

Attributes that support bidirectional synchronization between OMi and SM are:

- Description
- Lifecycle state (the state is only updated when the state changes to closed)
- Solution
- OMi event annotations are synchronized to SM activity log
- Contents under the Forwarding tab in the Event Details

Attribute Synchronization using Groovy Scripts

If you want to change the out-of-the-box behavior regarding which attributes are updated, you can specify this in the Groovy script used on the OMi side for synchronization or incident creation. In the Groovy script, you can specify which fields are updated in SM, and which fields are updated in OMi. You can also specify custom attributes in the Groovy script.

Tips for Customizing Groovy Scripts

This section provides some tips about customizing Groovy scripts. It contains a few selected examples of what you can customize. To see further items that can be modified, see the configuration section of a Groovy script.

In the configuration section of the Groovy script, you can define and modify the attributes that are to be synchronized between OMi and SM. The configuration section of the Groovy script also contains the default value mappings for lifecycle state, severity, and priority. You can also modify these, and it is possible to define the mappings for in-going and out-going requests differently.

More advanced configuration can be done in other parts of the Groovy script if required.

The beginning and the end of the configuration section of the Groovy script is marked as follows:

```
//  
  
// configuration section to customize the Groovy script  
// BEGIN  
  
...  
  
...  
  
//  
  
// configuration section to customize the Groovy script  
// END
```

Note: Modifications to Groovy scripts are not overwritten by patches and hotfixes. Your customized version of a script will remain after an update or a patch. If you want to use the newer version of a script, make a copy of your version, revert back to the predefined version, and then reapply your changes.

The mapping from OMi to SM is compliant to BDM 1.1 incident web service specifications. The mapping of the BDM 1.1 incident web service to SM is specified in SM in the BDM Mapping Manager. For more information about the BDM Mapping Manager, see the BDM Mapping Manager section of the HP Service Manager online help.

Controlling Attribute Synchronization

You can control how updates to certain attributes are synchronized between OMi and SM by setting

some Boolean variables to true or false.

Examples:

- `SyncAllProperties` variable. By default, it is false. If you set it to true, all properties will be synchronized in both directions. The other variables will be ignored.
- `private static final SyncTitleToSMOnUpdate = false;`

This line of the Groovy script disables the synchronization of changes to the title made in OMi to SM.

- `private static final Boolean SyncTitleToOPROnUpdate = false;`

This line of the Groovy script disables the synchronization changes to the title made in SM to OMi.

The title is a required attribute in SM, and it is set, independently of the flags above, using the title given in OMi during the creation of the incident.

Mapping OPR Lifecycle States to BDM Lifecycle States

Individual OPR event state and SM incident status changes may be selected for synchronization. Out of the box, only the "closed" state is synchronized in both directions. To change this behavior, add the desired states to the appropriate list, `SyncOPRStatesToSM` or `SyncSMStatusToOPR`.

Examples:

- `private static final Set SyncOPRStatesToSM = ["closed", "in_progress", "resolved"]`
- `private static final Set SyncSMStatusToOPR = ["closed", "resolved"]`

In the example, the OPR event lifecycle states `closed`, `in_progress`, and `resolved` are synchronized to the SM incident status, and SM incident statuses `closed` and `resolved` are synchronized to the OPR event state.

Note: The special state "*" denotes all states, so to synchronize all OPR event states to the SM incident status property, specify the following:

```
private static final Set SyncOPRStatesToSM = ["*"]
```

Additionally, two maps are used to specify the mapping of the OPR event lifecycle state to the BDM incident status. The maps are named `MapOPR2SMStatus` and `MapSM2OPRState`. Out of the box, all possible states have a mapping.

Examples:

- `private static final Map MapOPR2SMStatus = ["open": "open", "in_progress": "work-in-progress", "resolved": "resolved", "closed": "closed"]`
- `private static final Map MapSM2OPRState = ["accepted": "open", "assigned":`

```
"open", "open": "open", "reopened": "open",  
  
"pending-change": "in_progress", "pending-customer": "in_progress", "pending-  
other": "in_progress",  
  
"pending-vendor": "in_progress", "referred": "in_progress", "suspended": "in_  
progress",  
  
"work-in-progress": "in_progress", "rejected": "resolved", "replaced-problem":  
"resolved",  
  
"resolved": "resolved", "cancelled": "resolved", "closed": "closed"]
```

Syntax Errors

If you get a syntax error when customizing your Groovy scripts, you will get an event in the event browser with a detailed description of the error. In addition, you may view the `opr-event-sync-adapter.log` log file for information about how to resolve the error. You can find this log file at the following location:

```
<Gateway Server root directory>/log/opr-event-sync-adapter.log
```

Chapter 24: View Changes and Incidents in Service Health Using Standalone HP Universal CMDB

This integration enables you to view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health when you are using a standalone HP Universal CMDB.

Note: Beginning with UCMDB version 9.05, a new SM adapter (ServiceManagerAdapter9-x) is supplied with UCMDB out of the box, in addition to the legacy adapter (ServiceManagerAdapter7-1):

- For SM versions 9.3x, use ServiceManagerAdapter9.xx.
- For SM versions 9.2x, use ServiceManagerAdapter7-1.

This chapter includes the following:

- ["Prerequisite" on the next page](#)
- ["Step 1: Load the .unl File to Provide External Access to Service Manager" on the next page](#)
- ["Step 2: Configure the Service Manager Adapter Time Zone" on page 98](#)
- ["Step 3: Configure UCMDB to Generate Global IDs" on page 99](#)
- ["Step 4 \(for SM 9.2x only\): Add a Domain" on page 100](#)
- ["Step 5: Configure SM Adapter in UCMDB" on page 101](#)
- ["Step 6: Configure the SM-UCMDB Integration: Create an Integration Point" on page 101](#)
- ["Step 7: Configure the SM-UCMDB Integration: Set Up Data Push Jobs" on page 102](#)
- ["Step 8: Configure the SM-UCMDB Integration: Run Data Push Jobs" on page 103](#)
- ["Step 9: Configure the SM-UCMDB Integration: Add UCMDB Connection Information to SM" on page 104](#)
- ["Step 10: Configure the OMi-UCMDB Integration: Deploy CMS_to_RTSM_Sync.zip on UCMDB" on page 104](#)
- ["Step 11: Configure the OMi-UCMDB Integration: Create an Integration Point on OMi" on page 105](#)
- ["Step 12: Configure the OMi-UCMDB Integration: Create an Integration Point on the CMS" on page 107](#)

- ["Step 13 \(Optional\): Add CI Types to the Service Health Changes and Incidents Component" on page 109](#)
- ["View Changes and Incidents in Service Health Using Standalone HP Universal CMDB" on the previous page](#)
- ["Troubleshooting" on page 110](#)

Prerequisite

Trusted Sign-on and LW-SSO. If you want SM to use the SSL-based Trusted Sign-on protocol and LW-SSO, configure it according to the instructions in the HP Service Manager online help.

Step 1: Load the .unl File to Provide External Access to Service Manager

To enable OMi to query incidents and changes, you must apply the fix described in <http://support.openview.hp.com/selfsolve/document/KM1015767>. This is required because the .unl file expects the length of the name attribute in the EXTACCESSM1 table to be 50 in the database, but its default out-of-the-box length is 100.

Therefore, you must reduce the size of the attribute, load the .unl file, and then increase the size again:

Note: These steps are for the SQL Server, but you can see the KM document for the equivalent Oracle syntax.

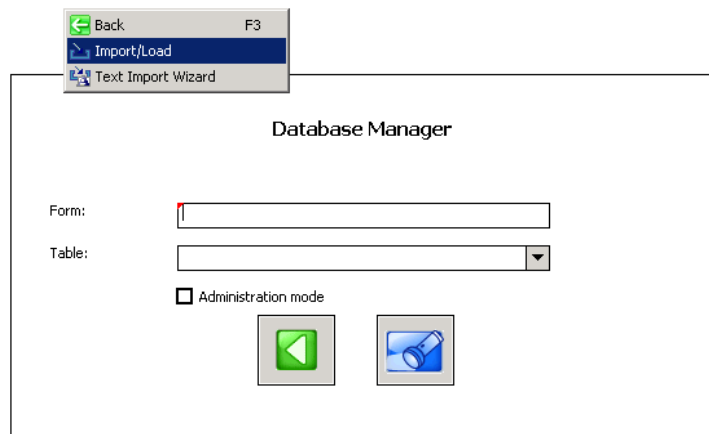
1. Reduce the length of the name attribute in the EXTACCESSM1 table:
 - a. Database field truncation may result in data loss if data in the field exceeds the default length, so first check the size of the data in the field:

```
Select NAME, LEN(NAME) from EXTACCESSM1 order by 2 desc
```

- b. Reduce the size of the field:

```
alter table EXTACCESSM1 alter column NAME VARCHAR(50)
```

2. In SM, type **db** in the command line text widget in the menu bar at the top of the client display.
3. Right-click the white background and select **Import/Load** from the context menu that appears.



4. Click the folder icon at the end of the File Name box and navigate to the .unl file on the DPS:

- **Windows:** %TOPAZ_HOME%\odb\runtime\fcmdb\CodeBase\ServiceManagerAdapter7-1\ucmdbIntegration7_1x.unl
- **Linux:** /opt/HP/BSM/odb/runtime/fcmdb/CodeBase/ServiceManagerAdapter7-1\ucmdbIntegration7_1x.unl

Select the file, and click **Open**.

5. Click **Load FG** on the toolbar to load the file. If you receive a message saying that the file you are loading will change the keys, click **Yes**.
6. Increase the size of the field back to what it was originally:

```
alter table EXTACCESSM1 alter column NAME VARCHAR(100)
```

Step 2: 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**.
2. In the **Date Info** tab, check the Time Zone setting.
3. On the DPS, open the following file:
 - **Windows:** %TOPAZ_HOME%\odb\runtime\fcmdb\CodeBase\<ServiceManagerAdapter9-x or ServiceDeskAdapter7-1>\serviceDeskConfiguration.xml

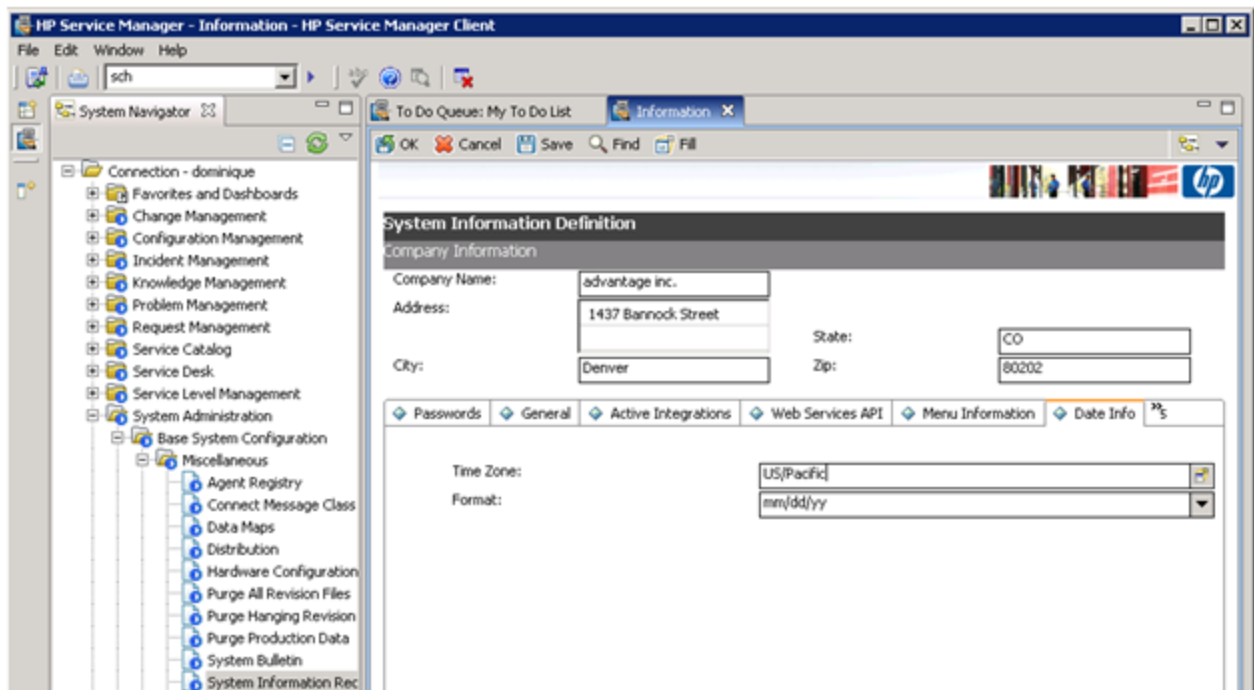
- **Linux:** /opt/HP/BSM/odb/runtime/fcddb/CodeBase/<ServiceManagerAdapter9-x or ServiceDeskAdapter7-1>/serviceDeskConfiguration.xml

4. 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/Pacific</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. Restart the corresponding server to make the change take effect. (If you changed the time zone on SM, restart the SM server; if you changed the time zone on OMi, restart the OMi server.)

Step 3: Configure UCMDB to Generate Global IDs


1. On the UCMDB server, navigate to:

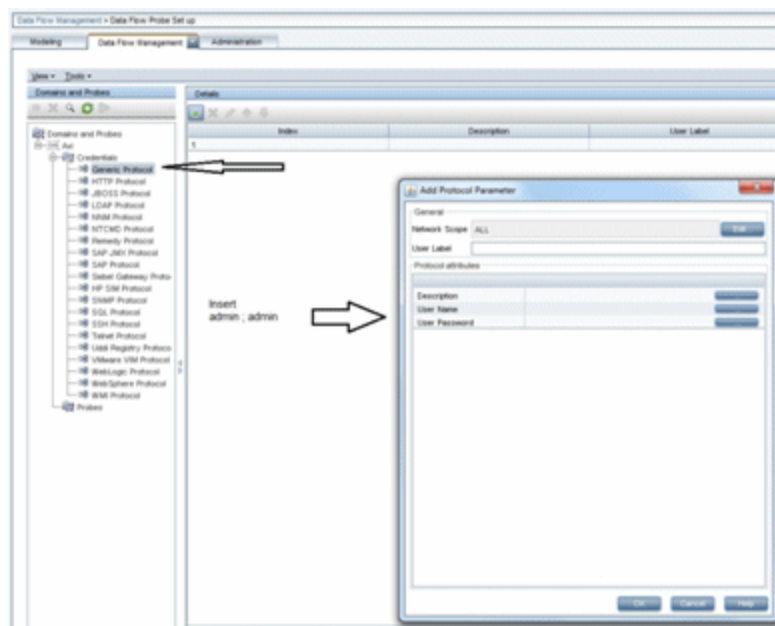
<http://<UCMDB server name>:21212/jmx-console>

2. Enter the user name and password.
3. In the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.
4. For **setAsGlobalIdGenerator**, click **Invoke**.
5. On the DPS, open the following file:
 - **Windows:** %TOPAZ_HOME%\odb\runtime\fcmdb\CodeBase\<ServiceManagerAdapter9-x or ServiceManagerAdapter7-1>\sm.properties
 - **Linux:** /opt/HP/BSM/odb/runtime/fcmdb/CodeBase/<ServiceManagerAdapter9-x or ServiceManagerAdapter7-1>/sm.properties
6. Set the **use.global.id** parameter to **true**.

For SM versions 9.2x, proceed with the next step. For SM versions 9.3x, skip to ["Step 5: Configure SM Adapter in UCMDB" on the next page](#).

Step 4 (for SM 9.2x only): Add a Domain

1. In OMi, select **Administration > RTSM Administration > Data Flow Management > Data Flow Probe Setup**.
2. In the **Domains and Probes** pane, click .
3. In the **Add New Domain** dialog box, enter a new domain name, and then click **OK**. This creates a new domain and its protocols.
4. Within the domain you added, select **Credentials > Generic Protocol**, and then click the **Add new connection details** button in the right pane. In the **Add Protocol Parameter** dialog box that opens, insert the SM administrator credentials.



Step 5: Configure SM Adapter in UCMDB

1. Within the UCMDB user interface, access **Data Flow Management > Adapter Management**.
2. In the resources window, select **ServiceManagerAdapter9-x** or **ServiceManagerAdapter7-1 > Configuration files**.
3. Select **ServiceManagerAdapter9-x/sm.properties** or **ServiceManagerAdapter7-1/sm.properties**.
4. In the window on the right side of the screen, modify the **use.global.id** parameter, set it to **false**, and click **OK**.

Step 6: Configure the SM-UCMDB Integration: Create an Integration Point

1. Within the UCMDB user interface, select **Data Flow Management > Integration Studio**.
2. In the Integration Point pane, select **Create New Integration Point**. 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.
Adapter	<user defined>	Select the appropriate adapter for the version of SM that you are using.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the SM server.
Port	<user defined>	The port through which you access SM.
Credentials	<user defined>	<ul style="list-style-type: none"> ■ For SM 9.2x, select the user credentials created in "Step 4 (for SM 9.2x only): Add a Domain" on page 100. ■ For SM 9.3x, in the default domain select Generic Protocol, and enter the credentials of the SM administrator.
Probe Name (for ServiceManagerAdapter9-x only)	<user defined>	If you are using ServiceManagerAdapter9-x, select the probe which reports to CMS (see "Prerequisite" on page 97).

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

If your SM backend server (SM Tomcat server) is configured to accept SSL connections, the port setting is ignored and you must configure URL Override. For details, see the UCMDB documentation.

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**, **Problem**, and **RequestForChange** are selected.

Step 7: Configure the SM-UCMDB Integration: Set Up Data Push Jobs

Depending on your adapter version, perform the following:

For ServiceManagerAdapter9-x:

1. Edit the **SM Push** job, and select **Scheduler Definition**.
2. For the **Repeat** field, you can select **Changes Sync/All Data Sync**.
3. Set the **Repeat Every** field to **1 Day**, and click **OK**.

For ServiceManagerAdapter7-1:

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

Step 8: Configure the SM-UCMDB Integration: Run Data Push Jobs

1. In the Integration Point pane, select the correct integration.
2. Select the **Data Push** tab. The Job Definition pane is displayed.
3. Select your job and click **Synchronize All** to run the push job.

Note: For ServiceManagerAdapter7-1, run this first for the **SM History-based Push** job, then repeat for the **SM Topology Comparison Push** job.

4. When the Confirm synchronizing window is displayed, click **Yes**.
5. Click the **Statistics** tab to view the progress of the synchronization.
6. Click **Refresh** to view the updated synchronization status.

Step 9: Configure the SM-UCMDB Integration: Add UCMDB Connection Information to SM

1. Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.
2. Log on to your SM system as an administrator.
3. Select **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
4. Select the **Active Integrations** tab.
5. Select the **HP Universal CMDB** option. The form displays the UCMDB Web service URL field.
6. In the UCMDB Web service URL field, enter the URL to the UCMDB Web service API. The URL has the following format:

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

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

Step 10: Configure the OMi-UCMDB Integration: Deploy CMS_to_RTSM_Sync.zip on UCMDB

1. Copy the `CMS_to_RTSM_Sync.zip` file located on the OMi-DPS machine file system under **%TOPAZ_HOME%\odb\conf\factory_packages** (Windows) or **/opt/HP/BSM/odb/conf/factory_packages** (Linux) to the file system on the UCMDB machine.
2. Within the UCMDB user interface, select the **Administration** tab.
3. Select **Package Manager > Deploy Packages to server (from local disk)**.
4. Click the **Add** button and select the **CMS_to_RTSM_Sync.zip** file through the file system browser.
5. Select **Deploy**.

Step 11: Configure the OMi-UCMDB Integration: Create an Integration Point on OMi

1. Within the OMi user interface, select **Administration > RTSM Administration > Data Flow Management > Integration Studio**.
2. In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens. Enter the following:

Recommended		
Name	Value	Description
Integration Name	<user defined>	The name you give to the integration point.
Adapter	UCMDB 9.x	Select the adapter type from the drop-down list.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the UCMDB server, load balancer, or reverse proxy.
Port	<user defined>	The port through which you access UCMDB, load balancer, or reverse proxy.
Credentials	<user defined>	<p>If credentials appear in the Credentials column, select them.</p> <p>If no credentials appear, select Generic Protocol and click the Add new connection details for selected protocol type button.</p> <p>Enter the following information:</p> <ul style="list-style-type: none"> ■ Description. Enter UCMDB. ■ User Name. Enter the UCMDB user name. The default value is admin. ■ User Password. Enter and confirm a password.
Probe Name (for ServiceManagerAdapter9-x only)	<user defined>	If you are using ServiceManagerAdapter9-x, select the probe which reports to <i>OMi</i> (see "Prerequisite" on page 97).

3. Click the **Add** icon on the right side of the window and add Job definitions as follows:
 - a. Name the **Job definition**.
 - b. Select the **Allow Delete** check box.
 - c. Click the **Add** icon in the Job definition window.
 - d. From the pop-up window, browse to **root - CMS sync** and select the **ActiveDirectory_sync** job and click **OK**.
 - e. Select the **Scheduler definition** check box.
 - f. In the Repeat window, select **Cron**.
 - g. For the Cron expression, enter the following string: *** 0/10 * * * ? ***.
 - h. Adjust other settings as needed.
 - i. When finished, click **OK** and save the integration.
 - j. Repeat steps **a** to **i** and configure the following jobs:
 - **FailoverCluster_Sync**
 - **IIS_Sync**
 - **BusinessAndFacilities_Sync**
 - **ExchangeServer_Sync**
 - **Virtualization_Sync**
 - **Credentials_Sync**
 - **Basicinfrastructure_Sync**
 - **J2EE_Sync**
 - **SAP_Sync**
 - Optionally, also configure **IIS, Exchange, J2EE and SAP**
4. Browse to UCMDB on port 21212 (for example, http://<DPS_host>.<domain>:21212), and select the **JMX Console**.
5. Log on to the JMX console.
6. From the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.

7. Invoke:
 - a. **setAsGlobalIdGenerator** and verify it succeeded.
 - b. **getGlobalIdGeneratorScopes** and verify it succeeded.
8. Within OMi, access **Administration > RTSM Administration > Data Flow Management > Integration Studio**.
9. Select the Integration Point that you have configured.
10. In the Job definition section, click **Synchronize All** to run the synchronization.

The Integration Point should be active and the jobs are displayed properly.

Step 12: Configure the OMi-UCMDB Integration: Create an Integration Point on the CMS

1. Log on to UCMDB and select **Data Flow Management > Integration Studio**.
2. In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens. Enter the following:

	Recommended	
Name	Value	Description
Integration Name	<user defined>	The name you give to the integration point.
Adapter	UCMDB 9.x	Select the adapter type from the drop-down list.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name of the OMi server, load balancer, or reverse proxy.
Port	<user defined>	The port through which you access OMi, load balancer, or reverse proxy.

Name	Recommended Value	Description
Credentials	<user defined>	<p>If credentials appear in the Credentials column, select them.</p> <p>If no credentials appear, select Generic Protocol and click the Add new connection details for selected protocol type button.</p> <p>Enter the following information:</p> <ul style="list-style-type: none"> ■ Description. Enter UCMDB. ■ User Name. Enter the UCMDB user name. The default value is admin. ■ User Password. Enter and confirm a password.
Probe Name (for ServiceManagerAdapter9-x only)	<user defined>	<p>If you are using ServiceManagerAdapter9-x, select the probe which reports to the CMS (see "Prerequisite" on page 97).</p>

3. Click the **Add** icon on the right side of the window and add Job definitions as follows:
 - a. Name the **Job definition**.
 - b. Select the **Allow Delete** check box.
 - c. Click the **Add** icon in the Job definition window.
 - d. From the pop-up window, browse to **root - CMS sync** and select the **ActiveDirectory_sync** job and click **OK**.
 - e. Select the **Scheduler definition** check box.
 - f. In the Repeat window, select **Cron**.
 - g. For the Cron expression, enter the following string: *** 0/10 * * * ? ***.
 - h. Adjust other settings as needed.
 - i. When finished, click **OK** and save the integration.

- j. Repeat steps **a** to **i** and configure the following jobs:
 - **FailoverCluster_Sync**
 - **IIS_Sync**
 - **BusinessAndFacilities_Sync**
 - **ExchangeServer_Sync**
 - **Virtualization_Sync**
 - **Credentials_Sync**
 - **Basicinfrastructure_Sync**
 - **J2EE_Sync**
 - **SAP_Sync**
 - Optionally, also configure **IIS**, **Exchange**, **J2EE** and **SAP**
4. Browse to UCMDB on port 8080 (for example, <http://yourUCMDBhost.domain:8080>), and select the **JMX Console**.
5. Log on to the JMX console.
6. From the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.
7. Invoke:
 - a. **setAsGlobalIdGenerator** and verify it succeeded.
 - b. **getGlobalIdGeneratorScopes** and verify it succeeded.
8. Within UCMDB, access **Data Flow Management > Integration Studio**.
9. Select the Integration Point that you have configured.
10. In the Job definition section, click **Synchronize All** to run the synchronization.

The Integration Point should be active and the jobs are displayed properly.

Step 13 (Optional): Add CI Types to the Service Health Changes and Incidents Component

By default, OMi Service Health displays information on incidents and requests for change 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 procedure described in ["How to Customize the Changes and Incidents Component" on page 120](#).

Result

You can now view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health.

Both products can now share information and data.

Troubleshooting

If you are not seeing expected incidents in OMi, perform the following:

1. On the Data Processing Server, search the `odb\odb\Error.log` file for **Error Code 802**.
2. In this error message, locate the following string: **property [<category or incident_status>=<attribute value>[STRING]] is defined as attribute**.

This indicates that a certain attribute value is missing in RTSM.
3. Access **RTSM Administration > CI Type Manager**.
4. From the **CI Types** menu, select **System Type Manager**, and open **Category** or **Incident Status** (depending on the error message) for editing.
5. Click the Add button (+), and add the missing attribute value (exactly as it appears in the error message) to the list of values.

Chapter 25: View Changes and Incidents in Service Health Using RTSM

This integration enables you to view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health when you are working with RTSM. For details, see the *OMi User Guide*.

This chapter includes the following:

- ["Prerequisite" below](#)
- ["Step 1: Configure the Service Manager Adapter Time Zone" below](#)
- ["Step 2: Create an Integration User Account in Service Manager" on page 113](#)
- ["Step 3: Add the OMi Connection Information in SM" on page 114](#)
- ["Step 4: Create an Integration Point in OMi" on page 114](#)
- ["Step 5: Create New Jobs to Synchronize Between OMi and SM" on page 116](#)
- ["Step 6: Run the Job" on page 116](#)
- ["Step 7: Test the Configuration" on page 116](#)
- ["Step 8 \(Optional\): Add CI Types to the Service Health Changes and Incidents Component" on page 119](#)
- ["Troubleshooting" on page 119](#)

Prerequisite

If you are using SM versions 9.3x, before you begin, you must install a data-flow probe with the OMi Gateway Server as its target. When you configure the integration point, you will select this probe for the integration.

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**.
2. In the **Date Info** tab, open the following file:

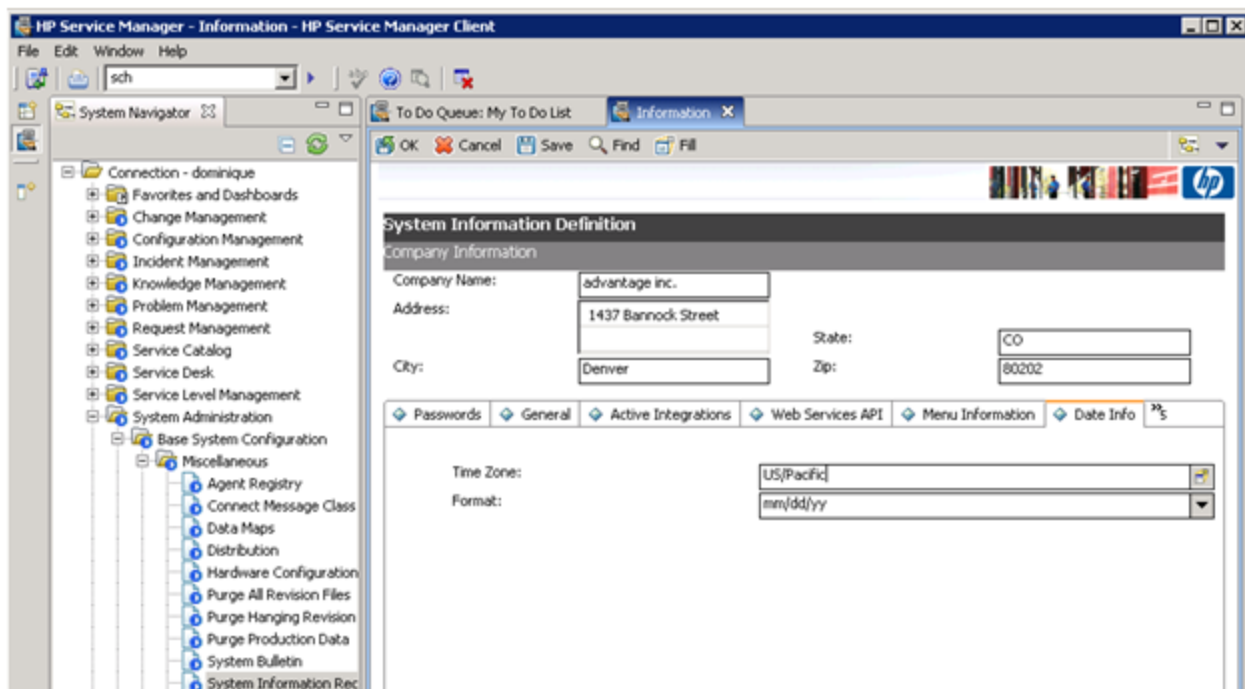
- **Windows:** %TOPAZ_HOME%\odb\runtime\fcmdb\CodeBase\<ServiceManagerAdapter9-x or ServiceDeskAdapter7-1>\serviceDeskConfiguration.xml
- **Linux:** /opt/HP/BSM/odb/runtime/fcmdb/CodeBase/<ServiceManagerAdapter9-x or ServiceDeskAdapter7-1>/serviceDeskConfiguration.xml

3. 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/Pacific</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).



4. Restart the corresponding server to make the change take effect. (If you changed the time zone on SM, restart the SM server; if you changed the time zone on OMi, restart the OMi server.)

Step 2: Create an Integration User Account in Service Manager

This integration requires an administrator user account for OMi to connect to SM. This user account must already exist in both OMi and SM.

To create a dedicated integration user account in SM:

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

The system administrator account displays.

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

The integration user account is created. Later you will need to add this user account (user name/password) in RTSM, and then specify this user account in the **Credentials ID** field when creating an integration point in RTSM administration.

Step 3: Add the OMi Connection Information in SM

The integration requires the OMi connection information to obtain CI attribute information from the OMi system, and display it in the Actual State section in the SM configuration item form.

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

Replace <UCMDB server name> with the host name of your OMi server, and replace <port> with the communications port your OMi server uses.

6. In **UserId** and **Password**, type the user credentials required to manage CIs on the OMi system. For example, the out-of-the-box administrator credentials are **admin/admin**.
7. Click **Save**. SM displays the message: **Information record updated**.
8. Log out of the SM system.
9. Log back into the SM system with an administrator account. The **Actual State** section will be available in CI records pushed from OMi.

Step 4: Create an Integration Point in OMi

A default RTSM installation already includes the `ServiceManagerAdapter9-x` package. To use the integration package, you must create an integration point listing the connection properties for the integration.

To create an integration point, follow these steps:

1. Create a user in OMi and set the RTSM Permissions in the Create Role page. For details about creating and configuring users, groups, and roles in OMi, see the OMi Administration Guide.
2. In OMi, select **Administration > RTSM Administration > Data Flow Management > Integration Studio**.

3. In the Integration Point pane, select **Create New Integration Point**. 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.
Adapter	<user defined>	Select HP BTO 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 "Step 2: Create an Integration User Account in Service Manager" on page 113 , and then select it. This account must exist in both Service Manager and OMi.
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.

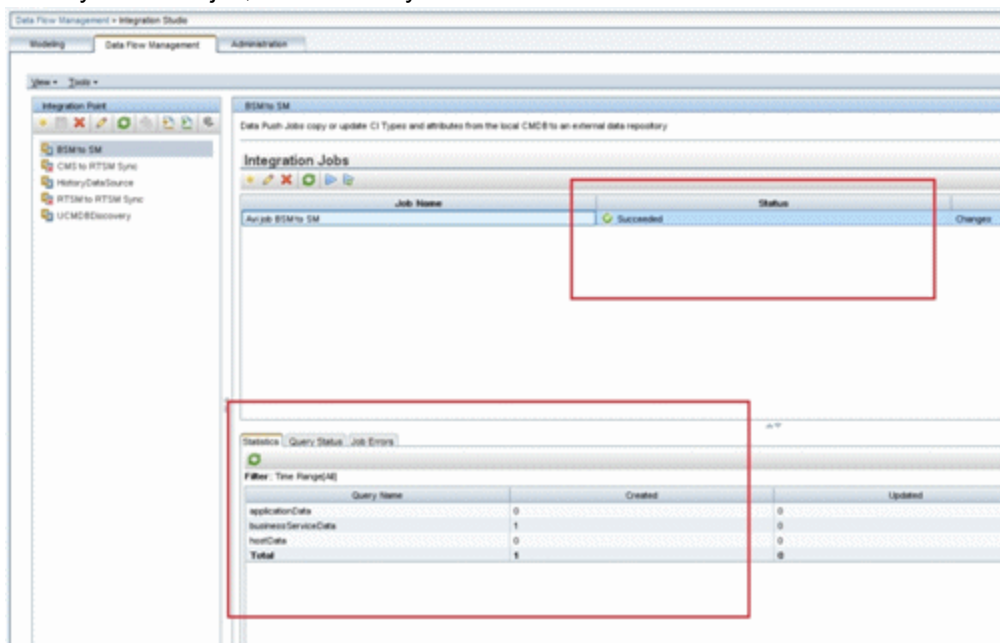
4. In the **Integration Point** pane, click the Integration Point you just created, and click the **Federation** tab in the right pane.
5. In the **Supported and Selected CI Types** area, verify that **Incident**, **Problem**, and **RequestForChange** are selected.

Step 5: Create New Jobs to Synchronize Between OMi and SM


1. In OMi, select **Administration > RTSM Administration > Data Flow Management > Integration Studio**.
2. Click the **Data Push** tab.
3. In the New Integration Job dialog box, click the **+** icon on the left.
4. In the Available Queries dialog box, select the relevant queries for the job.

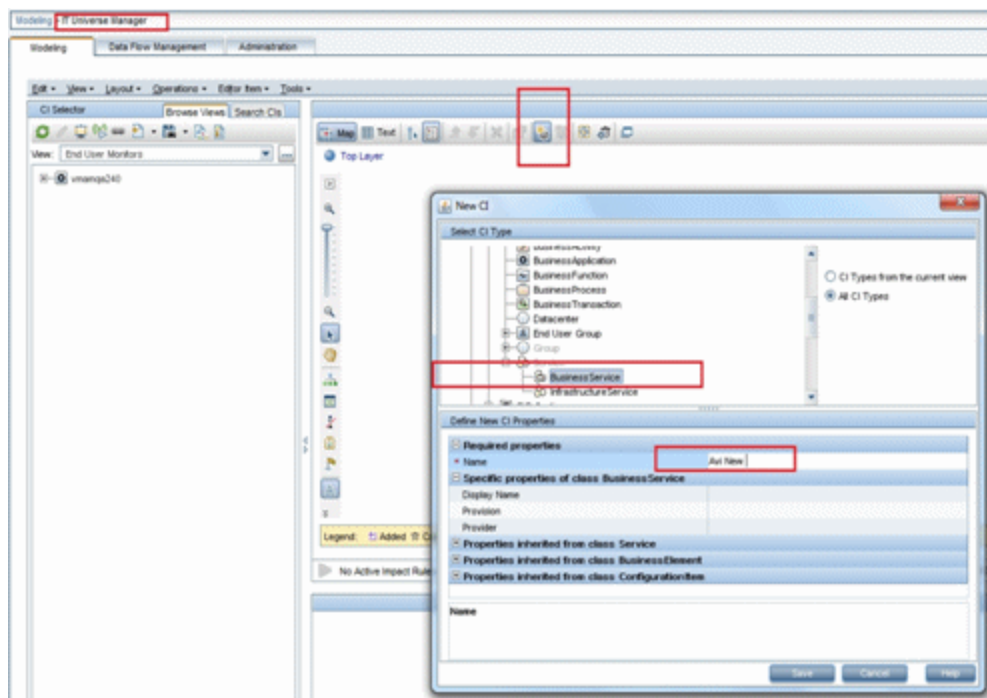
Step 6: Run the Job

When you run the job, the CIs are synchronized between OMi and SM.



Step 7: Test the Configuration

1. In OMi, select **Administration > RTSM Administration > Modeling > IT Universe Manager**.
2. In the **CI Selector** pane, select the relevant view, and click  in the right pane.
3. In the **New CI** dialog box that opens, create a new CI with the **BusinessService** type.



4. Create a TQL that includes only BusinessService CI Types (CITs):

Administration > Service Health > KPIs in Views

5. Click the **Calculate** button. The relevant CI appears in view.
6. Click the **Data Push** tab, and run the job in order to synchronize with SM. A message that the job was successful should be issued.
7. In SM, create a new incident for the new CI that you created above:
 - a. Select **Incident Management > Open New Incident**.
 - b. **Important:** Start by entering the name of the CI you want to attach to the incident in the **Affected CI** field. This creates the Incident Id.
 - c. Enter the CI name in the **Affected Service** field and click to search.

- d. Enter any incident detail.

HP Service Manager

Incident Details

Incident ID: 810170
Status: Open

Affected Service: Aut Pad
Affected CI: Aut Pad
CI is operational (no outage)

Outage Start:
Outage End:
Service Contract:

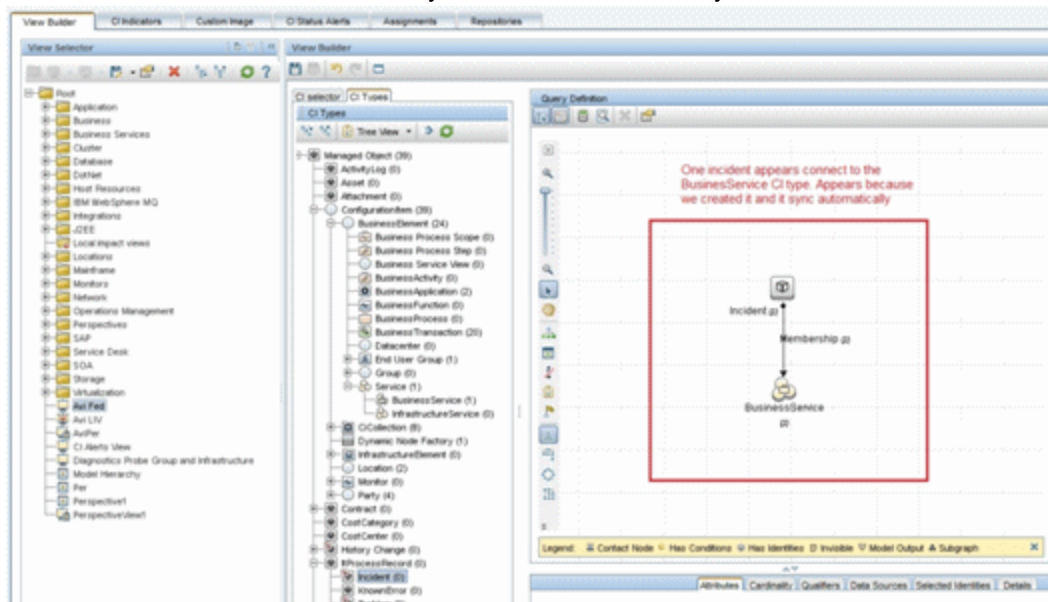
Title: Incident
Description: Incident

Assignment Group: Application
Assignee:
Vendor:
Vendor Ticket:

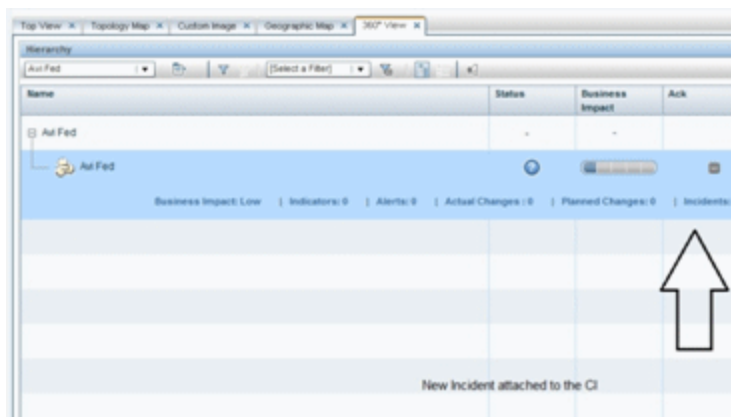
Category: Incident
Area: access
Subarea: authentication error
Impact: 1 - Enterprise
Urgency: 1 - Critical

The incident is automatically attached to the CI.

8. In OMi, create a TQL with the CI Type you created connected to the Incident CI Type in a membership relationship link.
9. Click the **Calculate** button. One incident appears connected to the BusinessService CI Type because this test created it and it is synchronized automatically.



10. Delete the incident from the TQL and save the TQL to be a view. The TQL is only used for the test.
11. Select **Application > Service Health**, and click the **360 View** tab. Check that the new incident is attached to the CI.



Step 8 (Optional): Add CI Types to the Service Health Changes and Incidents Component

By default, OMi Service Health displays information on incidents and requests for change 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 procedure described in ["How to Customize the Changes and Incidents Component" on page 120](#).

Troubleshooting

If you are not seeing expected incidents in OMi, see ["View Changes and Incidents in Service Health Using Standalone HP Universal CMDB" on page 96](#).

Chapter 26: 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
CollectTicketsWithImpacts	Retrieves SM incidents for the selected CI, and for its child CIs which have an Impact relationship.
CollectTicketsWithoutImpacts	Retrieves SM incidents for the selected CI.
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" on the next page](#).

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

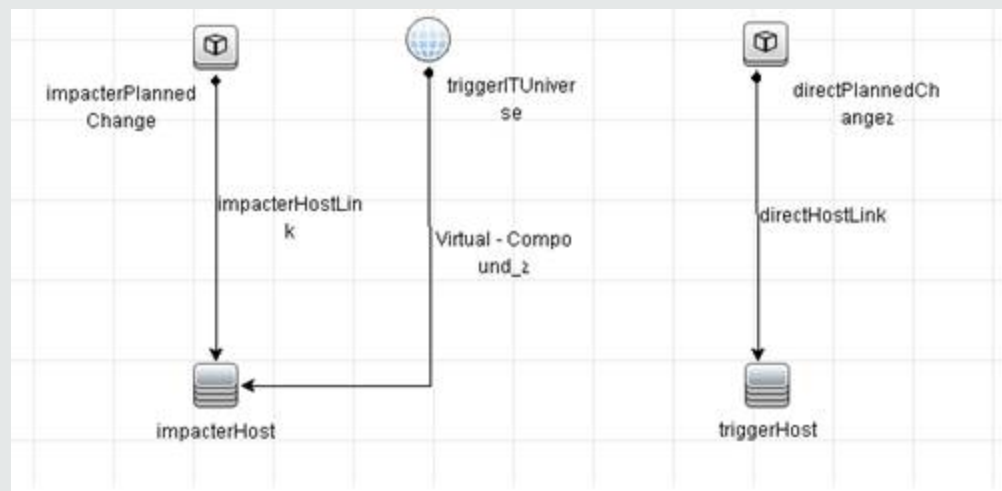
The following naming constraints should be followed in the request for change *without* impact TQL (see the TQL example below, on the right side of the image):

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

The following naming constraints should 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 should start with **impacter**.
- **triggerITU** represents the "impacted" child CIs.

Examples of request for change TQLs:



Naming Constraints for New Incident TQLs

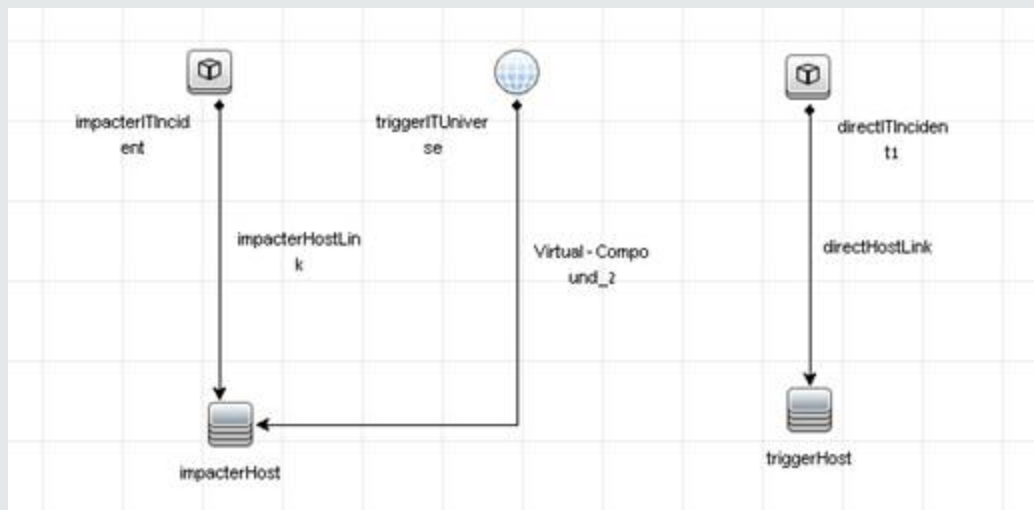
The following naming constraints should be followed in the incidents *without* impact TQL (see the TQL example below, on the right side of the image):

- The incident CI type should start with **directTIIncident**.
- The CI type related to the incident should start with **trigger**.

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

- **impacterITIncident** represents the incident CI type.
- The CI type related to the incident should start with **impacter**.
- **triggerITUniverse** represents the "impacted" child CIs.

Examples of incident TQLs:



Customizing the Service Manager 9.2 Integration

The ServiceManagerAdapter groovy script is provided for Event Forwarding to Service Manager. You can customize this script for your installations.

To customize the ServiceManagerAdapter groovy script, open the Scripts manager (📁), select the **sm:ServiceManagerAdapter** script and open it for editing (✎). The Edit Script window opens. The contents of the script are displayed in the **Script** tab.

Tip: Copying the script text into a text editor of your choice. When you have finished editing, copy the edited text back to the Edit Script window and save the script.

Near the beginning of the script, there are two sections used to modify the default behavior of the OMi event synchronization with Service Manager.

To access

Administration > Setup and Maintenance > Connected Servers

Click the 📁 button.

Configuring the ServiceManagerAdapter Script

This section controls which event and incident properties are synchronized to and from Service Manager, and is contained within the following comments:

- **BEGIN Configuration:** Customization of properties for synchronization
- **END Configuration:** Customization of properties for synchronization

The ServiceManagerAdapter script can be configured section contains constants, 6 "maps" and "8" sets to allow configuring the synchronization of the properties. Each is described below:

Service Manager Drilldown Constant

The first variable that can be adjusted is `SM_WEB_TIER_NAME`. Set this value to the base name of the web application deployed in the Tomcat container on the Service Manager system. This web application is used for drilling down into Service Manager. The name is used in the URL path for the drilldown. It must match the base name of the web application ("`.war`" is removed). The default is shown below:

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

OMi Administrator User

The `BSM_ADMINISTRATOR_LOGIN_NAME` variable is used to contain the name of the OMi Administrator user. By default this is set to `admin`.

For the events that are forwarded automatically by a forwarding rule, the `_is_recorded_by` attribute is set to the user specified in the `BSM_ADMINISTRATOR_LOGIN_NAME` variable.

For the events that are forwarded manually, the `_recorded_by` attribute is set to the user that initiated the forward request.

```
private static final String BSM_ADMINISTRATOR_LOGIN_NAME = 'admin'
```

Enumeration Value Maps

Maps are defined to map enumerated values of the event properties to values on Service Manager incident properties. These maps, in general, should not be customized, but they provide a list of possible values that can be specified in the sets described below. For details on each map, view the actual values defined in the script.

- **MapOPR2SMStatus:** Maps the event `state` to the Service Manager incident `status`
- **MapSM2OPRState:** Maps the Service Manager incident `status` to the event `state`
- **MapOPR2SMUrgency:** Maps the event `severity` to the Service Manager incident `urgency`
- **MapSM2OPRSeverity:** Maps the Service Manager incident `urgency` to the event `severity`

- **MapOPR2SMPriority:** Maps the event priority to the Service Manager incident priority
- **MapSM2OPRPriority:** Maps the Service Manager incident priority to the event priority

Custom Property Maps

The following maps allow a user to map any top-level event property to any top-level Service Manager incident property.

- **MapOPR2SMCustomAttribute:** Maps the specified custom attributes to a Service Manager incident property for synchronization.

Add a CA name to the map along with a Service Manager incident property name (XML tag name).

Target Service Manager Incident property name of "activity_log" will append the CA change to the Service Manager incident activity log.

Note: Only top-level Service Manager incident properties are supported in this map.

- **MapSM2OPRCustomAttribute:** Maps the specified Service Manager incident properties to an event custom attribute for synchronization.

Add a Service Manager incident property name to the map along with an event custom attribute name.

Note: Only top-level Service Manager incident properties are supported in this map.

Examples:

The following synchronizes the event custom attribute `MyCustomCA` to the Service Manager incident `activity_log` and the custom attribute `MyCustomCA1` to the Service Manager incident property `SMCustomAttribute`.

```
private static final Map<String, String> MapOPR2SMCustomAttribute =  
["MyCustomCA" : "activity_log", "MyCustomCA1" : "SMCustomAttribute"]
```

The following synchronizes the Service Manager incident property `incident_status` to the custom attribute `SMIncidentStatus`.

```
private static final Map<String, String> MapSM2OPRCustomAttribute = ["incident_  
status" : "SMIncidentStatus"]
```

Synchronization Change Sets

The following sets define which properties and enumerated values are synchronized whenever a change occurs in the OMi event or Service Manager incident. The properties synchronized upon a change as standard are marked in **bold**. For each list, the value of "*" can be specified. In this case, all

possible properties or enumerated values are synchronized for the specified list.

Note: When the Service Manager incident is created, all possible event properties and enumerated values are set in the Service Manager incident. The following sets are mainly used for synchronization of changes.

SyncOPRPropertiesToSM

Event properties to synchronize to a corresponding Service Manager Incident property on change:

- title
- **description**
- **state**
- severity
- priority
- **solution**
- assigned_user
- assigned_group

SyncOPRPropertiesToSMActivityLog

Event properties to synchronize to a corresponding Service Manager Incident activity log on change:

- **title**
- description
- **state**
- **severity**
- **priority**
- solution
- **annotation**
- **duplicate_count**
- **custom_attribute**
- **cause**

- **symptom**
- control_transferred_to
- **assigned_user**
- **assigned_group**

SyncSMPropertiesToOPR

Service Manager Incident properties to synchronize to a corresponding event property on change:

- name
- **description**
- **incident_status**
- urgency
- priority
- **solution**

SyncOPRStatesToSM

Event states to synchronize to the Service Manager incident status on change:

Note: state must be included in SyncOPRPropertiesToSM or this list is ignored.

- open
- in_progress
- in_progress
- resolved
- **closed**

SyncOPRSeveritiesToSM

Event severities to synchronize to the Service Manager incident urgency on change:

Note: severity must be included in SyncOPRPropertiesToSM or this list is ignored.

- **critical**
- **major**
- **minor**
- **warning**
- **normal**
- **unknown**

SyncSMStatusToOPR

Service Manager incident status to synchronize to the event states on change:

Note: status must be included in SyncSMPropertiesToOPR or this list is ignored.

- accepted
- assigned
- open
- reopened
- pending-change
- pending-customer
- pending-other
- pending-vendor
- referred
- suspended
- work-in-progress
- rejected
- replaced-problem
- resolved
- cancelled
- **closed**

SyncSMUrgenciesToOPR

Service Manager incident urgencies to synchronize to the event severities on change:

Note: urgency must be included in SyncSMPropertiesToOPR or this list is ignored.

Acceptable values are **1-4**.

SyncSMPrioritiesToOPR

Service Manager incident priorities to synchronize to the event priorities on change:

Note: priority must be included in SyncSMPropertiesToOPR or this list is ignored.

Acceptable values are **1-4**.

Examples:

The following example synchronizes the OMi title, state and description to the Service Manager incident whenever the corresponding property is changed in the OMi event.

```
private static final Set SyncOPRPropertiesToSM = ["title", "state", "description"]
```

The following example will synchronize the OMi states resolved and closed to the Service Manager incident whenever the corresponding property is changed in the OMi event.

```
private static final Set SyncOPRStatesToSM = ["resolved", "closed"]
```

Note: The properties that are synchronized to the Service Manager activity log are concatenated together for each change and then appended to the Service Manager incident activity log.

Localization

This section is provided to enable localizing some of the text that is displayed in the:

- The Event Browser **Forwarding** tab (not available for an Event Channel deployment)
- HP Service Manager incident activity log

This sections is contained within the following comments:

- BEGIN Localization: Customization of text values for language localization
- END Localization: Customization of text values for language localization

The following sections describe the text that can be localized.

Forwarding tab

The Service Manager incident properties urgency and priority are of type integer. In order to display a more meaningful value in the Forwarding tab, maps are provided to display a string. These strings may be localized for display in the browser.

- **Service Manager Urgency values**

The text value will be displayed on the **Forwarding** tab.

Note: This text may be localized for the desired locale.

```
private static final Map SMUrgency = ["1": "1 - Critical", "2": "2 - High", "3":  
"3 - Average", "4": "4 - Low"]
```

- **Service Manager Priority values**

The text value will be displayed on the **Forwarding** tab.

Note: This text may be localized for the desired locale.

```
private static final Map SMPriority = ["1": "1 - Critical", "2": "2 - High", "3":  
"3 - Average", "4": "4 - Low"]
```

Service Manager Incident Activity Log

Synchronization from OMi to Service Manager appends various text to the Service Manager incident activity log. This text may be localized as follows.

- **General Locale Setting:** Used mainly in formatting of dates. May be changed, for example to `Locale.JAPAN`. See Java *Locale* class documentation for all possible values.

```
private static final Locale LOCALE = Locale.getDefault()
```

- **Annotation date format:** See Java *SimpleDateFormat* class documentation for details on the syntax. Script default is below.

```
private static final String ANNOTATION_DATE_FORMAT = "yyyy.MM.dd HH:mm:ss z"
```

- **Description:** In Service Manager the incident description is a required attribute. In case it is not set in OMi this value is taken. An empty string is NOT allowed.

```
private static final String EMPTY_DESCRIPTION_OVERRIDE = "<none>"
```

- **Log Text:** The following text is prefixed to the appropriate event property when synchronizing it to an Service Manager Incident activity log.

NOTE: This text may be localized for the desired locale. Defaults are as shown below.

```
private static final String ACTIVITY_LOG_TITLE = "[Title]\n"

private static final String ACTIVITY_LOG_TITLE_CHANGE = "Event title changed to:
"

private static final String ACTIVITY_LOG_STATE = "[State]\n"

private static final String ACTIVITY_LOG_STATE_CHANGE = "Event state changed to:
"

private static final String ACTIVITY_LOG_DESCRIPTION = "[Description]\n"

private static final String ACTIVITY_LOG_DESCRIPTION_CHANGE = "Event description
changed to: "

private static final String ACTIVITY_LOG_SOLUTION = "[Solution]\n"

private static final String ACTIVITY_LOG_SOLUTION_CHANGE = "Event solution
changed to: "

private static final String ACTIVITY_LOG_ASSIGNED_USER = "[Assigned User]\n"

private static final String ACTIVITY_LOG_ASSIGNED_USER_CHANGE = "Event assigned
user changed to: "

private static final String ACTIVITY_LOG_ASSIGNED_GROUP = "[Assigned Group]\n"

private static final String ACTIVITY_LOG_ASSIGNED_GROUP_CHANGE = "Event assigned
group changed to: "

private static final String ACTIVITY_LOG_SEVERITY = "[Severity]\n"

private static final String ACTIVITY_LOG_SEVERITY_CHANGE = "Event severity
changed to: "

private static final String ACTIVITY_LOG_PRIORITY = "[Priority]\n"

private static final String ACTIVITY_LOG_PRIORITY_CHANGE = "Event priority
changed to: "

private static final String ACTIVITY_LOG_CONTROL_TRANSFERRED_TO = "[Control
Transferred To]\n"

private static final String ACTIVITY_LOG_CONTROL_TRANSFERRED_TO_CHANGED = "Event
control transfer state changed to: "

private static final String ACTIVITY_LOG_ANNOTATION = "[Annotation]\n"

private static final String ACTIVITY_LOG_CA = "[Custom Attribute]\n"
```

```
private static final String ACTIVITY_LOG_CAUSE = "[Cause] "

private static final String ACTIVITY_LOG_OMI_CAUSE = "[OMi Cause] "

private static final String ACTIVITY_LOG_OMI_SYMPTOM = "[OMi Symptom] "

private static final String ACTIVITY_LOG_DUPLICATE_COUNT = "[Duplicate Count] "

private static final String ACTIVITY_LOG_PREVIOUS = "previous "

private static final String ACTIVITY_LOG_CURRENT = "current "
```

Mapping Table: OMi Event to BDM Incident Property

The standard integration synchronizes the following OMi Event properties to Service Manager Incident properties:

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
-	-	-	global_id	id	-	There is no mapping and no synchronization for global_id between an OMi event and a Service Manager incident.
ID	-	id	external_process_reference	external.processs.reference	-	Set only on Service Manager incident creation.
-	External ID	control_transferred_to_external_id	reference_number	number	Incident ID	Set only on Service Manager incident creation.

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
Title	-	title	name	brief.description	Title	Set on incident creation. Standard configuration: only the OMi title changes are synchronized to the Service Manager incident activity log. If the event title exceeds 256 characters, or contains a newline character, it is truncated and the entire title is prepended to the description.
Description	-	description	description	action	Description	Can be a combination of the OMi event title and description. See title comments for details. Standard configuration: synchronized in both directions.
Solution	-	solution	solution	Resolution	Solution	Standard configuration: synchronized in both directions.

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
Lifecycle State	-	state	incident_status	problem.status	Status	Set on incident creation. Standard configuration: only 'closed' state is synchronized.
Severity	Severity	severity	urgency	severity	Urgency	Set on incident creation. Standard configuration: all value changes are synchronized.
Priority	Priority	priority	priority	priority.code	Priority	Set on incident creation. Standard configuration: all value changes are synchronized.
Assigned User	-	assigned_user_login_name	is_requester_by_party_display_label	contact.name	Contact	By default not synchronized.

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
-	Assigned User	-	has_assigned_party_display_label	assignee.name	Assignee	OMi queries the Service Manager Incident Web Service in real time for display in Forwarding Tab only. No synchronization between the OMi event and the Service Manager incident.
-	-	control_transferred_to_initiated_by	is_recorded_by_party_display_label	opened.by	Opened By	By default not synchronized.
Assigned Group	Assigned Group	assigned_group name	has_assigned_group_functional_group_display_label	assignment	Assignment Group	OMi queries the Service Manager Incident Web Service in real time for display on the Forwarding tab only. No synchronization between the OMi event and the Service Manager incident.

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
Category	-	category	category	sub_category	Area	Category is set by OMi only on Service Manager incident creation, but is by default ignored in Service Manager.
Subcategory	-	sub_category	sub_category	product_type	Subarea	Subcategory is set by OMi only on Service Manager incident creation, but is by default ignored in Service Manager.
Related CI	-	related_ci	is_registered_for	logical.name	Affected CI	Affected CI is set by OMi only on Service Manager incident creation.
Annotations	-	annotation_list	activity_log description	update.action	Activity Log	Synchronized from OMi to Service Manager only. OOTB synchronization enabled.

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
Custom Attributes	-	custom_attribute_list	activity_log description	update.action	Activity Log	Can be configured for synchronization to a specific Service Manager incident property, or the activity log. For Service Manager activity log, synchronization is from OMi to Service Manager only. Standard configuration: synchronization disabled.

OMi UI (Event)	OMi UI (Forwarding)	OMi Web Service (Event)	Service Manager Web Service (Incident)	Service Manager Object	Service Manager UI	Comments
Cause	-	cause->control_transferred_to_external_id	is_caused_by-master_reference_number	Links the two SM Incidents	Related Records	If the cause event has been synchronized to Service Manager, the two Service Manager Incidents are related, otherwise information about the OMi cause is appended to the Service Manager incident activity log. Standard configuration: synchronization enabled.
Symptoms	-	symptom_list	activity_log_description	update.action	Activity Log	Synchronization is from OMi to Service Manager only. Standard configuration: synchronization enabled.
Duplicate Count	-	duplicate_count	activity_log_description	update.action	Activity Log	Synchronization is from OMi to Service Manager only. Standard configuration: synchronization enabled.

Part VI: Operations Manager i - Network Node Manager i Integration

Chapter 27: 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 drilldown.** 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 28: 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 142](#).

Chapter 29: 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
Layer 2 Neighbor View	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.
Layer 3 Neighbor View	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.
MPLS VPN Inventory	This is an enterprise customer view of how their sites are connected via service provided MPLS networks.
Open Key Incidents	Shows the incidents that are most important to network operators and that often require more immediate action.
Overall Network Health (Node Group Overview)	Displays a map containing all (top-level) Node Groups that do not have parent Node Groups.
Overall Network Health - Routers	Displays a Node Group Map of the Router connectivity in your network.

Component Name	Description
Overall Network Health - Switches	Displays a Node Group map of the Switches connectivity in your network.
Router Redundancy Groups Inventory	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 30: 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 31: 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.

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** 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 Sun JRE.

For OO 9.xx:

- a. On the OO server, enter:

o **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"
```

o **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:

o **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"
```

o **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:

o **Windows:**

Enter the following commands:

- **"%JAVA_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"

- **"%JAVA_HOME%\jre\bin\keytool" -keystore "%TOPAZ_HOME%\JRE64\lib\security\cacerts" -import -alias "<Operations Orchestration fully qualified host name>" -file "<path>\<Operations Orchestration fully qualified host name>.cer"**

Tip: If your %JAVA_HOME% environment variable points to the JRE directory instead of the JDK directory, remove **jre** from the keystore path ("%JAVA_HOME%\bin\keytool" -keystore) in the commands.

Note: If JAVA_HOME is not set, use TOPAZ_HOME.

o **Linux:**

Enter the following command:

\$TOPAZ_HOME/JRE64/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 32: 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/jmx-console**.
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 33: 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 34: BSM Connector Integration Administration

BSM Connector captures and forwards data such as events, topology and metrics from third-party systems to OMi.

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

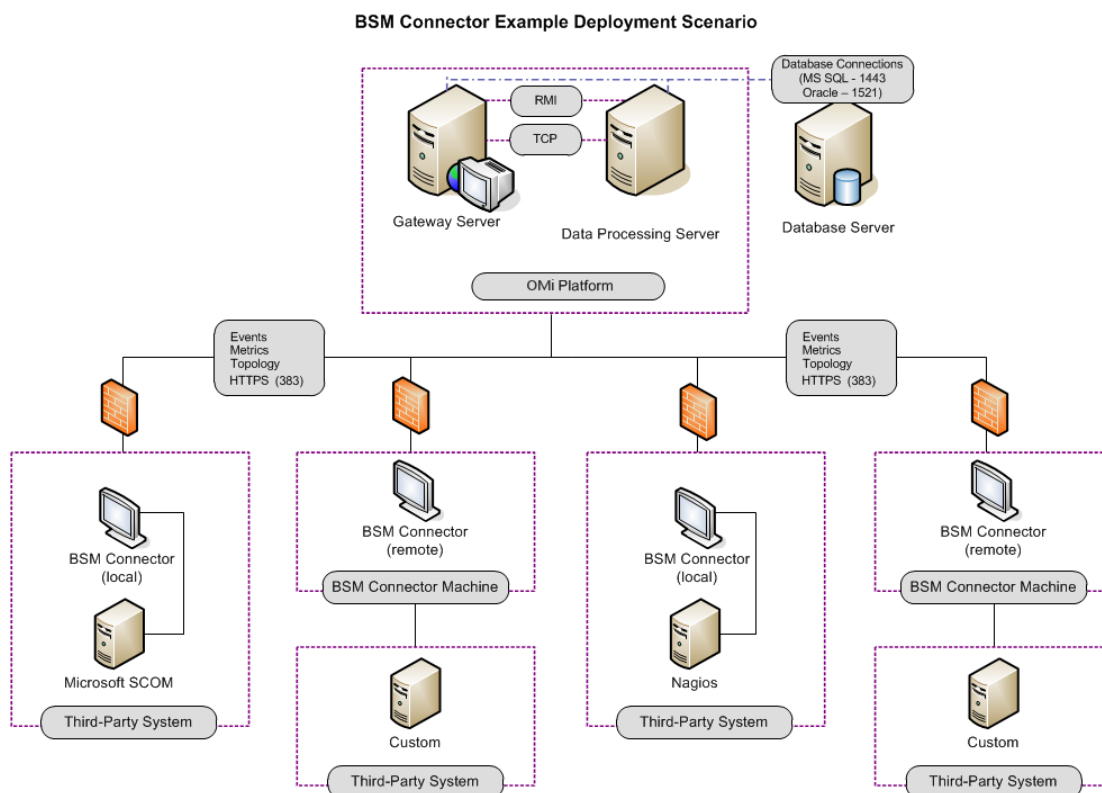
From the Connected Servers page, you can access and maintain all BSM Connectors in the OMi deployment environment, regardless of the operating system or host location on which the BSM Connector is installed.

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 10.00)

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.

We appreciate your feedback!



[Go OMi!](#)