

# HP Business Service Management

For the Linux and Windows® operating systems

Software Version: 9.10

---

## Using HP BSM Integration Adapter

Document Release Date: August 2011

Software Release Date: August 2011



## 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 2010-2011 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.

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

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

iPod is a trademark of Apple Computer, Inc.

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.

UNIX® is a registered trademark of The Open Group.

### Acknowledgements

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

## Support

Visit the HP Software Support Online web site at:

**<http://www.hp.com/go/hpsoftwaresupport>**

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

---

## Contents

Using HP BSM Integration Adapter.....	1
Contents.....	4
HP BSM Integration Adapter.....	8
HP BSM Integration Adapter overview.....	8
HP BSM Integration Adapter and HP Operations Agent.....	9
Event integration.....	10
Topology data.....	11
HP BSM Integration Adapter and Operations Manager i.....	11
User authentication.....	12
User interface.....	13
Configuring HP BSM Integration Adapter.....	14
Reconfigure HP BSM Integration Adapter.....	14
Grant certificate requests in BSM.....	17
Configure trusted certificates.....	18
Connect BSM Integration Adapter to a reverse proxy or load balancer.....	20
Configure group-based LW-SSO authentication.....	22
Prepare user-based LW-SSO authentication.....	24
Configure user-based LW-SSO authentication.....	25
Configure local user authentication.....	27
Activate flexible management.....	28
Use ia-config in silent mode.....	29
Accessing HP BSM Integration Adapter.....	31
Start the HP BSM Integration Adapter user interface from a web browser.....	31
Start the HP BSM Integration Adapter user interface in BSM.....	32
Log on to HP BSM Integration Adapter.....	32
Log out of HP BSM Integration Adapter.....	33
Managing HP BSM Integration Adapter with HPOM.....	33
To manage BSM Integration Adapter with HPOM for Windows.....	33

To manage BSM Integration Adapter with HPOM for UNIX or Linux.....	34
<b>Managing policies.....</b>	<b>37</b>
Managing policies in cluster environments.....	37
Edit policies.....	38
To edit unlocked policies.....	38
To break the edit lock on locked policies.....	38
Copy policies.....	39
To copy a policy.....	39
Delete policies.....	39
To delete policies.....	39
Activate and deactivate policies.....	39
To activate policies.....	40
To deactivate policies.....	40
Import policies.....	40
To import policies.....	41
Configure policy management options.....	41
To change the column display.....	41
<b>Developing discovery policies.....</b>	<b>42</b>
To configure a discovery policy.....	42
Configure discovery policy properties.....	42
To configure properties of discovery policies.....	42
Configure commands in discovery policies.....	43
To configure the command of discovery policies.....	49
Configure schedules in discovery policy.....	50
To configure the schedule of discovery policies.....	50
<b>Developing SNMP interceptor policies.....</b>	<b>51</b>
To configure HP Operations Agent to receive SNMP traps.....	51
To configure an SNMP interceptor policy.....	51
Configure SNMP interceptor policy properties.....	52
To configure properties of SNMP interceptor policies.....	52
Configure event defaults in SNMP interceptor policies.....	53
To configure attribute defaults in SNMP interceptor policies.....	53

Configure SNMP rules.....	60
To configure rules in SNMP interceptor policies.....	61
Configure SNMP interceptor policy options.....	73
To configure options in SNMP interceptor policies.....	73
<b>Developing XML interceptor policies.....</b>	<b>76</b>
To configure an XML log file policy.....	77
Configure XML log file policy properties.....	77
To configure properties of XML log file policies.....	78
Configure XML log file source properties.....	78
To configure the XML log file source.....	78
Configure XML log file mapping defaults.....	83
To configure mapping defaults in XML log file policies.....	85
Configure XML log file event defaults.....	85
To configure attribute defaults in XML log file policies.....	86
Configure XML log file rules.....	95
To configure rules in XML log file policies.....	97
Configure XML log file policy options.....	108
To configure options in XML log file policies.....	108
<b>Pattern matching.....</b>	<b>110</b>
Pattern-matching details.....	110
User-defined variables in patterns.....	113
Rules by which BSM Integration Adapter assigns strings to variables.....	113
Using subpatterns to assign strings to variables.....	114
Pattern matching for variables.....	115
Example.....	115
Examples of pattern matching in rule conditions.....	116
<b>Synchronizing events.....</b>	<b>118</b>
To configure event synchronization.....	118
Configure the HP BSM Integration Adapter server as a connected server.....	119
To configure a target connected server.....	119
Configure policies for event synchronization.....	121
To configure policies for event synchronization.....	121

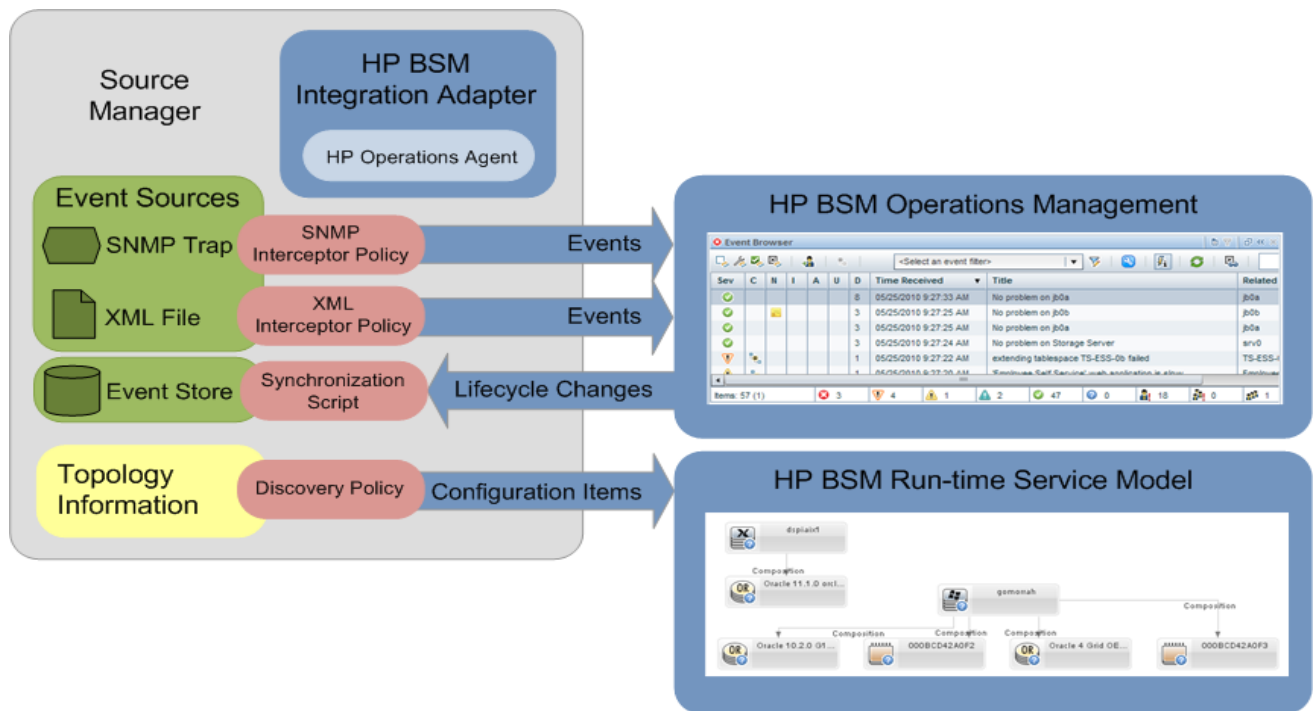
Write Perl scripts for event synchronization.....	122
To forward event changes to the source manager.....	122
<b>Configuring drilldown.....</b>	<b>123</b>
Configure launch of the HP BSM Integration Adapter user interface.....	123
Configure drilldown into source managers.....	124

## HP BSM Integration Adapter

HP BSM Integration Adapter enables you to monitor event sources, and, if certain conditions apply, to forward the detected events as HP Business Service Management (BSM) events directly to BSM Operations Management. BSM tries to associate the events that it receives with configuration items (CIs) using CI resolution and with indicators using ETI (event type indicator) resolution. This is only possible if the computer on which the event occurs is set up as a CI in the BSM RTSM (Run-time Service Model). Discovery policies automatically populate the RTSM (Run-time Service Model) with topology data based on discovery scripts executed within the BSM Integration Adapter environment.

### HP BSM Integration Adapter overview

The following figure shows an overview of the BSM Integration Adapter environment.





## HP BSM Integration Adapter and HP Operations Agent

BSM Integration Adapter includes HP Operations Agent. HP Operations Agent collects and monitors data on the event source, enriches these events with information that is meaningful to BSM users, and sends the events to BSM where they are displayed in the Operations Management Event Browser. HP Operations Agent can also run discovery scripts or programs, store and compare the CI details obtained in each discovery cycle, and send the discovery data to the RTSM (Run-time Service Model). BSM Integration Adapter uses monitor and discovery policies to configure the agent. For each monitor policy, you decide what kinds of events to monitor, how often to monitor, what to look for in the events, and what to do if certain events are detected. For each discovery policy, you decide which discovery script to run and how often to run.

For more information about HP Operations Agent, see the documentation that the HP Operations Agent provides.

## Event integration

For BSM Integration Adapter to be able to convert source events to BSM events, the event sources must make their data available as SNMP traps or in XML-formatted files:

- **SNMP traps**

SNMP event sources can range from simple hardware devices that send SNMP traps to sophisticated network management solutions such as HP Network Node Manager i (NNMi) (NNMi provides an out-of-the-box integration with BSM Integration Adapter, which converts NNMi incidents to SNMPv2c traps and forwards these SNMPv2c traps as BSM events to the BSM Operations Management Event Browser. For more information about this integration, see the *NNMi Deployment Reference*).

- **XML files**

BSM Integration Adapter can also monitor XML-formatted files. Because BSM Integration Adapter is agnostic to the content and syntax of the XML files, you can monitor any XML file (If the application that you want to monitor does not log its events in XML format, consider writing a program or script that diverts and converts the application's output to XML-formatted files.).

**Tip:** Monitoring XML files is a convenient way to forward events from other source managers to BSM Operations Management. In the context of BSM, a source manager is an HP or third-party software solution that monitors and manages performance, systems, services, or networks in the IT environment. Examples include HP Network Node Manager i (NNMi), Microsoft System Center Operations Manager (SCOM), or IBM Tivoli solutions.

After Operations Management receives an event, you can keep it up to date on the source by configuring BSM and BSM Integration Adapter to synchronize event lifecycle changes (to the state closed) back to the source manager that generated the original event. For example, if a BSM Operations Management operator closes an event, a notification can be automatically sent to NNMi.

## Topology data

Accurate and up-to-date CI topology data in the RTSM (Run-time Service Model) is essential for CI and ETI (event type indicator) resolution, TBEC (Topology-based Event Correlation), and context-specific tools. BSM Integration Adapter uses discovery policies to automatically discover IT infrastructure resources and their interdependencies.

Discovery policies execute a discovery script that you create and that must write details of each discovered CI and its relationships in XML to STDOUT (standard output stream). BSM Integration Adapter processes the XML data and publishes details of new, changed, and removed CIs and CI relationships to the discovery server on the BSM gateway servers, according to a schedule that you specify for each policy.

Before topology data is written to the RTSM, topology synchronization rules manipulate the data by applying mapping rules and scripts. Mapping rules and scripts transform the discovered topology data into CI and CI relations in the RTSM. For more information about topology synchronization, see the *OMi Extensibility Guide*.

**Note:** You can also create the CIs and CI relationships using the discovery features of the RTSM (Run-time Service Model) and HP Data Flow Management (DFM), using OMi topology synchronization, or manually. It is recommended to use BSM Integration Adapter discovery if you already use BSM Integration Adapter to forward events to the BSM Operations Management Event Browser. You can create CIs manually if the CIs you want to create are limited in number, and are stable in nature, so are unlikely to change.

## HP BSM Integration Adapter and Operations Manager i

In the context of Operations Manager i (OMi) BSM can receive events and topology data from HP Operations Manager (HPOM), or directly from BSM Integration Adapter. BSM Integration Adapter is the preferred method for sending events and topology data to OMi in the following situations:

- If you are developing *new* integrations for sending events and topology data to BSM Operations Management.
- If there is no need to use the HPOM event processing and discovery capabilities or console.
- If HPOM is not part of the BSM deployment. (For more information about deploying BSM, see the *BSM Deployment Guide*.)

You can integrate BSM Integration Adapter into Operations Management so that administrators can launch the BSM Integration Adapter user interface in the Connected Servers manager or in the context of an event. Single sign-on authentication enables BSM users to log into BSM once and gain access to BSM Integration Adapter without being prompted to log in again.

BSM also enables operators to start the user interface of the source manager in the context of an event in the Operations Management Event Browser.

## User authentication

BSM Integration Adapter supports the following user authentication strategies:

- Single Sign-On (SSO) for BSM applications (recommended)

The default single sign-on authentication strategy for BSM is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in BSM and does not require an external computer for authentication.

LW-SSO enables a user to log into BSM once and gain access to all BSM applications without being prompted to log in again. The applications inside BSM trust the authentication, and you do not need further authentication when moving from one application to another. For example, if you configure BSM Integration Adapter to use LW-SSO, BSM users can launch the BSM Integration Adapter user interface without having to provide additional credentials.

**Tip:** BSM enables you to group users to make managing user permissions more efficient. For example, you could add all BSM Integration Adapter users to a dedicated group (`IA_ADMINS`, for example) and assign permissions to access BSM Integration Adapter to the group.

For more information about LW-SSO, see the *BSM Platform Administration* guide.

- Local user authentication

Each BSM Integration Adapter instance maintains a local user store. These users can access the local BSM Integration Adapter instance only and cannot gain access to other BSM applications. When BSM users launch the BSM Integration Adapter user interface, they have to provide the credentials of a local BSM Integration Adapter user.

The BSM Integration Adapter configuration program by default creates a user account in the local user store. In addition, you can optionally enable single sign-on during the configuration. For more information about configuring LW-SSO authentication for BSM Integration Adapter, see ["Configure group-based LW-SSO authentication" \(on page 22\)](#). For more information about adding additional local users, see ["Configure local user authentication" \(on page 27\)](#).

## User interface

The BSM Integration Adapter user interface is web based; you can therefore access it from anywhere using a supported web browser.

Policy Type	Name	Description	Activation State	Edited By
Discovery	Discover web servers	Discover web servers in example.com	activated	
Discovery	Discover SNMP devices	Discover SNMP devices that send LLD traps	activated	
HPOM Service-Auto-Disco...	DiscoverOMTypes	Discover all service types that are defined on the OM Server	deactivated	
HPOM Service-Auto-Disco...	DiscoverOM	Discover all nodes, external nodes, node groups, and services ...	deactivated	
SNMP Interceptor	lldp_mib	Capture Link Layer Discovery traps	activated	
SNMP Interceptor	nnmi_snmp	NNMi SNMP Trap Forwarding and Management Event Integration...	deactivated	
XML Interceptor	XML logon alerts	Monitor logon alerts in logon.xml	deactivated	admin
XML Interceptor	Web server error detection	Monitor errors in web_error.xml	activated (reactivate for new version)	

The policies have been automatically reloaded at 11/30/2010 11:47:27 AM.

Transferring data from localhost... localhost:21350

## Configuring HP BSM Integration Adapter

After the initial configuration of BSM Integration Adapter, you can run the configuration program again to reconfigure BSM Integration Adapter, for example to change the BSM server, to enable or disable local user or single sign-on authentication, or to change the Apache Tomcat ports.

### Reconfigure HP BSM Integration Adapter

You can reconfigure BSM Integration Adapter by running the configuration program `ia-config` again. For more information about `ia-config`, type `ia-config -h`.

When you rerun `ia-config`, the program does the following:

- Replaces all existing values with new or default values.
- Creates a backup of the flexible management policy:

```
Windows: %OvDataDir%\conf\HPOprIA\<policy_ID>_data.bak
         %OvDataDir%\conf\HPOprIA\<policy_ID>_header.xml.bak
```

```
Linux: /var/opt/OV/conf/HPOprIA/<policy_ID>_data.bak
       /var/opt/OV/conf/HPOprIA/<policy_ID>_header.xml.bak
```

- Creates a backup of the SSO configuration values:

```
Windows: %OvDataDir%\conf\HPOprIA\lwssso-config.xml.bak
Linux: /var/opt/OV/conf/HPOprIA/lwssso-config.xml.bak
```

**Note:** The command line tool `ovconfchg` enables you to change one or more configuration parameters in the internal configuration settings file. `ovconfchg` is an expert tool and should be used by experienced administrators only.

To run `ovconfchg`:

```
Windows: ovconfchg -edit
```

```
Linux: /opt/OV/bin/ovconfchg -edit
```

The `-edit` option starts a text editor to edit the settings file. After you have saved your changes, you must restart the application.

#### To reconfigure BSM Integration Adapter

1. *Windows only.* Start the configuration program:

- a. Open a command prompt and type:

```
cd %OvDataDir%\installation\HPOprIA
```

- b. Start the BSM Integration Adapter configuration program, type:

```
ia-config.bat
```

*Linux only.* Start the BSM Integration Adapter configuration program, type.

```
/var/opt/OV/installation/HPOprIA/ia-config.sh
```

2. The configuration programs asks whether you want to connect BSM Integration Adapter to

another BSM server.

To keep the existing BSM server, type **no** or accept the default. (When connecting BSM Integration Adapter to a BSM environment that includes a man in the middle (for example, a reverse proxy or a load balancer), type **no**. See also ["Connect BSM Integration Adapter to a reverse proxy or load balancer"](#) (on page 20).)

To change the BSM server:

- a. Type **yes**.
- b. The configuration program asks whether to create a flexible management policy. Flexible management policies enable HP Operations Agent to send events to multiple BSM servers based on time and event attributes. If you allow the configuration program to create such a policy, the new server becomes the primary manager of the BSM Integration Adapter server. Both the old *and* the new BSM server receive events from BSM Integration Adapter, but only the primary manager receives the discovery data.

**Note:** The flexible management policy cannot be edited in BSM Integration Adapter. If you no longer need the policy, deactivate it and delete it.

Type **yes** to create a flexible management policy. The default is to not create a flexible management policy.

In an environment with multiple BSM servers, you must configure each server to trust certificates that the other servers issued. See ["Configure trusted certificates"](#) (on page 18).

Remember to activate the flexible management policy in the BSM Integration Adapter user interface. See ["Activate flexible management"](#) (on page 28).

- c. Type the FQDN (fully qualified domain name) of the *new* BSM server. In a distributed BSM deployment, choose the gateway server.
- d. Type or accept the FQDN of the *new* BSM certificate server. If your BSM deployment includes a dedicated certificate server, choose the FQDN of the certificate server. Otherwise type the FQDN of the gateway server. The gateway server forwards certificate requests to the data processing server, which by default also acts as certificate server.

When you change the BSM server, a certificate request is sent to the new BSM server and must be granted there. See ["Grant certificate requests in BSM"](#) (on page 17).

3. Type **yes** to create a BSM Integration Adapter user account in the local user store. If you accept the default values, the configuration program adds the user `admin` with the password `admin`. You can also add users manually using `ia-user`. For details, see ["Configure local user authentication"](#) (on page 27).

Type **no** to stop the configuration program from adding a local user to the user store. When you stop the configuration program from adding a local user to the user store, single sign-on authentication is enabled automatically. You must then also enable and configure LW-SSO in BSM as described in ["Configure group-based LW-SSO authentication"](#) (on page 22) or ["Prepare user-based LW-SSO authentication"](#) (on page 24).

**Caution:** You must either create local users or enable and configure single sign-on authentication. Otherwise you will not be able to log onto BSM Integration Adapter.

4. Type or accept the default HTTPS port (21350) for the Apache Tomcat server.

5. Type or accept the default HTTP port (21351) for the Apache Tomcat server.
6. The configuration program asks whether you want to change the existing single sign-on (SSO) configuration.

To keep the existing SSO configuration with the currently configured values, type **no** or accept the default.

To change or disable the SSO configuration, type **yes**. The configuration program asks whether you want to enable single sign-on authentication:

- a. Type **no** to disable single sign-on authentication if you only want to use local user authentication.
- b. Type **yes** to accept or change the single sign-on authentication, and type or accept the following values:
- c. **Domain name (SSO)**: Type or accept the domain in which BSM and the BSM Integration Adapter instance are running. The default domain name is extracted from the FQDN of the BSM server.
- d. **Token key (initString)**: Type the token key generated in the BSM Users and Permissions manager. See "[Configure group-based LW-SSO authentication](#)" (on page 22) and "[Prepare user-based LW-SSO authentication](#)" (on page 24) for more information.
- e. **Accessible BSM Groups/Roles (SSO)**: For group-based SSO authentication, type or accept the BSM users and roles that will gain access to BSM Integration Adapter. Separate individual groups and roles with commas (for example, IA\_ADMININS, SUPERUSER). The configuration program by default adds the group IA\_ADMININS and the role SUPERUSER.

**Tip:** You can also enter group and role names that contain spaces; for example: IA\_ADMININS, BSM Administrators, SUPERUSER, BSM User. Quotation marks are not needed.

*Optional for user-based authentication.* Type **DISABLED**. This indicates that group-based authentication is not used.

The configuration is complete when the message `HP BSM Integration Adapter configured successfully` appears.

7. *Optional.* Review the log file at:

Windows: %OvDataDir%\log\HPOprIA-CLIs.log

Linux: /var/opt/OV/log/HPOprIA-CLIs.log

The program appends log information to the file when you run the program again.

*Windows only.* If the log file contains errors relating to the OvControl service failing to start or restart, complete the following steps:

- a. Manually reinstall ovcd as a Windows service, type:  

```
ovcd -install
```
- b. Rerun `ia-config`.



## Grant certificate requests in BSM

Certificates enable BSM Integration Adapter to communicate securely with HP Business Service Management (BSM).

During the configuration phase, BSM Integration Adapter sends a certificate request to the BSM gateway server. You must then grant the certificate on the BSM certificate server (usually the data processing server):

1. On the BSM certificate server (usually the data processing server), type:

```
ovcm -listpending
```

The command returns the ID of the certificate request, for example:

```
2875f202-2c96-754f-01df-a19468c698fa
```

2. On the BSM certificate server, grant the certificate request, type:

```
ovcm -grant <request ID>
```

3. On the BSM certificate server, verify that communication with BSM Integration Adapter is possible, type:

```
bbcutil -ping <BSM Integration Adapter system>
```

Example output:

```
IAmgmt.example.com: status=eServiceOK
  coreID=50c5ba52-0013-7550-00a9-91b84b1758a6
  bbcV=11.00.044 appN=ovbbccb appV=11.00.044 conn=1
  time=500 ms
```

4. On the BSM Integration Adapter system, check the status of the installed certificates, type:

```
ovcert -list
```

The output should be similar to the following:

```
+-----+
| Keystore Content |
+-----+
| Certificates: |
|   50c5ba52-0013-7550-00a9-91b84b1758a6 (*) |
+-----+
| Trusted Certificates: |
|   CA_f719d932-2ac7-754f-07e0-ab13b12a93ad |
+-----+
```

5. On the BSM Integration Adapter system, verify that communication with the BSM gateway server is possible, type:

```
bbcutil -ping <BSM gateway server>
```

Example output:

```
bsm.example.com: status=eServiceOK
  coreID=f719d932-2ac7-754f-07e0-ab13b12a93ad
```

```
bbcV=06.21.002 appN=ovbbccb appV=06.21.002 conn=8  
time=411 ms
```

6. On the BSM Integration Adapter system, validate the settings for `CERTIFICATE_SERVER` and `MANAGER`, type:

```
ovconfchg -edit
```

Alternatively, use the `setup-secure-communication` tool on the BSM certificate server to grant pending certificate requests.

1. On the BSM certificate server, open a command prompt or shell and type:

```
Windows: cd %TOPAZ_HOME%\bin
```

```
Linux: cd /opt/HP/BSM/bin
```

2. Start the following command:

```
Windows: setup-secure-communication.bat
```

```
Linux: setup-secure-communication.sh
```

3. The command checks for pending certificate requests. For each pending certificate request, the command shows details of the request. For example:

```
INFO: Secure communication request from: IAmgmt.example.com
```

Press **g** to grant each request in turn. After you grant a certificate request, the command sends certificates to the BSM Integration Adapter server, and then verifies that secure communication is possible.

4. On the BSM Integration Adapter system, validate the settings for `CERTIFICATE_SERVER` and `MANAGER`, type:

```
ovconfchg -edit
```

## Configure trusted certificates

In an environment with multiple BSM servers, you must configure each server to trust certificates that the other servers issued. This task involves exporting every server's trusted certificate, and then importing this trusted certificate to every other server. You must also update the agent's trusted certificates, so that the agent also trusts the BSM servers.

Configure trusted certificates for *every* BSM:

1. On *every* BSM server, export the trusted certificate to a file using the following command:

```
ovcert -exporttrusted -file <file>
```

The command generates a file with the name that you specify.

2. Copy each file to *every other* server, and then import the trusted certificate using the following commands:

```
ovcert -importtrusted -file <file>
```

```
ovcert -importtrusted -ovrg server -file <file>
```

3. On the BSM Integration Adapter system, update the trusted certificates using the following

command:

```
ovcert -updatetrusted
```

## Connect BSM Integration Adapter to a reverse proxy or load balancer

Certificates enable BSM Integration Adapter to communicate securely with HP Business Service Management (BSM).

The certificate request that HP Operations Agent sends during the configuration phase to BSM may fail if the BSM environment uses a load balancer or reverse proxy and the load balancer or reverse proxy is configured for HTTPS communication only. Because HP Operations Agent does not have a certificate yet, the request is sent using HTTP, and is therefore blocked by the load balancer or reverse proxy.

To provide the agent with a certificate, you must issue the certificate manually on the BSM certificate server and then import it manually on the BSM Integration Adapter system:

1. On the BSM Integration Adapter system, use `ovcoreid` to show the core ID of the system:

Windows: `ovcoreid`

Linux: `/opt/OV/bin/ovcoreid`

2. On the BSM certificate server (usually the data processing server), use `ovcert` to export the trusted certificate, type:

Windows: `ovcert -exporttrusted -file omi.cer`

Linux: `/opt/OV/bin/ovcert -exporttrusted -file omi.cer`

3. On the BSM certificate server (usually the data processing server), use `ovcm` to generate a certificate, type:

Windows: `ovcm -issue -file cert.cer -name <FQDN of BSM Integration Adapter> -coreid <OvCoreId of BSM Integration Adapter> -pass <password>`

Linux: `/opt/OV/bin/ovcm -issue -file cert.cer -name <FQDN of BSM Integration Adapter> -coreid <OvCoreId of BSM Integration Adapter> -pass <password>`

4. Securely transfer the generated files to the BSM Integration Adapter system.

5. Use `ovcert` to import the certificates from the generated files, type:

Windows: `ovcert -importtrusted -file omi.cer`

Windows: `ovcert -importcert -file cert.cer`

Linux: `/opt/OV/bin/ovcert -importtrusted -file omi.cer`

Linux: `/opt/OV/bin/ovcert -importcert -file cert.cer`

The command prompts you for the password that you specified when you generated the certificates. Type the password and press **Enter**.

6. On the gateway server system, use `ovcoreid` to show the core ID of the system:

Windows: `ovcoreid`

Linux: `/opt/OV/bin/ovcoreid`

7. On the BSM Integration Adapter system, set the manager and certificate server manually, type:

**Windows:** `ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <FQDN of load balancer or reverse proxy>`

**Windows:** `ovconfchg -ns sec.core.auth -set MANAGER <FQDN of load balancer or reverse proxy>`

**Windows:** `ovconfchg -ns sec.core.auth -set MANAGER_ID <OvCoreId of gateway server>`

**Linux:** `/opt/OV/bin/ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <FQDN of load balancer or reverse proxy>`

**Linux:** `/opt/OV/bin/ovconfchg -ns sec.core.auth -set MANAGER <FQDN of load balancer or reverse proxy>`

**Linux:** `/opt/OV/bin/ovconfchg -ns sec.core.auth -set MANAGER_ID <OvCoreId of gateway server>`

8. Run `oainstall` to complete the HP Operations Agent setup, type:

**Windows 32-bit:** `cscript "%OvInstallDir%\bin\OpC\install\oainstall.vbs" -a -c`

**Windows 64-bit:** `cscript "%OvInstallDir%\bin\win64\OpC\install\oainstall.vbs" -a -c`

**Linux:** `/opt/OV/bin/OpC/install/oainstall.sh -a -c`

9. Review the agent installation log file:

**Windows:** `%OvDataDir%\log\oainstall.log`

**Linux:** `/var/opt/OV/log/oainstall.log`

*Windows only.* If the log file contains errors relating to the OvControl service failing to start or restart, complete the following steps:

- a. Manually reinstall `ovcd` as a Windows service, type:

`ovcd -install`

- b. Rerun `oainstall`.

10. Securely delete any copies of the files that contain the certificates. Depending on how you generate and transfer the files, you may, for example, have copies in the following locations:
- on the BSM data processing server
  - on a USB flash drive, CD, or other portable media
  - on the BSM Integration Adapter system
11. Configure BSM Integration Adapter. See "[Reconfigure HP BSM Integration Adapter](#)" (on page [14](#)) for more information.

## Configure group-based LW-SSO authentication

Lightweight Single Sign-On (LW-SSO) enables a user to log onto BSM once and gain access to all BSM applications without being prompted to log on again. The applications inside BSM trust the authentication, and you do not need further authentication when moving from one application to another. For example, if you configure BSM Integration Adapter to use LW-SSO, BSM users can launch the BSM Integration Adapter user interface without having to provide additional credentials.

For more information about LW-SSO, see the *BSM Platform Administration* guide.

If you want to use group-based LW-SSO authentication with BSM Integration Adapter, perform the following steps *before* configuring BSM Integration Adapter.

1. In BSM, make sure that LW-SSO is enabled and write down the token key (initString). You need this information when configuring BSM Integration Adapter for SSO authentication.

For details about how to configure LW-SSO, see the section on *Users, Permissions, and Recipients* in the Platform Administration online help in BSM.

If you want to use user-based LW-SSO authentication with BSM Integration Adapter, perform the following steps *before* configuring BSM Integration Adapter.

- a. In the BSM user interface, navigate to the Users and Permissions manager:

**Admin → Platform → Users and Permissions → Authentication Management**

- b. Click **Configure** to open the Authentication Wizard.
  - c. Click **Single Sign-On** and select **Lightweight**.
  - d. Generate the **Token Creation Key (initString)**.
  - e. Add your **Trusted Hosts/Domains**. For example, add the domain in which BSM and the BSM Integration Adapter instances are running.
  - f. Click **Finish** to save your changes and close the wizard.
2. *Group-based authentication only.* In BSM, make sure that user groups and user roles are enabled in LW-SSO tokens.

For details about how to configure infrastructure settings, see the Platform Administration online help in BSM.

- a. In the BSM user interface, navigate to the Infrastructure Settings manager:

**Admin → Platform → Setup and Maintenance → Infrastructure Settings**

- b. Click **Foundation** and select **Single Sign-On** in the drop-down list.
  - c. Set **Add user groups information to LW-SSO token** to **true**.
  - d. Set **Add user roles information to LW-SSO token** to **true**.
3. *Group-based authentication only.* In BSM, create groups, users, and roles (or use Lightweight Directory Access Protocol (LDAP) to map groups and synchronize BSM users with users configured on the external LDAP server).

**Tip:** When you configure BSM Integration Adapter, the configuration program by default adds the group `IA_ADMINS` and the role `SUPERUSER` to the BSM Integration Adapter SSO

configuration. The group `IA_ADMINS` does not by default exist in BSM. If you want to use the `IA_ADMINS` group, you must first add it to BSM and then add the desired users to the group.

#### **LW-SSO security warnings**

- Confidential `initString` parameter in LW-SSO security.

LW-SSO uses Symmetric Encryption to validate a LW-SSO token. The `initString` parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application that uses the same `initString` parameter validates the token.

#### **Caution:**

- It is not possible to use LW-SSO without setting the `initString` parameter.
- The `initString` parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
- The `initString` should be shared only between applications integrating with each other using LW-SSO.
- The minimum length of the `initString` is 12 characters.
- LW-SSO should be disabled unless it is specifically required.
- Symmetric encryption implication.

LW-SSO uses symmetric cryptography for issuing and validating LW-SSO Tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same `initString`. This potential risk is relevant when an application sharing the `initString` either resides or is accessible in an untrusted location.

## Prepare user-based LW-SSO authentication

In BSM, make sure that LW-SSO is enabled and write down the token key (initString). You need this information when configuring BSM Integration Adapter for SSO authentication.

For details about how to configure LW-SSO, see the section on *Users, Permissions, and Recipients* in the Platform Administration online help in BSM.

If you want to use user-based LW-SSO authentication with BSM Integration Adapter, perform the following steps *before* configuring BSM Integration Adapter.

1. In the BSM user interface, navigate to the Users and Permissions manager:  
**Admin** → **Platform** → **Users and Permissions** → **Authentication Management**
2. Click **Configure** to open the Authentication Wizard.
3. Click **Single Sign-On** and select **Lightweight**.
4. Generate the **Token Creation Key (initString)**.
5. Add your **Trusted Hosts/Domains**. For example, add the domain in which BSM and the BSM Integration Adapter instances are running.
6. Click **Finish** to save your changes and close the wizard.

After configuring BSM Integration Adapter using `ia-config`, continue configuring user-based LW-SSO as described in ["Configure user-based LW-SSO authentication" \(on page 25\)](#)



## Configure user-based LW-SSO authentication

To configure user-based authentication, you must add all BSM users that will gain access to BSM Integration Adapter to the BSM Integration Adapter local user store, and then modify the LW-SSO configuration file to activate the internal mode.

For more information about LW-SSO, see the *BSM Platform Administration* guide.

To configure user-based authentication for LW-SSO, perform the following steps *after* configuring BSM Integration Adapter.

1. On the BSM Integration Adapter system, add all BSM users that will access BSM Integration Adapter to the local user store.

*Windows only.* Run the user administration program:

- a. Open a command prompt and type:

```
cd %OvDataDir%\installation\HPOprIA
```

- b. Add the BSM users to the local user store, type:

```
ia-user.bat -add <BSM username> <BSM password>
```

*Linux only.* Start the BSM Integration Adapter user administration program, type:

```
/var/opt/OV/installation/HPOprIA/ia-user.sh -add <BSM username>  
<BSM password>
```

`ia-user` accepts the following options:

```
ia-user -help | -list | -add <username> <password> | -delete  
<username> | -version
```

### Command options

`-h,-help`

Shows tool usage and description.

`-l,-list`

Lists the users stored in the local user store.

`-a,-add <username> <password>`

Adds a user to the local users store. If the user already exists, the password is overwritten.

The username and password must contain ASCII characters only. The user name must contain at least three characters. Valid characters in user names are alphanumeric characters (a-z, A-Z, and 0-9), hyphens (-), underscores (\_), and periods (.).

`-d,-delete <username>`

Deletes the specified user from the local user store.

`-v,-version`

Displays the BSM Integration Adapter version number.

2. *Optional.* Review the log file at:

Windows: %OvDataDir%\log\HPOprIA-CLIs.log

Linux: /var/opt/OV/log/HPOprIA-CLIs.log

The program appends log information to the file when you run the program again.

*Windows only.* If the log file contains errors relating to the OvControl service failing to start or restart, complete the following steps:

- a. Manually reinstall ovcd as a Windows service, type:

```
ovcd -install
```

- b. Rerun ia-config.

3. Open the LW-SSO configuration file on the BSM Integration Adapter system:

Windows: %OvDataDir%\conf\HPOprIA\lwssso-config.xml

Linux: /var/opt/OV/conf/HPOprIA/lwssso-config.xml

4. In the LW-SSO configuration file, disable the external mode by enclosing it in the comment tag (<!-- -->).

```
<!-- EXTERNAL MODE -->
<!--
<lwssso-plugin type="SpringSecurity">
  <roleIntegration rolePrefix="ROLE_"
                  fromLWSSO2Plugin="external"
                  fromPlugin2LWSSO="enabled"
                  caseConversion="upperCase"/>
  <groupIntegration groupPrefix="ROLE_"
                   fromLWSSO2Plugin="external"
                   fromPlugin2LWSSO="enabled"
                   caseConversion="upperCase"/>
</lwssso-plugin>
-->
```

Enable the internal mode by removing the comment tag.

```
<!-- INTERNAL MODE -->
<lwssso-plugin type="SpringSecurity">
  <roleIntegration rolePrefix="ROLE_"
                  fromLWSSO2Plugin="internal"
                  fromPlugin2LWSSO="enabled"
                  caseConversion="upperCase"/>
</lwssso-plugin>
```

5. Restart Apache Tomcat, type:

Windows: ovc -restart ovtomcatB

Linux: opt/OV/bin/ovc -restart ovtomcatB

#### LW-SSO security warnings

- Confidential initString parameter in LW-SSO security.

LW-SSO uses Symmetric Encryption to validate a LW-SSO token. The `initString` parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application that uses the same `initString` parameter validates the token.

#### Caution:

- It is not possible to use LW-SSO without setting the `initString` parameter.
- The `initString` parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
- The `initString` should be shared only between applications integrating with each other using LW-SSO.
- The minimum length of the `initString` is 12 characters.
- LW-SSO should be disabled unless it is specifically required.
- Symmetric encryption implication.

LW-SSO uses symmetric cryptography for issuing and validating LW-SSO Tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same `initString`. This potential risk is relevant when an application sharing the `initString` either resides or is accessible in an untrusted location.

## Configure local user authentication

Each BSM Integration Adapter instance maintains a local user store. These users can access the local BSM Integration Adapter instance only and cannot not gain access to other BSM applications. When BSM users launch the BSM Integration Adapter user interface, they have to provide the credentials of a local BSM Integration Adapter user.

The BSM Integration Adapter configuration by default creates a user account in the local user store. The user store is located in the following file on the BSM Integration Adapter system:

**Windows:** `%OvDataDir%\conf\HPOprIA\users.properties`

**Linux:** `/var/opt/OV/conf/HPOprIA/users.properties`

To add additional users to the user store, run the BSM Integration Adapter user administration program `ia-user`.

`ia-user` accepts the following options:

```
ia-user -help | -list | -add <username> <password> | -delete  
<username> | -version
```

#### Command options

`-h,-help`

Shows tool usage and description.

`-l,-list`

Lists the users stored in the local user store.

`-a,-add <username> <password>`

Adds a user to the local users store. If the user already exists, the password is overwritten.

The username and password must contain ASCII characters only. The user name must contain at least three characters. Valid characters in user names are alphanumeric characters (a-z, A-Z, and 0-9), hyphens (-), underscores (\_), and periods (.).

`-d,-delete <username>`

Deletes the specified user from the local user store.

`-v,-version`

Displays the BSM Integration Adapter version number.

#### To add local users

1. *Windows only.* Run the user administration program:

- a. Open a command prompt and type:

```
cd %OvDataDir%\installation\HPOprIA
```

- b. Run the BSM Integration Adapter user administration program, type:

```
ia-user.bat -add <username> <password>
```

*Linux only.* Start the BSM Integration Adapter user administration program, type:

```
/var/opt/OV/installation/HPOprIA/ia-user.sh -add <username>  
<password>
```

2. *Optional.* Review the log file at:

**Windows:** %OvDataDir%\log\HPOprIA-CLIs.log

**Linux:** /var/opt/OV/log/HPOprIA-CLIs.log

The program appends log information to the file when you run the program again.

*Windows only.* If the log file contains errors relating to the OvControl service failing to start or restart, complete the following steps:

- a. Manually reinstall ovcd as a Windows service, type:

```
ovcd -install
```

- b. Rerun `ia-config`.

## Activate flexible management

To enable event forwarding to multiple BSM servers, activate the flexible management policy `BSM/OMi Integration` in the BSM Integration Adapter user interface.

The policy `BSM/OMi Integration` sends all events with the type attribute `BSM_IA_Message` to the new BSM server. Events that do not have this attribute set are sent to the old BSM server.

BSM Integration Adapter sets this attribute automatically to `BSM_IA_Message`. You can delete the value in a policy but BSM Integration Adapter inserts it again when you save the policy. The type attribute is available in the Advanced attributes tab of SNMP and XML interceptor policy editors.

**Note:** The agent sends *all* discovery data to the new BSM server. This includes new data discovered by already existing discovery policies.

**Note:** The flexible management policy `BSM/OMi Integration` cannot be edited in BSM Integration Adapter. If you no longer need the policy, deactivate it and delete it.

## Use ia-config in silent mode

The configuration program `ia-config` enables you to configure BSM Integration Adapter in silent or unattended mode. `ia-config` accepts the following options:

```
ia-config [ -help | -version | -silent [-srv <BSM_server>] [-cert_srv
<BSM_certificate_server>] [-force]
[-https_port <port_number>] [-http_port <port_number>] [-ssokey <BSM_
token_key>]
[-usr <user_name> -usrpwd <password>] ]
```

**Note:** Do not use the `-s`, `-cs`, and `-f` options when connecting BSM Integration Adapter to a BSM environment that includes a reverse proxy or load balancer. See ["Connect BSM Integration Adapter to a reverse proxy or load balancer" \(on page 20\)](#) for information about connecting BSM Integration Adapter to a reverse proxy or load balancer.

### Command options

`-h, -help`

Shows tool usage and description.

`-v, -version`

Displays the BSM Integration Adapter version number.

`-silent`

Configures BSM Integration Adapter in silent or unattended mode.

The `-silent` option uses the following defaults, if no additional options are provided:

Parameter	Default value	Description
Reconnect to another server	No	Applies to reconfigurations only. Use the <code>-f</code> option to reconfigure BSM Integration Adapter.
Flexible management policy	No	Applies to reconfigurations only. Use the <code>-f</code> option to force the configuration program to create a flexible management policy.
BSM certificate server	BSM server	Use the <code>-cert_srv</code> option to specify a dedicated certificate server.
Local user account	No	Use the <code>-usr</code> and <code>-usrpwd</code> options to create local user accounts.
Apache Tomcat HTTPS port	21350	Use the <code>-https_port</code> option to specify a different HTTPS port.
Apache Tomcat HTTP port	21351	Use the <code>-http_port</code> option to specify a different HTTP port.

Parameter	Default value	Description
Single sign-on	Disabled	Use the <code>-ssokey</code> option to specify the BSM token key.

`-s, -srv <BSM_server>`

Specifies the BSM server.

`<BSM_server>` is the fully qualified domain name (FQDN) of the BSM server. In a distributed BSM deployment, choose the gateway server.

**Caution:** Do not specify the HPOM management server. HP does not support environments with the HPOM management server acting as primary manager of a managed node that has BSM Integration Adapter installed.

`-cs, -cert_srv <BSM_certificate_server>`

Specifies the BSM certificate server.

`<BSM_certificate_server>` is the FQDN of the BSM certificate server. If your BSM deployment includes a dedicated certificate server, choose the FQDN of the certificate server. Otherwise type the FQDN of the gateway server. The gateway server forwards certificate requests to the data processing server, which by default also acts as certificate server.

If you omit this option, `ia-config` uses the BSM server.

`-f, -force`

Force mode (for example to reconfigure BSM Integration Adapter to connect to a different BSM server). This option also creates a flexible management policy. Flexible management policies enable HP Operations Agent to send events to multiple servers based on time and event attributes. If you allow the configuration program to create such a policy, the new server becomes the primary manager of the BSM Integration Adapter server. Both the old and the new server receive events from BSM Integration Adapter, but only the primary manager receives the discovery data.

**Note:** The flexible management policy cannot be edited in BSM Integration Adapter. If you no longer need the policy, deactivate it and delete it.

`-https_port <port_number>`

HTTPS port for the Apache Tomcat server. The default value is 21350.

`-http_port <port_number>`

HTTP port for the Apache Tomcat server. The default value is 21351.

`-ssokey <BSM_token_key>`

Specifies the token key generated in the BSM Users and Permissions manager.

The configuration program uses the following defaults:

Parameter	Default value
Domain Name (SSO)	Domain name of the BSM server. (Extracted from <code>&lt;BSM_server&gt;</code> .)
Accessible BSM Groups/Roles (SSO)	IA_ADMINS, SUPERUSER

`-usr <user_name>`

Name of an administration account in the BSM Integration Adapter local user store. The default is `admin`.

`-usrpwd <password>`

Password of the administration account. The default is `admin`.

## Accessing HP BSM Integration Adapter

You access BSM Integration Adapter using a supported web browser, from any computer with a network connection to a BSM Integration Adapter server. For more information about supported web browsers, see the *BSM Integration Adapter Release Notes*.

The BSM Integration Adapter user interface opens without prompting for user authentication if single sign-on (SSO) is configured and the user is already logged on to BSM. Alternatively, if local user authentication is configured, you can type the user name and password of a local BSM Integration Adapter user account.

## Start the HP BSM Integration Adapter user interface from a web browser

To start the BSM Integration Adapter user interface, open a web browser at the following URL:

`https://<Integration Adapter system>:21350/opr-policy-management/`

`<Integration Adapter system>` is `localhost` or the hostname of the BSM Integration Adapter server. If Apache Tomcat is configured to use a different port, use this port instead.

BSM Integration Adapter uses HTTPS to encrypt communication between the BSM Integration Adapter server and user interface. However, because the certificate that the user interface uses by default is not from a trusted certificate authority, you normally see certificate errors in the web browser when you connect to the BSM Integration Adapter server.

In Internet Explorer, the error states that there is a problem with the web site's security certificate. In Firefox, the error states that the connection is untrusted. In either case, you can continue to connect to the BSM Integration Adapter user interface by following the instructions that the browser provides. In Firefox, you can add an exception so that the security errors do not appear next time you connect to the web console.

After you start the BSM Integration Adapter user interface, depending on the security settings in your environment, you may have to log on. (See ["Log on to HP BSM Integration Adapter" \(on page 32\)](#).)

**Optional. Import a trusted certificate**

To prevent the certificate errors, you can obtain a certificate from a trusted certificate authority, and then import it into the BSM Integration Adapter keystore. The keystore location and password are:

Windows: %OvDataDir%\certificates\tomcat\b\tomcat.keystore

Linux: /var/opt/OV/certificates/tomcat/b/tomcat.keystore

Password: changeit

For example, to import a trusted certificate using the Java `keytool` command, type:

Windows: "%JAVA\_HOME%\bin\keytool" -import -alias <alias> -keystore "%OvDataDir%\certificates\tomcat\b\tomcat.keystore" -trustcacerts -file <file>

Linux: /opt/OV/nonOV/jre/b/bin/keytool -import -alias <alias> -keystore /var/opt/OV/certificates/tomcat/b/tomcat.keystore -trustcacerts -file <file>

After the certificate has been imported, restart Apache Tomcat:


Windows: `ovc -restart ovtomcatB`

Linux: `/opt/OV/bin/ovc -restart ovtomcatB`

## Start the HP BSM Integration Adapter user interface in BSM

BSM enables you to start the BSM Integration Adapter user interface directly from within Operations Management. The following integrations are available if you configure your BSM Integration Adapter server as a connected server in Operations Management:

- BSM Operations Management Connected Servers manager

You can start the BSM Integration Adapter user interface by clicking the  icon in the connected server details pane.

- BSM Operations Management Event Browser

You can start the BSM Integration Adapter user interface by right-clicking the event in the Operations Management Event Browser and selecting **Configure** → **Integration Policies**.

After you start the BSM Integration Adapter user interface, depending on the security settings in your environment, you may have to log on. (See ["Log on to HP BSM Integration Adapter" \(on page 32\)](#).)

## Log on to HP BSM Integration Adapter

Type the user name and password of a local user account. The user name and password of the default local user account is:

User name: `admin`

Password: `admin`

If you have added additional users to the local user store, you may also use one of these users. For details, see ["Configure local user authentication" \(on page 27\)](#).

The BSM Integration Adapter user interface opens without prompting for user authentication if single sign-on (SSO) is configured and the user is already logged on to BSM. In this case an LW-



SSO session cookie stored in the web browser contains the BSM authentication information. BSM users can access BSM Integration Adapter only if they have the necessary permissions (for example, if they have the `SUPERUSER` role assigned or are members of the `IA_ADMINS` group).

## Log out of HP BSM Integration Adapter

To log out of BSM Integration Adapter, click **Logout** at the top of the page.

If a user ends a BSM Integration Adapter user interface session by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option), BSM Integration Adapter automatically logs the user off after 60 seconds.

## Managing HP BSM Integration Adapter with HPOM

When you bring a BSM Integration Adapter system under HPOM management the BSM server remains the primary manager of BSM Integration Adapter. The HPOM management server becomes a secondary and action-allowed management server and can start actions, and deploy policies and packages.

BSM Integration Adapter sends all events with the type attribute `BSM_IA_Message` to the BSM server. Events that do not have this attribute set are sent to the HPOM management server. BSM Integration Adapter sets the event type attribute automatically to `BSM_IA_Message`. You can delete the value in a policy but BSM Integration Adapter inserts it again when you save the policy. The type attribute is available in the Advanced attributes tab of SNMP and XML interceptor policy editors.

**Note:** The agent sends all discovery data to the BSM server. This includes data discovered by service auto-discovery policies deployed from the HPOM management server.

**Note:** The flexible management policy cannot be edited in the BSM Integration Adapter user interface.

**Tip:** In the procedures below, use the `ovcoreid` command line tool to find out the required core ID of the system.

## To manage BSM Integration Adapter with HPOM for Windows

1. Exchange certificates between the BSM Integration Adapter and HPOM systems. For information about exchanging certificates, see ["Configure trusted certificates" \(on page 18\)](#).
2. On the HPOM management server, use the **Configure Managed Nodes** dialog box to add the BSM Integration Adapter system as a managed node. In the node's properties, manually add the core ID and set the certificate state to `Installed`.
3. On the BSM Integration Adapter system, create and activate an agent-based flexible management policy:
  - a. Make a copy of the flexible management policy template.  
BSM Integration Adapter on Windows  
Open a command prompt and type:

```
copy "%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-7A9492C35014_data.template" "%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-7A9492C35014_data"
```

```
copy "%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-7A9492C35014_header.xml.template" "%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-7A9492C35014_header.xml"
```

#### BSM Integration Adapter on Linux

Open a shell and type:

```
cp /var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-7A9492C35014_data.template /var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-7A9492C35014_data

cp /var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-7A9492C35014_header.xml.template /var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-7A9492C35014_header.xml
```

- b. Edit the policy data file `3F9A8F04-B5E3-43C3-999B-7A9492C35014_data`.
- c. Locate the string `${OM_MGR_SRV}` and replace all occurrences with the FQDN of the HPOM management server.

Locate the string `${OM_MGR_SRV_ID}` and replace all occurrences with the core ID of the HPOM management server.

- d. Locate the string `${OMi_MGR_SRV}` and replace all occurrences with the FQDN of the BSM gateway server.

Locate the string `${OMi_MGR_SRV_ID}` and replace all occurrences with the core ID of the BSM data processing server.

- e. Save the policy data file. Import the policy in BSM Integration Adapter and activate it.
4. In the HPOM console, right-click the node that represents the BSM Integration Adapter system and select **All Tasks** → **Synchronize inventory** → **Packages**.
5. On the HPOM management server, check that you can manage the BSM Integration Adapter system, type:

```
opcragt -status <BSM Integration Adapter hostname>
```

The output should indicate that the agent is running.

For more information about HPOM for Windows, see the HPOM for Windows online help.

## To manage BSM Integration Adapter with HPOM for UNIX or Linux

1. Exchange certificates between the BSM Integration Adapter and HPOM systems. For information about exchanging certificates, see ["Configure trusted certificates" \(on page 18\)](#).
2. On the HPOM management server, add the BSM Integration Adapter system as a managed node, type:

```
opcnode -add_node <BSM Integration Adapter hostname>
```

3. On the HPOM management server, specify the core ID of the BSM Integration Adapter server, type:

```
opcnode -chg_id node_name=<BSM Integration Adapter hostname>  
id=<core ID of BSM Integration Adapter system>
```

4. On the BSM Integration Adapter system, create and activate an agent-based flexible management policy:

- a. Make a copy of the flexible management policy template.

#### BSM Integration Adapter on Windows

Open a command prompt and type:

```
copy "%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-  
7A9492C35014_data.template" "%OvDataDir%\conf\HPOprIA\3F9A8F04-  
B5E3-43C3-999B-7A9492C35014_data"
```

```
copy "%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-  
7A9492C35014_header.xml.template"  
"%OvDataDir%\conf\HPOprIA\3F9A8F04-B5E3-43C3-999B-7A9492C35014_  
header.xml"
```

#### BSM Integration Adapter on Linux

Open a shell and type:

```
cp /var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-  
7A9492C35014_data.template /var/opt/OV/conf/HPOprIA/3F9A8F04-  
B5E3-43C3-999B-7A9492C35014_data
```

```
cp /var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-  
7A9492C35014_header.xml.template  
/var/opt/OV/conf/HPOprIA/3F9A8F04-B5E3-43C3-999B-7A9492C35014_  
header.xml
```

- b. Edit the policy data file 3F9A8F04-B5E3-43C3-999B-7A9492C35014\_data.
  - c. Locate the string `${OM_MGR_SRV}` and replace all occurrences with the FQDN of the HPOM management server.  
  
Locate the string `${OM_MGR_SRV_ID}` and replace all occurrences with the core ID of the HPOM management server.
  - d. Locate the string `${OMi_MGR_SRV}` and replace all occurrences with the FQDN of the BSM gateway server.  
  
Locate the string `${OMi_MGR_SRV_ID}` and replace all occurrences with the core ID of the BSM data processing server.
  - e. Save the policy data file. Import the policy in BSM Integration Adapter and activate it.
5. On the HPOM management server, check that you can manage the BSM Integration Adapter system, type:

```
opcragt -status <BSM Integration Adapter hostname>
```

The output should indicate that the agent is running.

## Using HP BSM Integration Adapter

### HP BSM Integration Adapter

---

For more information about HPOM for UNIX or Linux, see the documentation that HPOM for UNIX or Linux provides.

## Managing policies

Policies are collections of configuration information used to configure HP Operations Agent on the BSM Integration Adapter server to perform monitoring or discovery tasks. When you develop monitor policies, you decide what kinds of events to monitor, how often to monitor, what to look for in the events, and what to do if certain events are detected. Discovery policies automatically populate the BSM RTSM (Run-time Service Model) with topology data based on discovery scripts executed within the BSM Integration Adapter environment.

Rules define what a monitor policy should do in response to a specific type of event. Each rule consists of a condition and of settings for the event generated by the policy. The condition is the part of a policy that describes the type of event in the source. The settings enable you to configure the event that BSM Integration Adapter sends to the Operations Management Event Browser.

A policy must contain at least one rule. If the policy contains multiple rules, it is important to remember that the rules are evaluated in a specific order, and that when one condition is matched, no additional rules will be evaluated.

The rule types are:

- **Event on matched condition**  
If matched, BSM Integration Adapter sends an event to the Operations Management Event Browser. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used.
- **Suppress on matched condition**  
If matched, BSM Integration Adapter stops processing and does not send an event to the Operations Management Event Browser.
- **Suppress on unmatched condition**  
If not matched, BSM Integration Adapter stops processing and does not send an event to the Operations Management Event Browser.

BSM Integration Adapter enables you to create and edit policies of the type discovery, SNMP interceptor, and XML interceptor only. You can import policies developed on other servers, for example, HP Operations Manager (HPOM) management servers, HP Network Node Manager i (NNMi) management servers, or other BSM Integration Adapter servers.

When you create a new policy or import a policy, the policy exists in the BSM Integration Adapter policy repository but does not function yet. You must first activate the policy for it to start monitoring the corresponding event source or discovering topology data.

**Tip:** You can sort the information that appears in the columns in the BSM Integration Adapter policy list so that data appears in either ascending or descending order, indicated by either an up or down arrow at the top of the column. In addition, you can change the order of columns by dragging columns to other positions.

## Managing policies in cluster environments

Import and activate the same set of policies on all nodes in the cluster.


Make sure that you do not monitor data stored on the shared disk with the same policies activated on multiple cluster nodes. This may result in duplicate events in BSM after a failover. For example, do not activate the same XML interceptor policies on more than one cluster node if the policies monitor an XML file on the shared disk.

If the IP address of the resource group (also known as virtual IP address) sends SNMP events that you plan to capture, make sure that the IP address is set up as a CI (configuration item) with the attribute "host is virtual" in BSM. Otherwise the events display as unmapped events in the Operations Management Event Browser.

## Edit policies

BSM Integration Adapter enables multiple users to connect to the same server at the same time. However, only one user at a time can edit a policy to prevent changes from other users overwriting each other.




When you edit a policy, BSM Integration Adapter locks the policy for you so that only you can save the policy. Note that if you open a policy more than once, only the first editor instance receives the lock and can save the policy.


Locked policies display with a lock icon  and the name of the editing user in the list of policies in the BSM Integration Adapter user interface. (The tooltip explains who locked the policy and when.)

BSM Integration Adapter releases the lock when the policy is closed or when a user forcefully breaks the lock. It is recommended that you only break the edit lock when you have reason to believe that the locked policy editor was abandoned or stopped working. Policy editors that have been forcefully unlocked by another user change to read-only mode and you can no longer save any changes made.


**Tip:** When you open a locked policy for viewing, reload the policy from time to time to ensure that you are viewing the most recently saved version.

## To edit unlocked policies

1. In the list of policies in the BSM Integration Adapter user interface, select the policy that you want to edit.
2. Click  in the toolbar. The policy editor opens. The policy is marked with the lock icon  and the name of the editing user in the list of policies in the BSM Integration Adapter user interface.
3. Modify the policy.
4. Click  in the toolbar to save the policy and close the editor.



**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.


## To break the edit lock on locked policies

1. In the list of policies in the BSM Integration Adapter user interface, select the locked policy that you want to edit.
2. Click  in the toolbar. A dialog box opens and lists the name of the editing user, the hostname of the BSM Integration Adapter server, and the date and time the policy was locked.

The date and time displays using the current time zone of the computer on which the BSM Integration Adapter user interface runs. The language setting of the web browser determines the date and time format (for example, 09/14/2010 8:16:38 AM for English (United

States)). If the web browser and the computer on which the BSM Integration Adapter server run have different language settings, the language setting of the web browser takes precedence. However, English is the default language if the web browser is configured to use a language that is not available on the server.

3. Click **OK** to break the edit lock. The lock icon  and the name of the editing user disappear from the list of policies in the BSM Integration Adapter user interface..
4. Open the policy for editing and modify it.
5. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.


**Tip:** You can unlock a policy at any time, even while editing.

## Copy policies

Instead of creating a new policy from scratch, you can copy an existing policy and change the copy to meet your needs. Copied policies are by default deactivated.

**Note:** You can copy only one policy at a time.


### To copy a policy

1. In the list of policies in the BSM Integration Adapter user interface, select a policy.
2. Click  in the toolbar. The **Copy Policy** dialog box opens.
3. Change the policy name and optionally the description.
4. Click **OK**. The copied policy appears in the list of policies in the BSM Integration Adapter user interface and is by default deactivated.

## Delete policies

You can only delete deactivated policies and policies that are not being edited by other users. When you delete a policy the policy files are deleted from the file system. To temporarily stop a policy from functioning, deactivate the policy instead.

### To delete policies

1. In the list of policies in the BSM Integration Adapter user interface, select the policies that you want to delete.
2. Make sure that the policies are deactivated and not being edited.
3. Click  in the toolbar. A message box opens.
4. Confirm that you want to delete the policies.

## Activate and deactivate policies


When you create a new policy or import a policy, the policy exists in the BSM Integration Adapter policy repository but does not function yet. You must first activate the policy for it to start monitoring

the corresponding event source or discovering topology data.


When you edit an existing, active policy, the previous version of the policy remains active on the BSM Integration Adapter server and you must reactivate the policy for your changes to take effect.

When you deactivate a policy, the policy remains in the BSM Integration Adapter policy repository but does not function until it is activated again.

## To activate policies

1. In the list of policies in the BSM Integration Adapter user interface, select the policies that you want to activate. The activation state of at least one of the selected policies must be `deactivated` or `activated (reactivate for new version)`. (If you include an already activated policy in your selection, the policy is ignored and not activated again.)
2. Click  in the toolbar. The activation state changes to `activated`.

## To deactivate policies

1. In the list of policies in the BSM Integration Adapter user interface, select the policies that you want to deactivate. (If you include an already deactivated policy in your selection, the policy is ignored and not deactivated again.)
2. Click  in the toolbar. The activation state changes to `deactivated`.

## Import policies

BSM Integration Adapter enables you to create and edit policies of the type discovery, SNMP interceptor, and XML interceptor only. You can import policies developed on other servers, for example, HP Operations Manager (HPOM) management servers, HP Network Node Manager i (NNMi) management servers, or other BSM Integration Adapter servers.

**Note:** Although you can import and activate HPOM service auto-discovery policies you cannot edit them because they are incompatible with the BSM Integration Adapter discovery policy editor.

When you download policies on an HPOM management server, make sure the resulting policy files support the XML-based policy exchange format:

- HP Operations Manager for Windows: use the `ovpmutil` command line utility.
- HP Operations Manager for UNIX or Linux: use the `opccfgdwn` command line tool.

NNMi provides the `nnmopcexport.ovpl` command line tool, which exports an SNMP interceptor policy for use with BSM Integration Adapter. For more information about running this tool and the NNMi integration in general, see the *NNMi Deployment Reference*.


You can also import policies developed on other BSM Integration Adapter systems, for example, to ensure that the same set of policies is available on multiple BSM Integration Adapter systems. This is necessary, for example, when running BSM Integration Adapter in a cluster environment.

BSM Integration Adapter stores policies in the following folders:

- Windows: `%OvDataDir%\datafiles\policymanagement\store`
- Linux: `/var/opt/OV/datafiles/policymanagement/store`



## To import policies


1. In the BSM Integration Adapter user interface, click  in the toolbar. A file selection dialog box opens.
2. Navigate to the policy files and, for each policy, select both the header (\*\_header.xml) and the data (\*\_data) files. You can import up to 100 policies at once (that is, 200 policy files).
3. Click **Open** to start the import process.

If the same policies already exist in BSM Integration Adapter, you are asked whether you would like to replace them with the newly imported policies.


The imported policies appear in the list of policies in the BSM Integration Adapter user interface. They are by default deactivated.

## Configure policy management options

You can choose to show any combination of the following columns in the BSM Integration Adapter policy list:

Column	Description
Policy Type	The policy type indicates the function of the policy.
Policy ID	GUID (globally unique identifier) of the policy.
Name	Name of the policy.
Description	Description of the policy.
Activation State	The activation state indicates if a policy is activated, deactivated, or needs reactivation after modification.
Edited by	The lock icon  and the name of the editing user indicate that a policy is being edited and by whom.

## To change the column display

1. Click  in the toolbar. The **Options** dialog box opens.
2. Select or clear the check box beside the column you want to show or hide.
3. Click **OK** to save your changes and close the dialog box.



**Tip:** Click **Default** to restore the default selections.

## Developing discovery policies


Discovery policies automatically populate the BSM RTSM (Run-time Service Model), based on discovery scripts executed within the BSM Integration Adapter environment. Discovered attributes may be hardware resources, operating system attributes, applications, and other information that can be retrieved from an object and mapped to CI attributes in the RTSM (Run-time Service Model). The discovery scripts run according to a schedule that you specify for each policy.



**Note:** Although you can import and activate HPOM service auto-discovery policies you cannot edit them because they are incompatible with the BSM Integration Adapter discovery policy editor.

### To configure a discovery policy

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **Discovery**. The discovery policy editor opens.

Alternatively, double-click an existing discovery policy to edit it.



2. Complete the information in the following tabs:
  - **Properties** include information that is related to the policy itself (for example, the name and description of the policy).
  - **Command** defines the script or program that the HP Operations agent runs to discover configuration items.
  - **Schedule** defines the time, date, and frequency of discovery.
3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.
4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

### Configure discovery policy properties

Every policy has a set of properties that identify and describe the policy.


### To configure properties of discovery policies



1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **Discovery**. The discovery policy editor opens.

Alternatively, double-click an existing discovery policy to edit it.

2. Click **Properties**.
3. *Required.* In the **Name** box, type a name that will identify the policy. You can use spaces in policy names. The equal sign (=) is not allowed.
4. *Optional.* In the **Description** box, type a description of what the policy does. You might also add other notes, for example data sources that are used.

5. *Optional.* In the **Category** box, type one or more arbitrary categories. Policy categories may help you to better group your policies. Separate multiple categories with commas.
6. **Policy ID:** BSM Integration Adapter automatically assigns a GUID (globally unique identifier) to the policy when it is first created.
7. **Last modification:** The date and time that the policy was saved.

The date and time displays using the current time zone of the computer on which the BSM Integration Adapter user interface runs. The language setting of the web browser determines the date and time format (for example, 09/14/2010 8:16:38 AM for English (United States)). If the web browser and the computer on which the BSM Integration Adapter server run have different language settings, the language setting of the web browser takes precedence. However, English is the default language if the web browser is configured to use a language that is not available on the server.
8. **Last modified by:** The name of the user active when the policy was saved.
9. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.
10. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure commands in discovery policies

Configuring a discovery policy includes creating a script (or program) that the HP Operations agent can run on the BSM Integration Adapter system to discover configuration items (CIs) and CI relations. This discovery script must write details of each discovered CI in XML to the standard output stream (STDOUT). The agent stores these details in the agent repository, which is a local data store of CIs that exist in the BSM Integration Adapter environment. The agent publishes details of new, changed, and removed CIs to the BSM RTSM (Run-time Service Model), but does not resend details of unchanged CIs.

### Configuration Item XML Schema Definition (XSD)

Your discovery script must output XML that conforms to the following schema:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Service">
    <xs:complexType>
      <xs:choice maxOccurs="unbounded">
        <xs:element ref="NewInstance" />
        <xs:element ref="DeleteInstance" />
        <xs:element ref="NewRelationship" />
        <xs:element ref="DeleteRelationship" />
      </xs:choice>
    </xs:complexType>
    <xs:key name="InstanceKey">
      <xs:selector xpath="NewInstance|DeleteInstance">
    </xs:selector>
```

```

        <xs:field xpath="Key"></xs:field>
    </xs:key>
    <xs:keyref refer="InstanceKey" name="InstanceKeyRef">
        <xs:selector xpath="NewInstance|DeleteInstance">
            </xs:selector>
        <xs:field xpath="@ref"></xs:field>
    </xs:keyref>
    <xs:keyref refer="InstanceKey" name="InstanceRef">
        <xs:selector
xpath="NewRelationship/*/Instance|DeleteRelationship/*/Instance">
            </xs:selector>
        <xs:field xpath="@ref"></xs:field>
    </xs:keyref>
</xs:element>
<xs:element name="NewInstance" type="InstanceType" />
<xs:element name="DeleteInstance" type="InstanceType" />
<xs:complexType name="InstanceType">
    <xs:sequence>
        <xs:element ref="Std" />
        <xs:element ref="Virtual" minOccurs="0" />
        <xs:element ref="Key" />
        <xs:element ref="Attributes" />
    </xs:sequence>
    <xs:attribute name="ref" type="xs:string" use="required" />
</xs:complexType>
<xs:element name="NewRelationship" type="RelationType" />
<xs:element name="DeleteRelationship" type="RelationType" />
<xs:complexType name="RelationType">
    <xs:sequence>
        <xs:element ref="Parent" />
        <xs:element ref="GenericRelations" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
<xs:element name="Std">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="DiscoveredElement" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="Virtual">
    <xs:complexType />
</xs:element>
<xs:element name="Key" type="xs:string" />
<xs:element name="Attributes">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="Attribute" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>

```

```

</xs:element>
<xs:element name="Attribute">
  <xs:complexType>
    <xs:attribute name="value" type="xs:string" use="required" />
    <xs:attribute name="name" type="xs:string" use="required" />
  </xs:complexType>
</xs:element>
<xs:element name="Parent">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="Instance" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="GenericRelations" type="RelationsList" />
<xs:complexType name="RelationsList">
  <xs:sequence>
    <xs:element name="Relations" maxOccurs="unbounded">
      <xs:complexType>
        <xs:attribute name="type" type="xs:string"
use="required" />
        <xs:sequence>
          <xs:element ref="Instance" maxOccurs="unbounded" />
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:element name="Instance">
  <xs:complexType>
    <xs:attribute name="ref" type="xs:string" use="required" />
  </xs:complexType>
</xs:element>
</xs:schema>

```

The following table describes the elements that the XML document can contain.

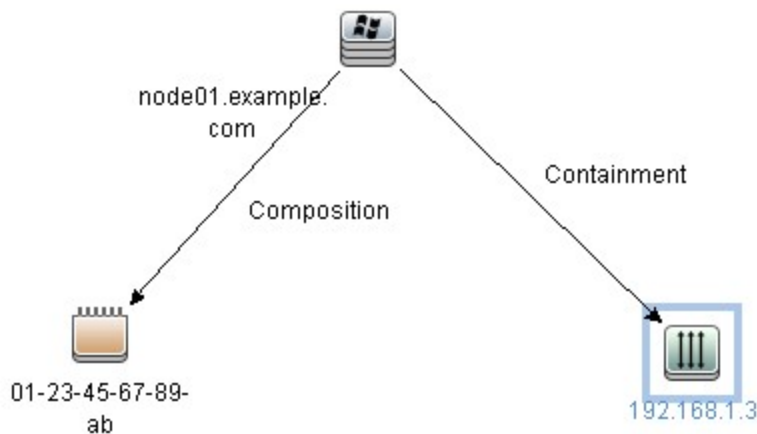
Element	Description
NewInstance	Represents a discovered CI. You must add a <code>ref</code> attribute, which must match the unique CI ID that you specify in the <code>Key</code> element. You can then use this reference in <code>Instance</code> elements in the current XML document if you want to create or delete relationships.
DeleteInstance	Represents a CI that you want to delete immediately.  The agent automatically deletes previously discovered CIs from the agent repository if your discovery script runs five times (by default) without including the CI as a <code>NewInstance</code> in the XML document.  You can control how often the discovery script must run before a missing CI is automatically deleted by changing the agent parameter <code>INSTANCE_</code>

Element	Description
	<p>DELETION_THRESHOLD in the <code>agtrep</code> namespace.</p> <p>However, if you specify this element, the agent deletes the CI immediately and publishes the change to the RTSM (Run-time Service Model).</p>
NewRelationship	Defines a new relationship between CIs. This element must contain exactly one <i>Parent</i> element and can contain one or more <i>GenericRelations</i> elements.
DeleteRelationship	Defines relationships that you want to delete. This element must contain exactly one <i>Parent</i> element and can contain one or more <i>GenericRelations</i> elements.
Std	Must contain the string <code>DiscoveredElement</code> .
Virtual	Include this element if the CI is virtual. A virtual CI is abstract and does not exist on any node CI. Omit this element if the CI is hosted on a node CI.
Key	Contains the full CI ID for this CI, which must be unique. You must include this element in all <i>NewInstance</i> and <i>DeleteInstance</i> elements. You must not specify a <i>NewInstance</i> and <i>DeleteInstance</i> with the same key in the same XML document.
Attributes	Contains <i>Attribute</i> elements.
Attribute	<p>Has a <code>name</code> attribute and a <code>value</code> attribute.</p> <p>Attributes with the following names have a special meaning:</p> <ul style="list-style-type: none"> <li><code>hpon_citype</code> specifies the CI type as stored in the RTSM (Run-time Service Model) (for example, <code>nt</code>).</li> </ul> <p>The <code>default</code> synchronization package on the BSM server assigns the context <code>IntegrationAdapter</code> to all CIs that have a <code>hpon_citype</code> attribute so that they are included for topology synchronization. CIs that do not have this attribute are filtered out and excluded from topology synchronization.</p> <ul style="list-style-type: none"> <li><code>hpon_rootcontainer</code> specifies the full ID of the CI that contains or hosts this CI. Maps to the CI attribute <code>Container</code>. Creates a composition relationship.</li> <li>Attribute names with the prefix <code>ucmdb_map</code> directly to CI attributes (for example, <code>ucmdb_primary_dns_name</code> maps to the CI attribute <code>Primary DNS Name</code>).</li> </ul>

Element	Description
Parent	<p>Contains an <i>Instance</i> element, which defines the CI that is the parent of this relationship.</p> <p>The parent instance that you specify must exist in the RTSM (Run-time Service Model) and in the agent repository BSM Integration Adapter server. Therefore, you may need to include a <i>NewInstance</i> element to add the parent to the agent repository, even if the parent already exists in the RTSM (Run-time Service Model).</p>
Instance	Has a <code>ref</code> attribute that refers to a <i>NewInstance</i> element in the current XML document.
GenericRelations	Contains one or more <i>Relations</i> elements.
Relations	Has a <code>type</code> attribute that refers to the type of relation as stored in the RTSM (Run-time Service Model) (for example, <code>usage</code> ). Contains one or more <i>Instance</i> elements, which refer to the CIs that are related to the specified <i>Parent</i> element.

#### Example Discovery XML

The following example XML creates a node instance with related IP address and MAC address instances. The IP address instance has a containment relationship and the MAC address has a composition relationship to the node instance:



```
<Service>
  <NewInstance>
    <Std>DiscoveredElement</Std>
    <Key>CBA3A4AC-2EC5-11E0-8071-4876DFD72085</Key>
    <Virtual />
    <Attributes>
      <!-- use nt as CI type attribute -->
      <Attribute name="hpom_citype" value="nt" />
      <!-- use node01 as name attribute -->
    </Attributes>
  </NewInstance>
  <Relations>
    <Relation type="Composition">
      <Instance ref="01-23-45-67-89-ab" />
    </Relation>
    <Relation type="Containment">
      <Instance ref="192.168.1.3" />
    </Relation>
  </Relations>
</Service>
```

```

        <Attribute name="ucmdb_name" value="node01" />
        <!-- use node01.example.com as primary_dns_name attribute -->
        <Attribute name="ucmdb_primary_dns_name"
value="node01.example.com" />
        <!-- use node01.example.com as user_label attribute -->
        <Attribute name="ucmdb_user_label" value="node01.example.com"
/>



        <!-- use "Windows 2003 R2 64 Bit" as discovered_os_name
attribute -->
        <Attribute name="ucmdb_discovered_os_name" value="Windows
2003 R2 64 Bit" />
    </Attributes>
</NewInstance>
<NewInstance>
    <Std>DiscoveredElement</Std>
    <Key>E0AD966E-2EC5-11E0-B5C8-4E76DFD72085</Key>
    <Virtual />
    <Attributes>
        <Attribute name="hpom_citype" value="ip_address" />
        <!-- use 192.168.1.3 as name attribute -->
        <Attribute name="ucmdb_name" value="192.168.1.3" />
        <Attribute name="ucmdb_routing_domain" value="DefaultDomain"
/>
    </Attributes>
</NewInstance>
<NewInstance>
    <Std>DiscoveredElement</Std>
    <Key>157C8328-2EC6-11E0-931A-C176DFD72085</Key>
    <Virtual />
    <Attributes>
        <!-- relation to the MAC address is composition -->
        <!-- this is handled by the attribute hpom_rootcontainer -->
        <Attribute name="hpom_rootcontainer" value="CBA3A4AC-2EC5-
11E0-8071-4876DFD72085" />
        <Attribute name="hpom_citype" value="interface" />
        <Attribute name="ucmdb_name" value="Intel(R) PRO/1000 MT
Network Connection" />
        <Attribute name="ucmdb_mac_address" value="01-23-45-67-89-ab"
/>
    </Attributes>
    <Attribute name="ucmdb_interface_description" value="Intel(R)
PRO/1000 MT Network Connection" />
    <Attribute name="ucmdb_description" value="Intel(R) PRO/1000
MT Network Connection" />
    </Attributes>
</NewInstance>
<NewRelationship>
    <!-- create relationship of type containment between node (node01)
-->
    <!-- and IP address (192.168.1.3) -->
    <Parent>

```



```
<Instance>
  <Key>CBA3A4AC-2EC5-11E0-8071-4876DFD72085</Key>
  <Virtual/>
  <Std>DiscoveredElement</Std>
</Instance>
</Parent>
<GenericRelations>
  <Relations type="containment">
    <Instance>
      <Key>E0AD966E-2EC5-11E0-B5C8-4E76DFD72085</Key>
      <Virtual/>
      <Std>DiscoveredElement</Std>
    </Instance>
  </Relations>
</GenericRelations>
</NewRelationship>
</Service>
```

## To configure the command of discovery policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **Discovery**. The discovery policy editor opens.

Alternatively, double-click an existing discovery policy to edit it.


2. Click **Command**.
3. Type the name of your discovery script in the **Command** box. For example, you could specify the command line "\$ACTION\_DIR/custom\_discovery.cmd".


\$ACTION\_DIR represents the folder that contains instrumentation on the BSM Integration Adapter system:


**Windows:** %OvDataDir%\bin\instrumentation

**Linux:** /var/opt/OV/bin/instrumentation

Escape any backslashes (\) with a second backslash (\\).

4. *Optional.* By default, the HP Operations agent starts the discovery script under the same account as the agent is running under, which is Local System or root by default. You can specify a different user and password if you want the script to run under a different account.
5. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

6. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

**Tip:** The maximum frequency that you can schedule for a discovery policy is hourly. This frequency may not be convenient when you are developing and testing your policy. However, after you



activate the policy, you can run the policy on demand using the command `ovagtrep -run <policy name>` on the BSM Integration Adapter system.

## Configure schedules in discovery policy

Use the Schedule tab of the discovery policy editor to specify a discovery schedule for the current policy. By default, a discovery policy runs the discovery script every Sunday at 00:00.

**Tip:** You can associate a single schedule only with a discovery policy. To run the same discovery script according to different schedules, create a policy for each schedule. This enables you to, for example, run a discovery script Monday to Friday at 15:00, and Saturday and Sunday at 16:00.

## To configure the schedule of discovery policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **Discovery**. The discovery policy editor opens.

Alternatively, double-click an existing discovery policy to edit it.

2. Click **Schedule**.

3. Indicate when the discovery script should run:

- **Days of Week:** Specify the day or multiple days of the week that the discovery script should run.

To specify the day of the week, click the day in the **Days of Week** display. To select multiple days, click a day, press **Ctrl** or **Shift**, and select additional days. A blue bar indicates your choice.

- **Hours of Day:** Specify the specific hour or multiple hours of day that the discovery script should run.


To specify the hour of the day, click the hour in the **Hours of Day** display. To select multiple hours, click an hour, press **Ctrl** or **Shift**, and select additional hours. A blue bar indicates your choice.


- **Minute of Hour:** Specify the minute or multiple minutes within the hour that the discovery script should run. The maximum frequency is once in five minutes.

To specify the minute of the hour, click one of the five-minute intervals in the **Minute of Day** display. To select multiple intervals, click an interval, press **Ctrl** or **Shift**, and select additional intervals. A blue bar indicates your choice.

Your choices are summarized in the **Schedule Summary** at the bottom of the page.

4. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

5. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Developing SNMP interceptor policies

This policy type monitors SNMP events, and responds when a character pattern that you choose is found in an SNMP trap. Choose this policy type if you want to monitor network components that send SNMP traps.

**Tip:** When you install BSM Integration Adapter on an HP Network Node Manager i (NNMi) management server, you must enable the HP Operations Agent integration with NNMi so that the HP Operations Agent can receive SNMP traps from the NNMi northbound interface. To enable the NNMi integration, follow the procedures in the *NNMi Deployment Reference* instead of the one below.

### To configure HP Operations Agent to receive SNMP traps

By default, the trap interceptor (opctrapi) of HP Operations Agent uses the Net-SNMP APIs to receive SNMPv1 and SNMPv2 traps at port 162. If port 162 is already bound by another process (for example the Microsoft SNMP Trap service or the Linux snmptrapd process), the trap interceptor fails to start.

You can reconfigure the trap interceptor to listen at another port by setting the `SNMP_TRAP_PORT` variable. Alternatively, for Windows systems, you can configure the trap interceptor to subscribe to the Microsoft SNMP Trap service. This configuration provides the trap interceptor with SNMPv1 traps only.

To configure HP Operations Agent for the Microsoft SNMP Trap service, complete the following steps:

1. Open a command prompt, and then type:



```
ovconfchg -ns eaagt -set SNMP_SESSION_MODE WIN_SNMP
```

2. Restart the trap interceptor process:

```
ovc -restart opctrapi
```

For more information about the `SNMP_SESSION_MODE` and `SNMP_TRAP_PORT` variables, see the HP Operations Agent documentation.


### To configure an SNMP interceptor policy


1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **SNMP**. The SNMP interceptor policy editor opens.


Alternatively, double-click an existing SNMP interceptor policy to edit it.

2. Complete the information in the following tabs:

- **Properties** include information that is related to the policy itself (for example, the name and description of the policy).
- The policy **defaults** include default settings for all events generated by the policy (for example, default event attributes).
- **Rules** define what the policy should do in response to a specific type of event.
- **Options** configure several policy behaviors (for example, pattern matching options).

3. Click  in the toolbar to save the policy and close the editor.



**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure SNMP interceptor policy properties

Every policy has a set of properties that identify and describe the policy.

### To configure properties of SNMP interceptor policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **SNMP**. The SNMP interceptor policy editor opens.


Alternatively, double-click an existing SNMP interceptor policy to edit it.


2. Click **Properties**.
3. *Required.* In the **Name** box, type a name that will identify the policy. You can use spaces in policy names. The equal sign (=) is not allowed.
4. *Optional.* In the **Description** box, type a description of what the policy does. You might also add other notes, for example data sources that are used.
5. *Optional.* In the **Category** box, type one or more arbitrary categories. Policy categories may help you to better group your policies. Separate multiple categories with commas.
6. **Policy ID:** BSM Integration Adapter automatically assigns a GUID (globally unique identifier) to the policy when it is first created.
7. **Last modification:** The date and time that the policy was saved.

The date and time displays using the current time zone of the computer on which the BSM Integration Adapter user interface runs. The language setting of the web browser determines the date and time format (for example, 09/14/2010 8:16:38 AM for English (United States)). If the web browser and the computer on which the BSM Integration Adapter server run have different language settings, the language setting of the web browser takes precedence. However, English is the default language if the web browser is configured to use a language that is not available on the server.

8. **Last modified by:** The name of the user active when the policy was saved.

9. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.



10. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure event defaults in SNMP interceptor policies

The Defaults tab enables you to indicate default settings for all events generated by the policy.

These defaults affect all new and existing rules. You can override the defaults in individual rules if needed. If a rule contains empty event attributes, the agent will use the defaults for the new event.

## To configure attribute defaults in SNMP interceptor policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **SNMP**. The SNMP interceptor policy editor opens.

Alternatively, double-click an existing SNMP interceptor policy to edit it.

2. Click **Defaults - Event**. The default settings include:

- Configure event attributes

The event attributes tab enables you to set the event attributes for the event defaults. These attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events.

- **Severity:** Severity assigned to the event (Critical, Major, Minor, Warning, Normal, Unknown).
- **Category:** Name of the logical group to which the event belongs (for example, Database, Security, or Network). The event category is similar in concept to the HP Operations Manager message group.
- **Related CI:** Contains the related CI hint, which BSM uses to identify the CI related to the event (for example, oraclesid01@@node.example.com or C:@@server.example.com). Use the format `<hint 1>:<hint 2>:...:<hint n>@@<hostname>`.

### Best practices for related CI hints

The related CI hint should have sufficient hints to find the corresponding CI.

It is necessary to differentiate between CIs that have a composition relationship to a host, and those that do not have such a relation:

- For “hosted on” CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>@@<hostname>
```

Typically, a “hosted on” CI is a sub-type of “software element”. For example, a CI of type `websphereas` has a container-link relation to the host.

Another example is the exchange server role CI type `exchangeclientaccessserver`. The root-container for this CI type is a software element, and for that CI type the root-container is host.

- For virtual CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>
```

A virtual CI does not have a strong containment relation (container-link or root-container) to a host.

An example of a typical virtual CI type is cluster. This CI type does not have a strong containment relation to a host.

**Tip:** If you have problems resolving non-hosted CIs, provide the RTSM ID of the desired CI as a hint using the format `UCMDB:<ci_uuid>`.

For more information about CI resolution in BSM, see the *Using Operations Management* PDF or online help.

- **Configure event correlation**

Event correlation helps to prevent the Operations Management Event Browser from becoming cluttered by events that describe the same problem. When event correlation is enabled, you can set the type of duplicate event suppression and define the method used to suppress duplicate events.

- **Event Key:** An identifier used to identify duplicates and for Close Events with Key.
- **Close Events with Key:** If events with the event key that you type here exist in the Operations Management Event Browser when this event is received, these events are automatically closed. You can use pattern matching and variables to match multiple event keys. For example, consider the following pattern:

```
<${MSG_SEV}>:<${MSG_NODE_NAME}>:<5*>
```

This pattern is evaluated by first replacing the variables with the values that they resolve to, for example:

```
critical:cabbage.example.com:<5*>
```

This pattern is then compared using pattern matching rule against the event keys for all events in the Operations Management Event Browser. The pattern above would match the following event keys:

```
critical:cabbage.example.com:12345  
critical:cabbage.example.com:TEST1
```

- **Deduplication on Server:** Clear to disable deduplication on the server. Stops automatic discarding of new events that are duplicates of existing events.

**Suppress events which are:**

- **Generated by the same rule:** Select this option to suppress events that match the pattern specified for the selected rule. This is a more general setting for the suppression of duplicate events. For example, an XML log file entry policy might contain a rule with this match pattern: `Error Message<#>` The log file lines `Error Message10` and `Error Message20` are not identical, but would both match this rule.
- **Generated by the same input event:** Select this option to suppress events that were

sent in response to two separate input events that are identical except for the date and time that the event was generated (for example, identical entries in an XML log file).

- **Identical relative to their attributes:** Select this option to suppress either events that have the same event key or (if no event key is present) events that have identical event attributes (except for the date and time that the event was generated).

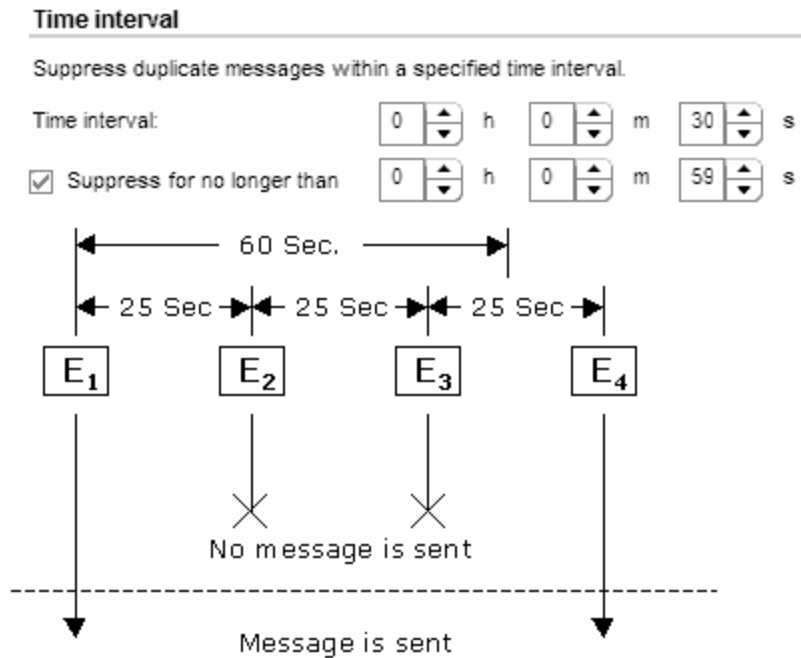
### Suppression Method

For event correlation, you can define one of three correlation methods:

- **Time interval:** This correlation method lets you define an interval during which duplicate events will be ignored. For more information, read this [detailed example](#).

### Time interval correlation example

In the illustration below, the interval is set to 30 seconds, but the suppression is limited to 60 seconds.

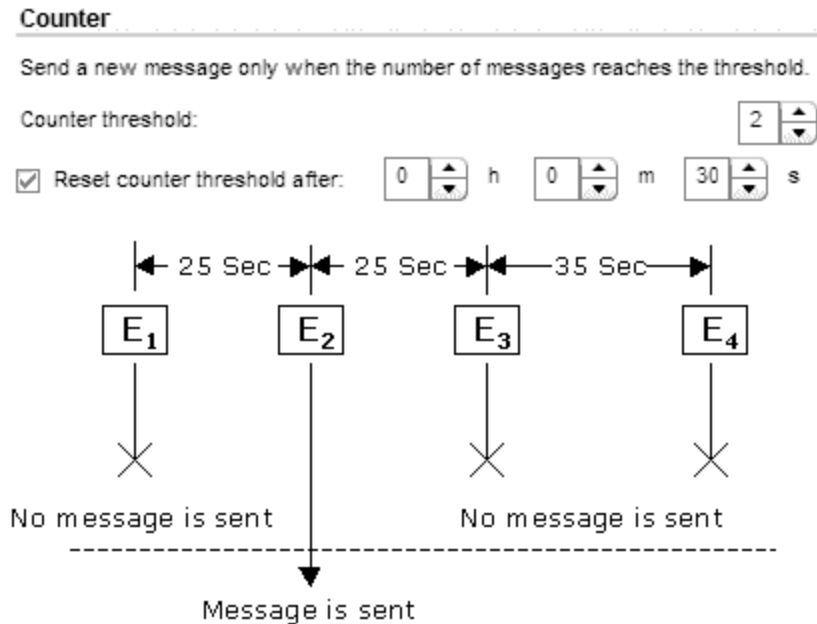


The **E<sub>x</sub>** represents events that are identical.

- The first input event (E<sub>1</sub>) matches a rule in the policy. The policy sends an event and starts timing.
- A second matching event (E<sub>2</sub>) occurs 25 seconds later. This event occurred *less than 30* seconds after the first event, and is therefore suppressed.
- A third matching event (E<sub>3</sub>) occurs *less than 30 seconds after the second event*, and so is also suppressed.

- The next matching event (E4) occurs less than thirty seconds after the third event, but is also *more than 60 seconds after the first event*, and therefore the policy sends an event.
- **Counter:** This correlation method counts the number of matching input events and sends an event only after the number of matching input events equals the counter threshold. The counter can also be reset to zero after a time period that you specify. For more information, read this [detailed example](#).

#### Counter correlation example



The **E<sub>x</sub>** represent events that are identical.

- The first input event (E1) matches a rule in the policy, and the counter increments to one. No event is sent.
- A second matching event (E2) occurs, the counter increments to two, an event is sent, and the counter resets.
- A third matching event (E3), and the counter increments to one no event is sent.
- The next matching event (E4) occurs *more than thirty seconds* after the third event. Since at thirty seconds the counter was reset to zero, the counter now increments to one no event is sent.
- **Time interval/Counter** If you use the Time interval and Counter together, events are evaluated first by the timer. If an event passes the timer, it is then evaluated by the counter, which either suppresses it or sends an event to the Operations Management Event Browser.



**Note:** If you specify just time interval correlation or just counter-based correlation in an individual event, any event defaults for the other correlation method also apply. For example, if you specify time interval correlation for an event, and the event defaults specify counter-based correlation, the combined time interval and counter-based correlation applies to both new rules and existing rules.

You can change this default behavior, so that only the correlation method that you specify in the individual event applies. To change the default behavior, set the parameter `OPC_IGNORE_DEFAULT_MSG_CORRELATION=TRUE` in the `eaagt` namespace on the node. You can configure this parameter using `ovconfchg` or `ovconfpar` at a command prompt.

- **Configure advanced attributes**

The advanced attributes tab enables you to specify additional HPOM-related attributes and to configure the interface between messages and external programs on the HP Operations Agent.

- **OM attributes**

HPOM-related attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events. Some attributes are used by CI resolution to relate the event to the impaired CI.

- **Application:** Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, Oracle and OS).
- **Object:** Device such as a computer, printer, or modem. Unlike the Related CI attribute, which is a direct relationship to a CI in the the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, C:, and /dev/spool).
- **HPOM Service ID:** ID of the service associated the event. A service ID is a unique identifier for a service and can be used in BSM to identify the node and CI associated with the event.

- **Message stream interface**

The message stream interface allows external applications to interact with the internal message flow of HP Operations Agent. The external application can be a read-write application, for example, a message processing program that can read HP Operations messages, modify attributes, and generate new messages for retransmission to the server. The application could also read messages, or send its own messages.

When you enable the message stream interface, you can also allow external applications using the interface to set up automatic or operator-initiated commands.

Select **Agent message stream interface** to allow messages to be directed to the **message stream interface** on the node. When switched on, you can choose between the following options:

- Divert a message to the message stream interface instead of to the server when a message is requested by an external application.

- Send the message to the server, and a copy of the message to the message stream interface.
- Add policy variables

You can use policy variables in event attributes. BSM Integration Adapter replaces the variables with the appropriate values in the generated event.

It is often useful to surround the variable with quotation marks, especially if it may return a value that contains spaces.

<\$#>

Returns the number of variables in an enterprise-specific SNMP event (generic event 6 Enterprise specific ID). Sample output: 2

<\$\*>

Returns all variables assigned to the event up to the possible fifteen. Sample output:  
[1] .1.1 (OctetString): arg1 [2] .1.2 (OctetString):  
turnip.example.com

<\$@>

Returns the time the event was received as the number of seconds since Jan 1, 1970 using the *time\_t* representation. Sample output: 859479898

<\$1>

Returns one or more of the fifteen possible event parameters that are part of an SNMP event. (<\$1> returns the first variable, <\$2> returns the second variable, and so on.)

<\$\>1>

Returns all attributes greater than *n* as *value* strings, useful for printing a variable number of arguments. <\$\>0> is equivalent to \$\* without sequence numbers, names, or types. Sample output: bokchoy.example.com

<\$\>+1>

Returns all attributes greater than *n* as *name:value* string. Sample output: .1.2 :  
asparagus.example.com

<\$+2>

Returns the *n*th variable binding as *name:value* . Sample output: .1.2 :  
artichoke.example.com

<\$\>-n >

Returns all attributes greater than *n* as [*seq*] *name (type): value* strings. Sample output:  
[2] .1.2 (OctetString): cauliflower.example.com

<\$-2>

Returns the *n*th variable binding as [*seq*] *name-type:value* . Sample output: [2] .1.2  
(OctetString): brusselsprouts.example.com

<\$A>

Returns the node that produced the event. Sample output: eggplant.example.com

<\$C>

Returns the community of the event. Sample output: public

<\$E>

Returns the enterprise ID of the event. Sample output: .1.3.6.1.4.1.11.2.17.1

<\$e>

Returns the enterprise object ID. Sample output: .1.3.6.1.4.1.11.2.17.1

<\$F>

Returns the textual name of the remote postmaster daemon's computer if the event was forwarded. Sample output: cress.example.com

<\$G>

Returns the generic event ID. Sample output: 6

<\$MSG\_GEN\_NODE>

Returns the IP address of the node that sends the message. Sample output:  
192.168.1.123.

<\$MSG\_GEN\_NODE\_NAME>

Returns the host name of the node that sends the message. Sample output:  
node123.example.com.

<\$MSG\_NODE>

Returns the IP address of the node on which the original event took place. Sample output: 192.168.1.123

<\$MSG\_NODE\_NAME>

Returns the name of the node on which the original event took place. This is the hostname that the agent resolves for the node. This variable is not fixed, however, and can be changed by a policy on a per-message basis. For example, if the policy is intercepting SNMP traps that originate from other devices, you might want to set this variable to the name of the device where the trap originated. If the policy is monitoring a log file on a network share where applications on several nodes write messages, you could extract the name of the node from the error message, save it in a user-defined variable, and assign it to MSG\_NODE\_NAME.

<\$MSG\_OBJECT>

Returns the name of the object associated with the event. This is set in the Message Defaults section of the policy editor.

<\$MSG\_TEXT>

Returns the full text of the event. In general, there are default texts for all editors derived from incoming event properties. Sample output: SU 03/19 16:13 + tt7p7 bill-root

<\$N>

Returns the event name (textual alias) of the event format specification used to format the event, as defined in the Event Configurator. Sample output: OV\_Node\_Down

<\$O>

Returns the name (object identifier) of the event. Sample output:  
.1.3.6.1.4.1.11.2.17.1.0.58916865

<\$o>

Returns the numeric object identifier of the event. Sample output:  
.1.3.6.1.4.1.11.2.17.1.0.58916865

<\$OPC\_GUI\_CLIENT>

Returns the hostname of the client where the HP Operations GUI is currently running. This variable is valid in the Node box for an operator-initiated command.

<\$OPC\_GUI\_CLIENT\_WEB>

Returns the hostname and default web browser of the client where the HP Operations GUI is currently running. This can be used with an operator-initiated command to load a web page in the default browser on the HP Operations GUI client. This variable is valid in the node field for an operator-initiated command .

<\$R>

Returns the true source of the event. This value is inferred through the transport mechanism which delivered the event. Sample output: `carrot.example.com`

<\$r>

Returns the implied source of the event. This may not be the true source of the event if the true source is proxying for another source, such as when a monitoring application running locally is reporting information about a remote node. Sample output: `rutabaga.example.com`

<\$S>

Returns the specific event ID. Sample output: `5891686`

<\$s>

Returns the event's severity. Sample output: `Normal`

<\$T>

Returns the event time stamp. Sample output: `0`

<\$V>


Returns the event type, based on the transport from which the event was received. Currently supported types are SNMPv1, SNMPv2, CMIP, GENERIC, and SNMPv2INFORM. Sample output: `SNMPv1`


<\$X>


Returns the time the event was received using the local time representation. Sample output: `17:24:58`

<\$x>

Returns the date the event was received using the local date representation. Sample output: `03/27/10`

3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure SNMP rules

Rules define what a monitor policy should do in response to a specific type of event. Each rule consists of a condition and of settings for the event generated by the policy. The condition is the part of a policy that describes the type of event in the source. The settings enable you to configure the event that BSM Integration Adapter sends to the Operations Management Event Browser.

An SNMP interceptor policy must contain at least one rule. If the policy contains multiple rules, it is important to remember that the rules are evaluated in a specific order, and that when one condition is matched, no additional rules will be evaluated.

The rule types are:

- **Event on matched condition**  
If matched, BSM Integration Adapter sends an event to the Operations Management Event Browser. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used.
- **Suppress on matched condition**  
If matched, BSM Integration Adapter stops processing and does not send an event to the Operations Management Event Browser.
- **Suppress on unmatched condition**  
If not matched, BSM Integration Adapter stops processing and does not send an event to the Operations Management Event Browser.

**Note:** In all cases, if a rule evaluates as true, no more rules are processed. It is important to pay attention to the [rule order](#).

The order in which rules are evaluated has a large effect on the type of messages you receive. It also affects the speed with which messages are sent and the amount of processor time that is required by the policy.

For example, you might have a policy that monitors CPU activity, containing these two rules:



1. If usage is greater than 80%,  
send a warning message and stop processing rules.
2. If usage is greater than 95%,  
send a critical message and stop processing rules.


If the rules were evaluated in the order shown, disk usage of 99% would only produce a warning message. If the order were reversed, however, a critical message would be sent. You could solve the problem by making the rules more specific, so that the order was not important:

1. If usage is between 80% and 94%,  
send a warning message and stop processing rules.
2. If usage is greater than 95%,  
send a critical message and stop processing rules.

In the example above, disk usage of 99% produces a critical message regardless of which rule is evaluated first. However, if the rules are evaluated in the order shown, disk usage of 99% is evaluated by two rules. If the order were reversed, it would be evaluated only by the first rule, thereby sending the message more quickly and reducing processing time on the managed node.

## To configure rules in SNMP interceptor policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **SNMP**. The SNMP interceptor policy editor opens.  
  
Alternatively, double-click an existing SNMP interceptor policy to edit it.
2. Click **Rules**.

3. Click  in the toolbar and select the rule type. Then type a description for the rule. After a rule has been added, you can change the rule type by clicking the current rule type in the list of rules and selecting another rule type from the drop-down list.

Alternatively, select an existing rule and click  to copy the rule. You can then rewrite the description of the copied rule and edit the rule.

4. Configure the following settings for the rule:

- Configure the condition

With this tab, you set the match conditions for an SNMP interceptor rule.

- **Node:** If you only want to match SNMP events from a specific node, type the FQDN (Fully Qualified Domain Name), the primary node name, or the IP address. Give multiple entries with the **OR** operator (for example, `celery.veg.com|broccoli.veg.com`), or leave blank for all nodes.

- **Event Information**

If you want to match a specific event, select **Event Object ID**. If you want to match a range of events or specify a specific event in **SNMPv1 Notation**, select the **SNMPv1 Notation** option.

- **Event Object ID**

Type the complete Event Object Identifier for the SNMP event that you want to match.

For example: `.1.3.6.1.4.1.11.2.17.1.0.40000001`

- **SNMPv1 notation**

You can type the complete event object ID in SNMPv1 format or you can specify only part of the identifier. For example, by specifying only the Enterprise ID, you can match all events with a specific Enterprise ID.

- **Enterprise ID**

Type in the enterprise ID for incoming SNMP traps to be compared with this condition. The enterprise ID is a vendor-specific identifier for the trap. Standard BSM Integration Adapter pattern-matching syntax may not be used in this field; however, it is possible to match a range of objects by entering only a prefix. For instance, the pattern:

`.1.3.6.1.4.1.11.2.17`

would match:

`.1.3.6.1.4.1.11.2.17.1`

`.1.3.6.1.4.1.11.2.17.2`

and so on.

- **Generic ID**

From the list, select the appropriate Generic Trap ID. Possible values are:

- (0) **ColdStart**
- (1) **WarmStart**
- (2) **LinkDown**
- (3) **LinkUp**
- (4) **Authentication**
- (5) **EgpNeighborLoss**
- (6) **EnterpriseSpecific**
- (7) **don't care**

If you select **(6) EnterpriseSpecific**, you can type in the specific trap ID. Select **don't care** to intercept any kind of trap.

- **Specific ID**

Type in the specific trap ID if you have selected **(6)EnterpriseSpecific** in Generic Trap. Enterprise-specific SNMP traps can be implemented by vendors on their specific network devices. The specific trap ID is used to identify the source of the trap.

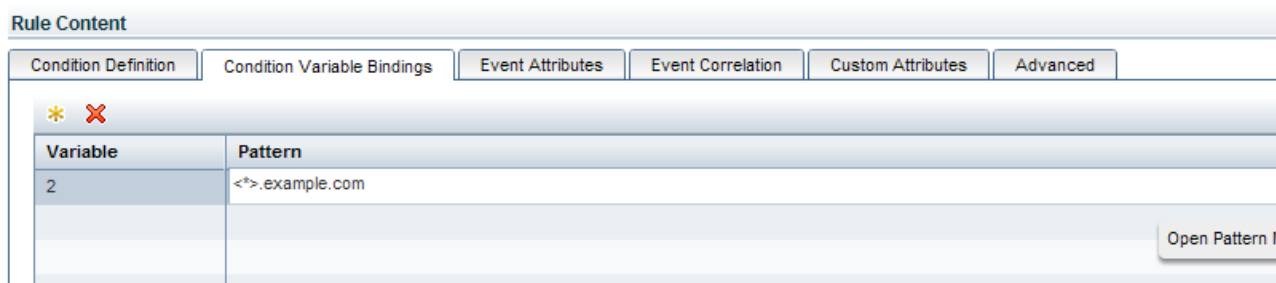
**NOTE:**

The SNMP syntax used by the editor requires that the trap string begins with a point.


- **Configure the condition variable bindings**

Select the variable bindings you want the policy to monitor, and write one or more match patterns for each binding. You can use pattern-matching rules when matching variable bindings. 1 represents the first variable binding in the event, 2 the second variable, and so on.


For example, \$2 contains in many SNMP events the hostname of the sender of the SNMP event. To only match events from systems in the domain example.com, use the pattern `<*>.example.com`:




To configure conditions for variable bindings:

- i. Click  and type the variable. You do not need to prefix the variable with a dollar sign (\$); BSM Integration Adapter does this automatically.

- ii. Type the match pattern in the Pattern field.

**Tip:** Click the  button to open the pattern matching expression toolbox.

- iii. *Optional.* To specify case sensitivity and field separators for the rule, click the  button. If you do not specify case sensitivity and separators for the rule, either the defaults (case sensitive; a blank and the tab character as separators) or the default options set for the policy will be used.

- **Configure event attributes**

The event attributes tab enables you to set the event attributes for a specific event. Except for the source event ID attribute, all attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events.

The source event ID attribute identifies the event in the source manager that provides the source event, for example Microsoft System Center Operations Manager (SCOM). BSM Integration Adapter must be able to identify the event to synchronize changes to the event with other servers, including the source management server, and to enable drilldown to a specific event in the source manager.

- **Title:** Brief description of the nature of the event.
- **Description:** Detailed description of the event.
- **Severity:** Severity assigned to the event. Accept the severity that is set in the event defaults or choose a specific event severity: Critical, Major, Minor, Warning, Normal.
- **Time Created:** Date and time when the event was created.

If you leave the attribute empty, then the date and time when the agent created the event displays in the Operations Management Event Browser. This time always displays using the time zone of the agent at creation time (for example, 11:30 (CET/winter). This means that this time always displays in this fixed time zone.

- **Category:** Name of the logical group to which the event belongs (for example, Database, Security, or Network). The event category is similar in concept to the HP Operations Manager message group.
- **Subcategory:** Name of the logical subgroup (category) to which the event belongs (for example, Oracle (database), Accounts (security), or Routers (network))
- **ETI:** Contains the event type indicator (ETI) resolution hint, which BSM uses to associate the event with an ETI. Use the format `<ETI name>:<ETI value>`. Specify a namespace that matches the name of the indicator (for example, CPUload). Specify an instance that matches an indicator state (for example, High). When an event with an ETI resolution hint of CPUload:High is received, and ETI and values exist, the event attribute ETI is set. BSM uses ETIs to calculate the status reported by the event and the current value.
- **Node:** Contains the node hint, which BSM uses to find a node in the RTSM (Run-time Service Model). This is the host system where the event occurred.
- **Related CI:** Contains the related CI hint, which BSM uses to identify the CI related to



the event (for example, oraclesid01@@node.example.com or C:@@server.example.com). Use the format `<hint 1>:<hint 2>:...:<hint n>@@<hostname>`.

#### Best practices for related CI hints

The related CI hint should have sufficient hints to find the corresponding CI.

It is necessary to differentiate between CIs that have a composition relationship to a host, and those that do not have such a relation:

- For “hosted on” CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>@@<hostname>
```

Typically, a “hosted on” CI is a sub-type of “software element”. For example, a CI of type `websphereas` has a container-link relation to the host.

Another example is the exchange server role CI type `exchangeclientaccessserver`. The root-container for this CI type is a software element, and for that CI type the root-container is host.

- For virtual CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>
```

A virtual CI does not have a strong containment relation (container-link or root-container) to a host.

An example of a typical virtual CI type is cluster. This CI type does not have a strong containment relation to a host.

**Tip:** If you have problems resolving non-hosted CIs, provide the RTSM ID of the desired CI as a hint using the format `UCMDB:<ci_uuid>`.

- **Source Manager:** Contains the source CI hint. In the context of BSM Integration Adapter, type the name and instance of the event and performance monitoring solution that provides events to BSM Integration Adapter (for example, `NNMi:mgmt1.example.com` or `SCOM:mgmt2.example.com`).
- **Source Event ID:** ID of the event in the source manager. This ID is required for synchronization of event changes with the source event. It also enables drilldown into the source manager in the Operations Management Event Browser.
- **Send with closed status** Sets the event's lifecycle status to Closed before sending it to the Operations Management Event Browser.

For more information about CI resolution in BSM, see the *Using Operations Management* PDF or online help.

- Configure event correlation

Event correlation helps to prevent the Operations Management Event Browser from becoming cluttered by events that describe the same problem. When event correlation is enabled, you can set the type of duplicate event suppression and define the method used to

suppress duplicate events.

- **Event Key:** An identifier used to identify duplicates and for Close Events with Key.
- **Close Events with Key:** If events with the event key that you type here exist in the Operations Management Event Browser when this event is received, these events are automatically closed. You can use pattern matching and variables to match multiple event keys. For example, consider the following pattern:

```
<$MSG_SEV>:<$MSG_NODE_NAME>:<5*>
```

This pattern is evaluated by first replacing the variables with the values that they resolve to, for example:

```
critical:cabbage.example.com:<5*>
```

This pattern is then compared using pattern matching rule against the event keys for all events in the Operations Management Event Browser. The pattern above would match the following event keys:

```
critical:cabbage.example.com:12345
```

```
critical:cabbage.example.com:TEST1
```

- **Deduplication on Server:** Clear to disable deduplication on the server. Stops automatic discarding of new events that are duplicates of existing events.

#### Suppress events which are:

- **Generated by the same rule:** Select this option to suppress events that match the pattern specified for the selected rule. This is a more general setting for the suppression of duplicate events. For example, an XML log file entry policy might contain a rule with this match pattern: `Error Message<#>` The log file lines `Error Message10` and `Error Message20` are not identical, but would both match this rule.
- **Generated by the same input event:** Select this option to suppress events that were sent in response to two separate input events that are identical except for the date and time that the event was generated (for example, identical entries in an XML log file).
- **Identical relative to their attributes:** Select this option to suppress either events that have the same event key or (if no event key is present) events that have identical event attributes (except for the date and time that the event was generated).

#### Suppression Method

For event correlation, you can define one of three correlation methods:

- **Time interval:** This correlation method lets you define an interval during which duplicate events will be ignored. For more information, read this [detailed example](#).

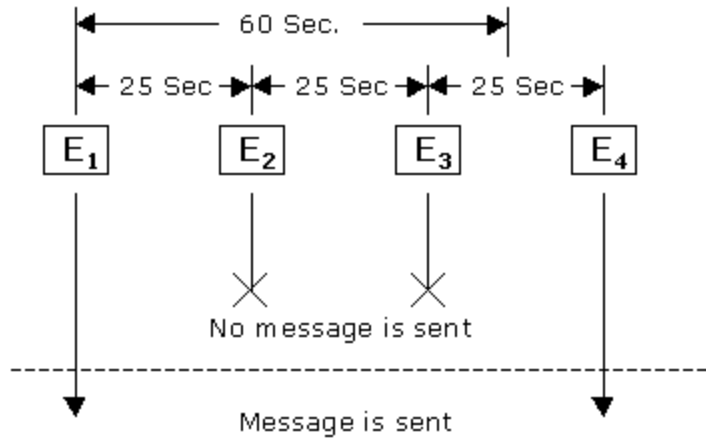
#### Time interval correlation example

In the illustration below, the interval is set to 30 seconds, but the suppression is limited to 60 seconds.

### Time interval

Suppress duplicate messages within a specified time interval.

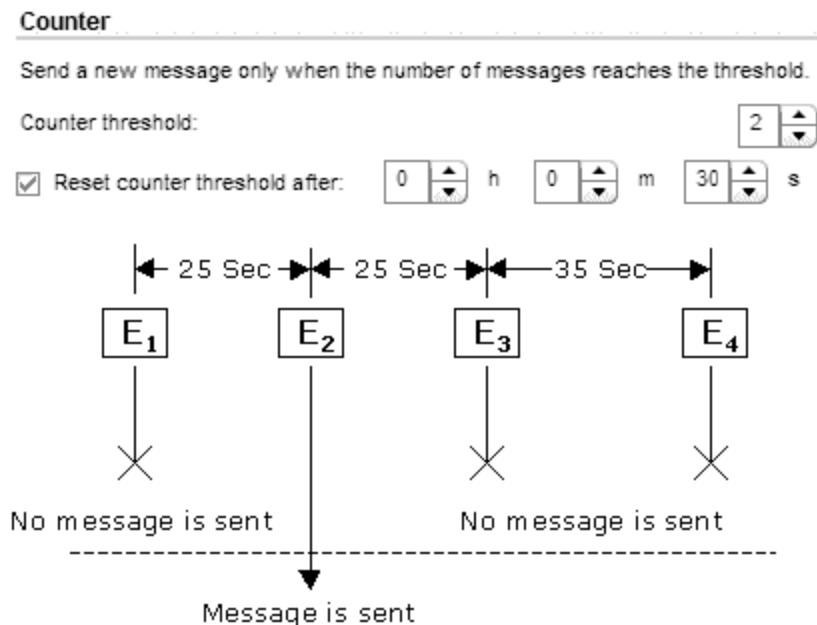
Time interval: 0 h 0 m 30 s  
 Suppress for no longer than 0 h 0 m 59 s



The **E<sub>x</sub>** represents events that are identical.

- The first input event (E1) matches a rule in the policy. The policy sends an event and starts timing.
- A second matching event (E2) occurs 25 seconds later. This event occurred *less than 30* seconds after the first event, and is therefore suppressed.
- A third matching event (E3) occurs *less than 30 seconds after the second event*, and so is also suppressed.
- The next matching event (E4) occurs less than thirty seconds after the third event, but is also *more than 60 seconds after the first event*, and therefore the policy sends an event.
- **Counter:** This correlation method counts the number of matching input events and sends an event only after the number of matching input events equals the counter threshold. The counter can also be reset to zero after a time period that you specify. For more information, read this [detailed example](#).

### Counter correlation example



The  $E_x$  represent events that are identical.

- The first input event (E1) matches a rule in the policy, and the counter increments to one. No event is sent.
- A second matching event (E2) occurs, the counter increments to two, an event is sent, and the counter resets.
- A third matching event (E3), and the counter increments to one no event is sent.
- The next matching event (E4) occurs *more than thirty seconds* after the third event. Since at thirty seconds the counter was reset to zero, the counter now increments to one no event is sent.
- **Time interval/Counter** If you use the Time interval and Counter together, events are evaluated first by the timer. If an event passes the timer, it is then evaluated by the counter, which either suppresses it or sends an event to the Operations Management Event Browser.

**Note:** If you specify just time interval correlation or just counter-based correlation in an individual event, any event defaults for the other correlation method also apply. For example, if you specify time interval correlation for an event, and the event defaults specify counter-based correlation, the combined time interval and counter-based correlation applies to both new rules and existing rules.


You can change this default behavior, so that only the correlation method that you specify in the individual event applies. To change the default behavior, set the parameter `OPC_IGNORE_DEFAULT_MSG_CORRELATION=TRUE` in the `eaagt` namespace on the node.

You can configure this parameter using `ovconfchg` or `ovconfpar` at a command prompt.

- Configure custom attributes

Custom attributes are additional attributes that contain any information that is meaningful to you. For example, you might add a company name, contact information, or a city location to an event. You can have more than one custom attribute attached to a single event. This attribute information displays in the Operations Management Event Browser in a column you have previously created to contain it.

To create a new custom attribute:

- i. Click  in the toolbar.
- ii. Type the name of the custom attribute. The name is case-insensitive.

The following custom attribute names are reserved for use by HP:

```
Description
EtiHint
NodeHint
NoDuplicateSuppression
RelatedCiHint
SourceCiHint
SourcedFromExternalId
SourcedFromExternalUrl
SubCategory
```

- iii. Type a value for the custom attribute.

- **Configure advanced attributes**

The advanced attributes tab enables you to configure event drilldown to the source manager that forwards the event, to specify additional HPOM-related attributes, and to configure the interface between messages and external programs on the HP Operations Agent.

- **Event drilldown**

Event drilldown information enables BSM users to launch the user interface of the source manager in the context of an event.

**Note:** The following event attribute can also be set by BSM based on connected server configuration. If a policy and a connected server configuration both set this attribute, the information in the policy takes precedence.

- **Event Drilldown URL:** URL of the event in the source manager. This is the complete path of the URL, and includes the FQDN (Fully Qualified Domain Name) of the computer that hosts the source manager, the communication port, and the root URL path (for example,  
`http://nnmi.example.com:8004/nnm/launch?cmd=showForm&objtype=Incident&objuuid=$OPC_CUSTOM[nnm.incident.uuid]&menus=true).`

**Tip:** To drill down to a specific event in the source manager, add the source event ID to the URL.

- **OM attributes**

HPOM-related attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events. Some attributes are used by CI resolution to relate the event to the impaired CI.

- **Application:** Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, Oracle and OS).
- **Object:** Device such as a computer, printer, or modem. Unlike the Related CI attribute, which is a direct relationship to a CI in the the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, C:, and /dev/spool).
- **Type:** String used to organize different types of events within an event category or subcategory (for example, users or applications, accounts and security).

BSM Integration Adapter sets this attribute automatically to `BSM_IA_Message`. You can delete the value but BSM Integration Adapter inserts it again when you save the policy.

- **HPOM Service ID:** ID of the service associated the event. A service ID is a unique identifier for a service and can be used in BSM to identify the node and CI associated with the event.

- **Message stream interface**

The message stream interface allows external applications to interact with the internal message flow of HP Operations Agent. The external application can be a read-write application, for example, a message processing program that can read HP Operations messages, modify attributes, and generate new messages for retransmission to the server. The application could also read messages, or send its own messages.

When you enable the message stream interface, you can also allow external applications using the interface to set up automatic or operator-initiated commands.

Select **Agent message stream interface** to allow messages to be directed to the **message stream interface** on the node. When switched on, you can choose between the following options:

- Divert a message to the message stream interface instead of to the server when a message is requested by an external application.
- Send the message to the server, and a copy of the message to the message stream interface.

- **Add policy variables**

You can use policy variables in event attributes. BSM Integration Adapter replaces the variables with the appropriate values in the generated event.

It is often useful to surround the variable with quotation marks, especially if it may return a value that contains spaces.

<\$#>

Returns the number of variables in an enterprise-specific SNMP event (generic event 6 Enterprise specific ID). Sample output: 2

<\$\*>

Returns all variables assigned to the event up to the possible fifteen. Sample output:  
[1] .1.1 (OctetString): arg1 [2] .1.2 (OctetString):  
turnip.example.com

<\$@>

Returns the time the event was received as the number of seconds since Jan 1, 1970 using the *time\_t* representation. Sample output: 859479898

<\$1>

Returns one or more of the fifteen possible event parameters that are part of an SNMP event. (<\$1> returns the first variable, <\$2> returns the second variable, and so on.)

<\$\>1>

Returns all attributes greater than *n* as *value* strings, useful for printing a variable number of arguments. <\$\>0> is equivalent to \$\* without sequence numbers, names, or types. Sample output: bokchoy.example.com

<\$\>+1>

Returns all attributes greater than *n* as *name:value* string. Sample output: .1.2:  
asparagus.example.com

<\$+2>

Returns the *n*th variable binding as *name:value*. Sample output: .1.2:  
artichoke.example.com

<\$\>-n >

Returns all attributes greater than *n* as [*seq*] *name (type): value* strings. Sample output:  
[2] .1.2 (OctetString): cauliflower.example.com

<\$-2>

Returns the *n*th variable binding as [*seq*] *name-type:value*. Sample output: [2] .1.2  
(OctetString): brusselsprouts.example.com

<\$A>

Returns the node that produced the event. Sample output: eggplant.example.com

<\$C>

Returns the community of the event. Sample output: public

<\$E>

Returns the enterprise ID of the event. Sample output: .1.3.6.1.4.1.11.2.17.1

<\$e>

Returns the enterprise object ID. Sample output: .1.3.6.1.4.1.11.2.17.1

<\$F>

Returns the textual name of the remote postmaster daemon's computer if the event was forwarded. Sample output: cress.example.com

<\$G>

Returns the generic event ID. Sample output: 6

<\$MSG\_GEN\_NODE>

Returns the IP address of the node that sends the message. Sample output:

192.168.1.123.

<\$MSG\_GEN\_NODE\_NAME>

Returns the host name of the node that sends the message. Sample output:

node123.example.com.

<\$MSG\_NODE>

Returns the IP address of the node on which the original event took place. Sample output: 192.168.1.123

<\$MSG\_NODE\_NAME>

Returns the name of the node on which the original event took place. This is the hostname that the agent resolves for the node. This variable is not fixed, however, and can be changed by a policy on a per-message basis. For example, if the policy is intercepting SNMP traps that originate from other devices, you might want to set this variable to the name of the device where the trap originated. If the policy is monitoring a log file on a network share where applications on several nodes write messages, you could extract the name of the node from the error message, save it in a user-defined variable, and assign it to MSG\_NODE\_NAME.

<\$MSG\_OBJECT>

Returns the name of the object associated with the event. This is set in the Message Defaults section of the policy editor.

<\$MSG\_TEXT>

Returns the full text of the event. In general, there are default texts for all editors derived from incoming event properties. Sample output: SU 03/19 16:13 + tty7 bill-root

<\$N>

Returns the event name (textual alias) of the event format specification used to format the event, as defined in the Event Configurator. Sample output: OV\_Node\_Down

<\$O>

Returns the name (object identifier) of the event. Sample output:

.1.3.6.1.4.1.11.2.17.1.0.58916865

<\$o>

Returns the numeric object identifier of the event. Sample output:

.1.3.6.1.4.1.11.2.17.1.0.58916865

<\$OPC\_GUI\_CLIENT>

Returns the hostname of the client where the HP Operations GUI is currently running. This variable is valid in the Node box for an operator-initiated command.

<\$OPC\_GUI\_CLIENT\_WEB>

Returns the hostname and default web browser of the client where the HP Operations GUI is currently running. This can be used with an operator-initiated command to load a web page in the default browser on the HP Operations GUI client. This variable is valid in the node field for an operator-initiated command .

<\$R>



Returns the true source of the event. This value is inferred through the transport mechanism which delivered the event. Sample output: `carrot.example.com`

<\$r>

Returns the implied source of the event. This may not be the true source of the event if the true source is proxying for another source, such as when a monitoring application running locally is reporting information about a remote node. Sample output:

`rutabaga.example.com`

<\$S>

Returns the specific event ID. Sample output: `5891686`

<\$s>

Returns the event's severity. Sample output: `Normal`

<\$T>

Returns the event time stamp. Sample output: `0`

<\$V>

Returns the event type, based on the transport from which the event was received. Currently supported types are SNMPv1, SNMPv2, CMIP, GENERIC, and SNMPv2INFORM. Sample output: `SNMPv1`


<\$X>


Returns the time the event was received using the local time representation. Sample output: `17:24:58`

<\$x>

Returns the date the event was received using the local date representation. Sample output: `03/27/10`

5. Click  in the toolbar to save the policy and close the editor.



**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

6. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure SNMP interceptor policy options

The options tab enables you to configure several policy behaviors.

### To configure options in SNMP interceptor policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **SNMP**. The SNMP interceptor policy editor opens.

Alternatively, double-click an existing SNMP interceptor policy to edit it.

2. Click **Options**. Options include:

- Log local events

BSM Integration Adapter allows you to define which events, if any, are logged on the node

from which they originated. These events are logged on the local node in the log file: `<data_dir>\log\OpC\opcmsglg`.

Three logging options are available.

- Log local events **that match a rule and trigger a message**. This selection logs any events in the event source that match the policy rules.
- Log local events **that match a rule and are ignored**. This selection logs any events in the event source that are suppressed (that is, they do not cause an event to be sent to the Operations Management Event Browser).
- Log local events **that don't match any rule**. This selection logs any events that do not match any of the rules in the policy.

#### ■ Capture unmatched events

You can configure a policy to send an event to the Operations Management Event Browser when an event does not match any rule in the policy because none of the conditions apply or because the policy does not contain any rules. This ensures that unexpected events that might be important do not go unreported. By default, unmatched events are ignored.

Each policy that sends unmatched events to the Operations Management Event Browser creates an event with the default values of the policy.

**Tip:** If you want a policy to send events only with the default values, omit all rules from the policy.

The following options are available:

- Unmatched events **are sent to the messages browser**
- Unmatched events **are sent to the acknowledged messages browser**
- Unmatched events **are ignored** (default)

Nodes create an event about an unmatched event only if the input event is unmatched in all SNMP interceptor policies on the node. Nodes send only one event for each unmatched input event.

#### ■ Pattern matching options

The following pattern matching options are available:

- **Case sensitivity**

You can choose whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the event. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the event and the pattern. This is the default setting.

- **Field separators**


You can indicate which characters should be considered to be field separators. Field separators are used in the pattern as separator characters for the rule condition. You can define up to seven separators, including these special characters:

- \n new line (NL)
- \t horizontal tab (HT)
- \v vertical tab (VT)
- \b backspace (BS)
- \r carriage return (CR)
- \f form feed (FF)
- \a alert (BEL)
- \\ backslash (\)


For example, if you wanted a backslash, an asterisk, and the letter A to define the fields in the event, you would type `\\*A` (with no spaces separating the characters).


If you leave this box empty, the default separators (a blank and the tab character) are used by default.

If you change the pattern matching options, they apply to all new rules in a policy. Click **Apply to all** to apply them to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.

You can set case sensitivity and separator characters for individual rules in a policy by clicking the  button in the **Condition Variable Bindings** tab of a rule.

3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Developing XML interceptor policies

XML interceptor policies monitor values in XML log files and respond when the value that you choose appears in the log file. XML log file policies are especially suited for integrating events from other applications.

XML interceptor policies process XML files and send events to the Operations Management Event Browser when certain conditions apply. You can define the attributes of the BSM event based on information in the XML file. This enables you to process events generated by other applications and to convert them to BSM events.

XML interceptor policies process exactly the XML elements and attributes that you define. The XML syntax is not important to the policy, as long as the event information is embedded in XML elements and attributes.

XML log files must meet the following criteria so that they can be processed correctly by XML interceptor policies:

- The root element is optional.
- If a root element exists, it must not be closed by an end tag.
- All other XML elements must be complete.

The following example XML begins with the root tag `<AllAlerts>` and contains two types of events: performance alerts and availability alerts. If you define the XML elements `<PerformanceAlert>` and `<AvailabilityAlert>` as event tags in the Source tab of XML interceptor policies, only those events are processed by XML interceptor policies.






```
<AllAlerts>
  <AvailabilityAlert>
    <Title>Host Unreachable</Title>
    <Severity>Critical</Severity>
    <TimeOccured>02/11/10 03:52:18AM</TimeOccured>
    <MonitoringObject>Host:fish.example.com</MonitoringObject>
  </AvailabilityAlert>
  <PerformanceAlert>
    <Title>Disk IO rate high</Title>
    <Severity>Warning</Severity>
    <TimeOccured>02/11/10 04:08:31AM</TimeOccured>
    <MonitoringObject>Disk:disk0:dog.example.com</MonitoringObject>
  </PerformanceAlert>
  <AvailabilityAlert>
    <Title>Web Application unresponsive</Title>
    <Severity>Critical</Severity>
    <TimeOccured>02/11/10 05:01:26AM</TimeOccured>
    <MonitoringObject>WebApp:http://employeeportal.intra.example.com</MonitoringObject>
  </AvailabilityAlert>
  <PerformanceAlert>
    <Title>Phyiscal Read Rate high for Bufferpool BP1</Title>
    <Severity>Warning</Severity>
    <TimeOccured>02/11/10 08:37:09AM</TimeOccured>
    <MonitoringObject>DB:USRDB:cat.example.com</MonitoringObject>
```

```
</PerformanceAlert>
<PerformanceAlert>
  <Title>Phyiscal Read Rate high for Bufferpool BP1</Title>
  <Severity>Warning</Severity>
  <TimeOccured>02/11/10 08:37:09AM</TimeOccured>
  <MonitoringObject>DB:USRDB:cat.example.com</MonitoringObject>
</PerformanceAlert>
```

**Tip:** If the application does not store its events in XML files, you may write a program or script that extracts the events from wherever they are stored, formats the data using XML syntax, and generates an XML file with the events. If you have control over the XML elements that are used in the XML file, choose XML elements and attributes that map to event attributes and values. This will simplify the policy.

**Note:** XML interceptor policies read each line of an XML log file individually. Therefore, you cannot match patterns that span multiple lines in the log file.



## To configure an XML log file policy

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.  
  
Alternatively, double-click an existing XML log file policy to edit it.
2. Complete the information in the following tabs:
  - **Properties** include information that is related to the policy itself (for example, the name and description of the policy).
  - The policy **source** is the XML log file that the policy monitors (for example, the path and name of the XML log file).
  - The policy **defaults** include:
    - Default mappings of XML elements and attributes to custom variables
    - Default settings for all events generated by the policy (for example, default event attributes)
  - **Rules** define what the policy should do in response to a specific type of event.
  - **Options** configure several policy behaviors (for example, pattern matching options).
3. Click  in the toolbar to save the policy and close the editor.  
**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.
4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure XML log file policy properties

Every policy has a set of properties that identify and describe the policy.


## To configure properties of XML log file policies



1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.

Alternatively, double-click an existing XML log file policy to edit it.

2. Click **Properties**.
3. *Required*. In the **Name** box, type a name that will identify the policy. You can use spaces in policy names. The equal sign (=) is not allowed.
4. *Optional*. In the **Description** box, type a description of what the policy does. You might also add other notes, for example data sources that are used.
5. *Optional*. In the **Category** box, type one or more arbitrary categories. Policy categories may help you to better group your policies. Separate multiple categories with commas.
6. **Policy ID**: BSM Integration Adapter automatically assigns a GUID (globally unique identifier) to the policy when it is first created.
7. **Last modification**: The date and time that the policy was saved.

The date and time displays using the current time zone of the computer on which the BSM Integration Adapter user interface runs. The language setting of the web browser determines the date and time format (for example, 09/14/2010 8:16:38 AM for English (United States)). If the web browser and the computer on which the BSM Integration Adapter server run have different language settings, the language setting of the web browser takes precedence. However, English is the default language if the web browser is configured to use a language that is not available on the server.



8. **Last modified by**: The name of the user active when the policy was saved.
9. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.
10. *Optional*. If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure XML log file source properties

The source tab of the XML log file policy editor enables you to specify which log file the policy reads. You can also set options that configure how the policy reads the log file.

## To configure the XML log file source

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.

Alternatively, double-click an existing XML log file policy to edit it.

2. Click **Source**. Configure the XML log file and other options:

- Select the log file to monitor

*Required.* Specify the log file that the policy reads. Type the drive letter and the full path for the location of this log file on the BSM Integration Adapter system. You can use Windows environmental variables (for example **winnt** or **clusterlog**) to make your policies more flexible. The proper syntax for these variables is `<$variablename>`.

You can also call a script or command that returns the path and name of the log file you want to monitor. For example, type

```
<`command`>
```

where `command` is the name of a script that returns the path and name of the log file you want to monitor. The command can also return more than one log file path separated by spaces. The HP Operations Agent monitors each of the files using the same options and conditions as configured for this policy. This is very useful when you want to dynamically determine the log file path or monitor multiple instances of a log file.

- Set the log file polling interval

You can indicate how often the policy should read the log file. This period of time is the polling interval. The polling interval should be as large as possible, although this depends on the amount of new data written to the file and the read mode that you choose. Set the interval to no less than 30 seconds; usually 5 minutes is appropriate. Note, however, that a policy begins to evaluate data *after* the first polling interval passes. A shorter polling interval is better when you are testing a policy.

- Select the log file character set

Indicate the name of the character set used by the log file that you are monitoring. It is important to choose the correct character set. If the character set that the policy is expecting does not match the character set in the log file, pattern matching may not work, and the event details can have incorrect characters or be truncated in the Operations Management Event Browser. If you are unsure of which character set is used by the log file that you want to monitor, consult the documentation of the program that writes the log file.

**Note:** The character set of the log file must be convertible to the HP Operations Agent character set. For example, if agent character set is iso88591 (English) then, ACP 1252, ACSII, ISO 8859-1, OEMCP 850, OEMCP 437, ROMAN 8, or EBCDIC may be used. If the agent character set is sjis (Japanese), then ACP 932, ACSII, or EUC may be used. If the agent character set is iso88595 (Cyrillic), then iso88595, ASCII, ACP 1251, or OEMCP 866 may be used.

The character sets supported by Windows and Linux nodes are:

Character set	Description
ACP 1250	Central European
ACP 1251	Cyrillic
ACP 1252	Western European

## Using HP BSM Integration Adapter

### Developing XML interceptor policies

---

ACP 932	Includes all characters defined in the shift-JIS code. This character set is supported by the Japanese versions of Microsoft Windows NT and Microsoft Windows 95/98.
ACSII	English (American Standard Code for Information Interchange)
BIG-5 Taiwanese	Taiwanese
EBCDIC	(Extended Binary-Coded Decimal Interchange Code) Generally used only on large IBM computers.
EUC Japanese	(Extended UNIX Code) Japanese
EUC Korean	(Extended UNIX Code) Korean
EUC Taiwanese	(Extended UNIX Code) Taiwanese
GB-2312- 80 Chinese	Chinese
ISO 8859- 1	Most West European languages, including French, Spanish, Catalan, Basque, Portuguese, Italian, Albanian, Rhaeto-Romanic, Dutch, German, Danish, Swedish, Norwegian, Finnish, Faeroese, Icelandic, Irish, Scottish, and English. Also Afrikaans, Swahili.
ISO 8859- 15	Latin alphabet
ISO 8859- 2	Central and Eastern European languages, including Czech, Hungarian, Polish, Romanian, Croatian, Slovak, Slovenian, Sorbian.
ISO 8859- 5	Languages that use Cyrillic characters, including Bulgarian, Belorussian, Macedonian, Russian, Serbian and Ukrainian.
ISO 8859- 6	Arabic
ISO 8859- 7	Greek
ISO 8859- 8	Hebrew and Yiddish
ISO 8859- 9	Same as ISO 8859-1, but with Turkish, instead of Icelandic.



## Using HP BSM Integration Adapter

### Developing XML interceptor policies

---

OEMCP 437	U.S. English
OEMCP 737	Greek (formerly 437G)
OEMCP 775	Baltic
OEMCP 850	All the characters used by most European, North American, and South American languages
OEMCP 852	Slavic (Latin II)
OEMCP 857	IBM Turkish
OEMCP 860	Portuguese
OEMCP 861	Icelandic
OEMCP 862	Hebrew
OEMCP 863	Canadian-French
OEMCP 864	Arabic
OEMCP 865	Nordic
OEMCP 866	Russian
OEMCP 869	IBM Modern Greek
ROMAN 8	European characters
SHIFT-JIS	Microsoft's standard encoding for Japanese.
UCS-2	This codeset is intended to express all characters in the world in a united character set.
UTF-8	(Unicode Transformation Format-8) This codeset is intended to express all characters in the world in a united character set.

- Send event if log file does not exist

*Optional.* Select if you want BSM Integration Adapter to send an event if the specified XML file does not exist

- Close after reading

*Optional.* Clear if you want the policy to keep the XML file open (and retain its file handle) after reading it. Do not use a polling interval of less than one minute when this option is selected.

If you do not select this option and the name of the XML file changes, the policy continues to read the open, renamed XML file instead of processing the new XML file. Consider the following example: a policy monitors the log file `syslog.log`. Mondays at 23:59, the file is renamed to `syslog.monday`, and a new version of `syslog.log` is created for the Tuesday log. Without Close after reading being selected, the policy continues to monitor `syslog.monday` because the file handle refers to the original, renamed file.

- Set the read mode

*Required.* The read mode of an XML log file policy indicates whether the policy should process the entire log file or should only process new log file entries. The available read modes are described in the table below.

Note that every policy reads the same log files independently from any other policies. This means, for example, that if "Policy 1" with read mode **Read from beginning (first time)** is activated on a node where "Policy 2" with the same read mode already exists, "Policy 1" will still read the entire log file after it has been enabled.

#### Log file read modes

Mode: Description	Advantage / Disadvantage
<p><b>Read from last position:</b> The policy reads only new—appended—entries written in the log file while the policy is activated on the node. If the log file decreases in size between readings, then the entire log file is read. Log file entries that are added to the log file when the policy is deactivated are not processed by the policy.</p> <p>Choose this option if you are concerned only with log file entries that occur when the policy is enabled.</p>	<p><b>Advantage:</b> No chance of reading the same entry twice. (Unless the log file decreases in size because some entries were deleted.)</p> <p><b>Disadvantage:</b> Entries written to the log file while the policy is deactivated or the agent is not running will not be processed by the policy.</p>
<p><b>Read from beginning (first time):</b> The policy reads the complete log file each time the policy is activated or the agent restarts on the node. This ensures that all entries in the log file are compared with the rules in the policy. Each successive time that the policy reads the log file, only new (appended) entries in the log file are processed.</p>	<p><b>Advantage:</b> Every existing and future entry in the log file will be processed by the policy.</p> <p><b>Disadvantage:</b> Duplicate entries can</p>

<p>Choose this option if you want to ensure that every existing and future entry in the log file will be processed by the policy while it is enabled.</p>	<p>occur if an activated policy is deactivated and reactivated, or if the agent stops and restarts.</p>
<p><b>Read from beginning (always):</b> The policy reads the complete log file every time it detects that the log file has changed. The policy scans the log file at the specified polling interval. If no change is detected, the log file is not processed. Any log file entries overwritten while the agent is not running or the policy is deactivated will not be evaluated by the policy.</p> <p>Choose this option if you are monitoring a log file that is overwritten, rather than appended.</p>	<p><b>Advantage:</b> Ensures that log files that are overwritten are correctly processed.</p> <p><b>Disadvantage:</b> Only valid for log files that are overwritten, rather than appended.</p>



- Load XML sample data

*Optional.* Load a sample of the XML log file that you want to monitor with this policy. BSM Integration Adapter makes the XML elements and values of the sample file available to you in the defaults and rules tabs so that you can insert them by dragging and dropping.

To load a sample XML file, click **Load** and then select the file. You can also display the selected XML file by clicking **View**. When you load sample data, BSM Integration Adapter replaces already loaded data with the new data. This does not affect any mappings that are defined based on previously available sample data.


- Specify the XML event tag


*Required.* The XML event tag creates a shortcut to the XML element that you want to monitor. An event tag typically identifies an event record in an XML log file. You can define more than one event tag. For example, an XML file may contain two types of events: `<PerformanceAlert>` and `<AvailabilityAlert>`. To monitor both types, define both elements as event tags.

To specify an XML event tag, click  and select **manually**, then type the XML element. Alternatively, if you are working with sample data, click  and select **from XML sample data**, then double-click the XML element in the list.

**Caution:** Deleting an event tag that is referenced in a policy corrupts the policy and renders it unusable.

3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure XML log file mapping defaults

The mapping defaults tab enables you to map XML elements and attributes to custom variables.

A custom variable consists of a map name, an optional XML property (XML elements or attributes), and one or more source and target value pairs. For example, you can assign the XML element `Severity` to the map name `mapSeverity`, and add a source value of `Warning`. You can then assign the target value `Major` to the variable so that BSM Integration Adapter inserts the value `Major` into the event in all places where the variable is used and the source value is `Warning` in the XML log file.

Map Name	XML Property	Source Value	Target Value
<code>mapSeverity</code>	<code>&lt;\${DATA:./PerformanceAlert/Severity}&gt;</code>	<code>Critical</code>	<code>Error</code>
<code>mapTitle</code>	<code>&lt;\${DATA:./PerformanceAlert/Title}&gt;</code>	<code>Warning</code>	<code>Major</code>

XML properties use the following syntax: `<${DATA:./<XML_property>}`

`<XML_property>` is the XML path, separated by slash marks (`/`), from the XML event tag to the XML element or attribute.

For example, the custom variable `mapSeverity` has the following XML property:

`<${DATA:./Performance_Alert/Severity}>` where `Severity` is a child element of `Performance_Alert`.


XML properties are optional. If you do not assign an XML property to a variable, you must add the source value directly to the variable when you insert the variable in an event attribute.

**Note:** The XML properties list is empty if no sample data has been loaded into the policy or if the sample data does not match any specified XML event tags.

The XML properties list shows the following information if sample data is available:



- XML Properties section

If sample data is available, then the XML Properties section shows all XML elements and attributes that match an XML event tag. (You can identify attributes based on the preceding at sign (`@`.)

The XML Properties section by default shows the short path to the XML property or value. To view the full path, click . The full path begins with the XML event tag specified in the Source tab.

You can sort the information that appears in the XML Properties section so that data appears in either ascending or descending order, indicated by either an up or down arrow at the top of the list. The items in the XML Properties section are by default sorted alphabetically in ascending order. To change the sort order, click the arrow at the top of the list.



To search for an XML property or value, type the search string in the Search Properties box. The list changes as you type; only matching items appear.

- The Values section displays the values of an XML property selected in the XML Properties section. If a value appears more than once, click  to show or hide duplicate values. To find values that belong to more than one XML property, select the value and click . The XML Sample Data window opens and shows all XML properties that have the selected value.


When you drag an XML element or attribute from the XML properties list and drop it on the Default Value Mapping List, BSM Integration Adapter automatically adds the default prefix `map` to the map name and inserts the correct path to the XML property. You can then drag one or more XML source


values from the XML values list and drop them on the Source Value list. You then finally only have to type the target values.


## To configure mapping defaults in XML log file policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.

Alternatively, double-click an existing XML log file policy to edit it.

2. Click **Defaults - Mappings**.
3. Create one or more custom variables by defining map names and XML properties, either manually or by dragging them from the XML properties list.
4. Add one or more source and target value pairs to each custom variable, either manually or by dragging them from the XML values list.
5. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

6. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

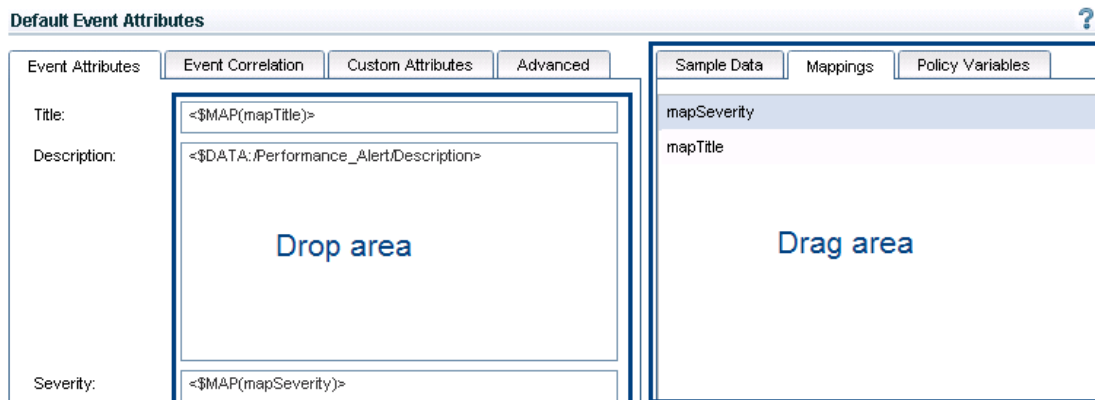
## Configure XML log file event defaults

The attribute defaults tab enables you to indicate default settings for all events generated by the policy.



These defaults affect all new and existing rules. You can override the defaults in individual rules if needed. If a rule contains empty event attributes, the agent will use the defaults for the new event.

**Tip:** The BSM Integration Adapter user interface enables you to drag data from the tabs on the right onto boxes on the left.

The following illustration shows the default event attributes page of XML interceptor policies. You can select data in the Sample Data, Mappings, and Policy Variables tabs on the right and drag it to the Event Attributes, Event Correlation, Custom Attributes, and Advanced tabs on the left. BSM Integration Adapter inserts the data at the current cursor position.



## To configure attribute defaults in XML log file policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.

Alternatively, double-click an existing XML log file policy to edit it.

2. Click **Defaults - Event**. The default settings include:

- **Configure event attributes**

The event attributes tab enables you to set the event attributes for the event defaults. Except for the source event ID attribute, all attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events.

The source event ID attribute identifies the event in the source manager that provides the source event, for example Microsoft System Center Operations Manager (SCOM). BSM Integration Adapter must be able to identify the event to synchronize changes to the event with other servers, including the source management server, and to enable drilldown to a specific event in the source manager.

- **Title:** Brief description of the nature of the event.
- **Description:** Detailed description of the event.
- **Severity:** Severity assigned to the event.
- **Time Created:** Date and time when the event was created.

Use the following conventions when specifying the date and time attribute:

- **Integers.** XML interceptor policies interpret integers in XML files as seconds since 00:00:00 UTC on 1 January 1970 (Unix time). For example, 1276600333 is 15 June 2010, at 11:12:13.
- **Default time formats.** XML interceptor policies by default interpret the following time formats:

yyyy-mm-ddTHH:MM:SS (for example, 2010-06-15T11:12:13)

mm/dd/yyyy HH:MM:SS (for example, 06/15/2010 11:12:13)

- **Pattern matching.** You can use the function `<$DATETIME (FORMAT, VALUE) >` to specify a pattern (`FORMAT`) that matches the time string in a given XML property (`VALUE`). You can use standard BSM Integration Adapter pattern-matching rules when matching values. By default, pattern matching for the time format is case sensitive. The default field separators are the space and the tab characters.

`FORMAT` must be enclosed in quotation marks ("`FORMAT`") and accepts the following variables:

`H` (hours), `M` (minutes), `S` (seconds). If `H`, `M`, or `S` is not set, the hour, minute, or second displays as zero.

*d* (day), *m* (month), *y* (year). If *d* or *m* is not set, the day or month display as one. If *y* is not set, the current year is assumed. If *y* is less than 100, the current millennium is assumed; for example, if *y* matches 10, the year displays as 2010. It is not possible to match a year earlier than 1970.

*p* (P.M.) If *p* is set, XML interceptor policies add 12 hours to the hours that precede the variable.

VALUE is the XML property or value to match.

XML properties use the following syntax: `<$DATA:/<XML_property>`

`<XML_property>` is the XML path, separated by slash marks (/), from the XML event tag to the XML element or attribute.

Examples:

To match the time format 06/15/2010 11:12:13 in the XML property

```
<$DATA:/SCOM_Alert/TimeRaised>, type  
<$DATETIME ("^<#.m>/<#.d>/<#.y>  
<#.H>:<#.M>:<#.S>$", <$DATA:/SCOM_Alert/TimeRaised>)>
```

To match the time format 11:12 15.06.2010 in the XML property

```
<$DATA:/SCOM_Alert/TimeRaised>, type  
<$DATETIME ("^<#.H>:<#.M> <#.d>.<#.m>.<#.y>$", <$DATA:/SCOM_  
Alert/TimeRaised>)>
```

To match the time format 06/15/2010 1:35 PM in the XML property

```
<$DATA:/SCOM_Alert/TimeRaised>, type  
<$DATETIME ("^<#.m>/<#.d>/<#.y> <#.H>:<#.M>  
<2*.p>$", <$DATA:/SCOM_Alert/TimeRaised>)>
```

If you leave the attribute empty or if none of the time formats above can be matched, then the date and time when the agent created the event displays in the Operations Management Event Browser. This time always displays using the time zone of the agent at creation time (for example, 11:30 (CET/winter). This means that this time always displays in this fixed time zone.

- **Category:** Name of the logical group to which the event belongs (for example, Database, Security, or Network). The event category is similar in concept to the HP Operations Manager message group.
- **Subcategory:** Name of the logical subgroup (category) to which the event belongs (for example, Oracle (database), Accounts (security), or Routers (network))
- **ETI:** Contains the event type indicator (ETI) resolution hint, which BSM uses to associate the event with an ETI. Use the format `<ETI name>:<ETI value>`. Specify a namespace that matches the name of the indicator (for example, CPUload). Specify an instance that matches an indicator state (for example, High). When an event with an ETI resolution hint of CPUload:High is received, and ETI and values exist, the event attribute ETI is set. BSM uses ETIs to calculate the status reported by the event and the current value.
- **Node:** Contains the node hint, which BSM uses to find a node in the RTSM (Run-time

Service Model). This is the host system where the event occurred.

- **Related CI:** Contains the related CI hint, which BSM uses to identify the CI related to the event (for example, oraclesid01@@node.example.com or C:@@server.example.com). Use the format `<hint 1>:<hint 2>:...:<hint n>@@<hostname>`.

Best practices for related CI hints

The related CI hint should have sufficient hints to find the corresponding CI.

It is necessary to differentiate between CIs that have a composition relationship to a host, and those that do not have such a relation:

- For “hosted on” CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>@@<hostname>
```

Typically, a “hosted on” CI is a sub-type of “software element”. For example, a CI of type `websphereas` has a container-link relation to the host.

Another example is the exchange server role CI type `exchangeclientaccessserver`. The root-container for this CI type is a software element, and for that CI type the root-container is host.

- For virtual CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>
```

A virtual CI does not have a strong containment relation (container-link or root-container) to a host.

An example of a typical virtual CI type is `cluster`. This CI type does not have a strong containment relation to a host.

**Tip:** If you have problems resolving non-hosted CIs, provide the RTSM ID of the desired CI as a hint using the format `UCMDB:<ci_uid>`.

- **Source Manager:** Contains the source CI hint. In the context of BSM Integration Adapter, type the name and instance of the event and performance monitoring solution that provides events to BSM Integration Adapter (for example, NNMI:mgmt1.example.com or SCOM:mgmt2.example.com).
- **Source Event ID:** ID of the event in the source manager. This ID is required for synchronization of event changes with the source event. It also enables drilldown into the source manager in the Operations Management Event Browser.

**Tip:** The monitored XML file usually contains the source event ID. If you are working with sample data, you can drag the source event ID from the Sample Data tab and add it to the source event ID field.

For more information about CI resolution in BSM, see the *Using Operations Management* PDF or online help.

- Configure event correlation



Event correlation helps to prevent the Operations Management Event Browser from becoming cluttered by events that describe the same problem. When event correlation is enabled, you can set the type of duplicate event suppression and define the method used to suppress duplicate events.

- **Event Key:** An identifier used to identify duplicates and for Close Events with Key.
- **Close Events with Key:** If events with the event key that you type here exist in the Operations Management Event Browser when this event is received, these events are automatically closed. You can use pattern matching and variables to match multiple event keys. For example, consider the following pattern:

```
<$MSG_SEV>:<$MSG_NODE_NAME>:<5*>
```

This pattern is evaluated by first replacing the variables with the values that they resolve to, for example:

```
critical:cabbage.example.com:<5*>
```

This pattern is then compared using pattern matching rule against the event keys for all events in the Operations Management Event Browser. The pattern above would match the following event keys:

```
critical:cabbage.example.com:12345  
critical:cabbage.example.com:TEST1
```

- **Deduplication on Server:** Clear to disable deduplication on the server. Stops automatic discarding of new events that are duplicates of existing events.

#### Suppress events which are:

- **Generated by the same rule:** Select this option to suppress events that match the pattern specified for the selected rule. This is a more general setting for the suppression of duplicate events. For example, an XML log file entry policy might contain a rule with this match pattern: `Error Message<#>` The log file lines `Error Message10` and `Error Message20` are not identical, but would both match this rule.
- **Generated by the same input event:** Select this option to suppress events that were sent in response to two separate input events that are identical except for the date and time that the event was generated (for example, identical entries in an XML log file).
- **Identical relative to their attributes:** Select this option to suppress either events that have the same event key or (if no event key is present) events that have identical event attributes (except for the date and time that the event was generated).

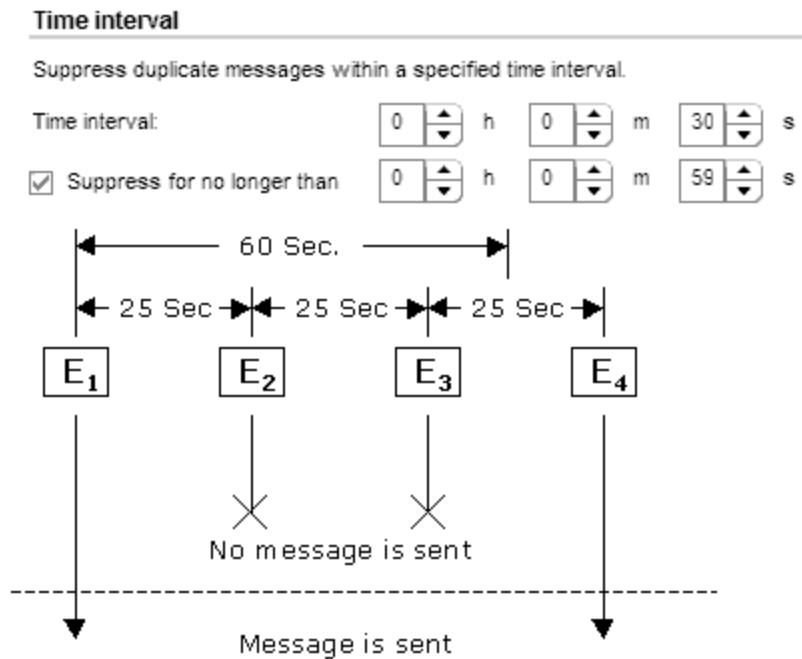
#### Suppression Method

For event correlation, you can define one of three correlation methods:

- **Time interval:** This correlation method lets you define an interval during which duplicate events will be ignored. For more information, read this [detailed example](#).

#### Time interval correlation example

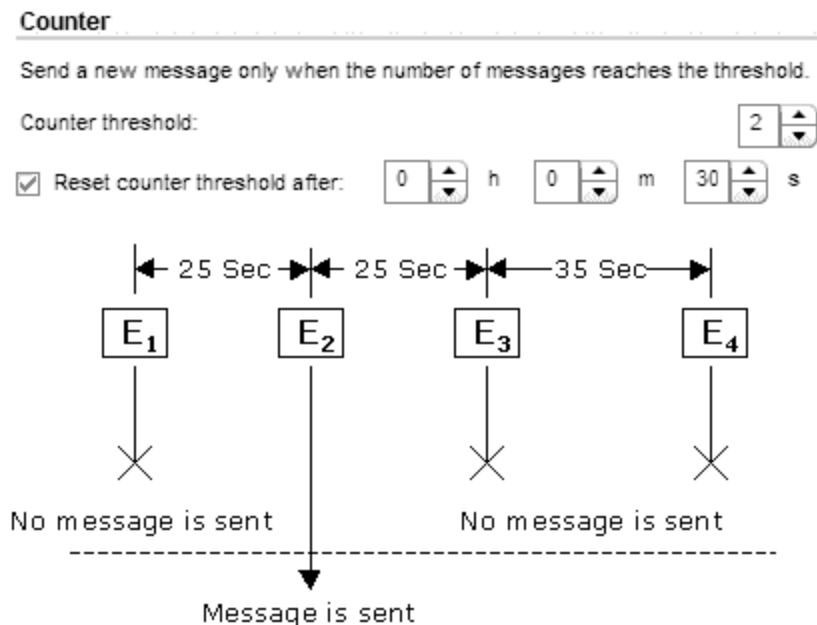
In the illustration below, the interval is set to 30 seconds, but the suppression is limited to 60 seconds.



The **E<sub>x</sub>** represents events that are identical.

- The first input event (E1) matches a rule in the policy. The policy sends an event and starts timing.
- A second matching event (E2) occurs 25 seconds later. This event occurred *less than 30 seconds* after the first event, and is therefore suppressed.
- A third matching event (E3) occurs *less than 30 seconds after the second event*, and so is also suppressed.
- The next matching event (E4) occurs less than thirty seconds after the third event, but is also *more than 60 seconds after the first event*, and therefore the policy sends an event.
- **Counter:** This correlation method counts the number of matching input events and sends an event only after the number of matching input events equals the counter threshold. The counter can also be reset to zero after a time period that you specify. For more information, read this [detailed example](#).

#### Counter correlation example



The  $E_x$  represent events that are identical.

- The first input event (E1) matches a rule in the policy, and the counter increments to one. No event is sent.
- A second matching event (E2) occurs, the counter increments to two, an event is sent, and the counter resets.
- A third matching event (E3), and the counter increments to one no event is sent.
- The next matching event (E4) occurs *more than thirty seconds* after the third event. Since at thirty seconds the counter was reset to zero, the counter now increments to one no event is sent.
- **Time interval/Counter** If you use the Time interval and Counter together, events are evaluated first by the timer. If an event passes the timer, it is then evaluated by the counter, which either suppresses it or sends an event to the Operations Management Event Browser.

**Note:** If you specify just time interval correlation or just counter-based correlation in an individual event, any event defaults for the other correlation method also apply. For example, if you specify time interval correlation for an event, and the event defaults specify counter-based correlation, the combined time interval and counter-based correlation applies to both new rules and existing rules.


You can change this default behavior, so that only the correlation method that you specify in the individual event applies. To change the default behavior, set the parameter `OPC_IGNORE_DEFAULT_MSG_CORRELATION=TRUE` in the `eaagt` namespace on the node.

You can configure this parameter using `ovconfchg` or `ovconfpar` at a command prompt.

- Configure custom attributes

Custom attributes are additional attributes that contain any information that is meaningful to you. For example, you might add a company name, contact information, or a city location to an event. You can have more than one custom attribute attached to a single event. This attribute information displays in the Operations Management Event Browser in a column you have previously created to contain it.

To create a new custom attribute:

- i. Click  in the toolbar.
- ii. Type the name of the custom attribute. The name is case-insensitive.

The following custom attribute names are reserved for use by HP:

```
Description
EtiHint
NodeHint
NoDuplicateSuppression
RelatedCiHint
SourceCiHint
SourcedFromExternalId
SourcedFromExternalUrl
SubCategory
```

- iii. Type a value for the custom attribute.

- **Configure advanced attributes**

The advanced attributes tab enables you to configure event drilldown to the source manager that forwards the event, to specify additional HPOM-related attributes, and to configure the interface between messages and external programs on the HP Operations Agent.

- **Event drilldown**

Event drilldown information enables BSM users to launch the user interface of the source manager in the context of an event.

**Note:** The following event attribute can also be set by BSM based on connected server configuration. If a policy and a connected server configuration both set this attribute, the information in the policy takes precedence.

- **Event Drilldown URL:** URL of the event in the source manager. This is the complete path of the URL, and includes the FQDN (Fully Qualified Domain Name) of the computer that hosts the source manager, the communication port, and the root URL path (for example,  
`http://nnmi.example.com:8004/nnm/launch?cmd=showForm&objtype=Incident&objuuid=$OPC_CUSTOM[nnm.incident.uuid]&menus=true`).

**Tip:** To drill down to a specific event in the source manager, add the source event ID to the URL. If you are working with sample data, you can drag the source event ID from the Sample Data tab and add it to the Event Drilldown URL field.

- **OM attributes**

HPOM-related attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events. Some attributes are used by CI resolution to relate the event to the impaired CI.

- **Application:** Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, Oracle and OS).
- **Object:** Device such as a computer, printer, or modem. Unlike the Related CI attribute, which is a direct relationship to a CI in the the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, C:, and /dev/spool).
- **Type:** String used to organize different types of events within an event category or subcategory (for example, users or applications, accounts and security).

BSM Integration Adapter sets this attribute automatically to `BSM_IA_Message`. You can delete the value but BSM Integration Adapter inserts it again when you save the policy.

- **HPOM Service ID:** ID of the service associated the event. A service ID is a unique identifier for a service and can be used in BSM to identify the node and CI associated with the event.

- **Message stream interface**

The message stream interface allows external applications to interact with the internal message flow of HP Operations Agent. The external application can be a read-write application, for example, a message processing program that can read HP Operations messages, modify attributes, and generate new messages for retransmission to the server. The application could also read messages, or send its own messages.

When you enable the message stream interface, you can also allow external applications using the interface to set up automatic or operator-initiated commands.

Select **Agent message stream interface** to allow messages to be directed to the **message stream interface** on the node. When switched on, you can choose between the following options:

- Divert a message to the message stream interface instead of to the server when a message is requested by an external application.
- Send the message to the server, and a copy of the message to the message stream interface.

- **Add XML sample data**

If you are working with sample data, you can drag XML properties (XML elements and attributes) and values from the Sample Data tab and drop them onto the attribute boxes.

Alternatively, you can type the path to the XML property or value directly into the attribute box.

XML properties use the following syntax: `<$DATA:/<XML_property>`

`<XML_property>` is the XML path, separated by slash marks (/), from the XML event tag to the XML element or attribute.


BSM Integration Adapter replaces the XML property at runtime with the value of the specified XML element or attribute. If you insert an XML value, the value will be used.

**Note:** The Sample Data tab is empty if no sample data has been loaded into the policy or if the sample data does not match any specified XML event tags.

The Sample Data tab shows the following information if sample data is available:



- XML Properties section

If sample data is available, then the XML Properties section of the Sample Data tab shows all XML elements and attributes that match an XML event tag. (You can identify attributes based on the preceding at sign (@).)

The XML Properties section by default shows the short path to the XML property or value. To view the full path, click . The full path begins with the XML event tag specified in the Source tab.

You can sort the information that appears in the XML Properties section so that data appears in either ascending or descending order, indicated by either an up or down arrow at the top of the list. The items in the XML Properties section are by default sorted alphabetically in ascending order. To change the sort order, click the arrow at the top of the list.

To search for an XML property or value, type the search string in the Search Properties box. The list changes as you type; only matching items appear.

- The Values section displays the values of an XML property selected in the XML Properties section. If a value appears more than once, click  to show or hide duplicate values. To find values that belong to more than one XML property, select the value and click . The XML Sample Data window opens and shows all XML properties that have the selected value.

- Add mappings

Mappings are custom variables that you define in the mappings tab. To insert a custom variable, you can drag it from the Mappings list and drop it on the event attribute.

Alternatively, type the custom variable into the attribute box using the following syntax:

`<$MAP(<custom_variable>)>` where `<custom_variable>` is the map name of the variable (for example, `<$MAP (map@Severity) >`).

If the custom variable does not have an XML property assigned, use the following syntax:

`<$MAP(<custom_variable>,<<source_value>>)>` where `<source_value>` can be one of the following:

- XML path to the source value, for example `<$MAP(map@Severity, <$DATA/Performance_Alert/Severity>)>`
- The source value itself, for example `<$MAP(map@Severity, Warning)>`
- Add policy variables

You can use policy variables in event attributes. BSM Integration Adapter replaces the variables with the appropriate values in the generated event.

It is often useful to surround the variable with quotation marks, especially if it may return a value that contains spaces.

`<$LOGFILE>`

Returns the name of the log file that contains the input event. Sample output: `program_log.txt`

`<$LOGPATH>`

Returns the name and path of the log file that contains the input event. Sample output: `C:\temp\mylogfile\program_log.txt`

`<$MSG_NODE>`


Returns the IP address of the node on which the original event took place. Sample output: `192.168.1.123`


`<$MSG_NODE_NAME>`


Returns the name of the node on which the original event took place. This is the hostname that the agent resolves for the node. This variable is not fixed, however, and can be changed by a policy on a per-message basis. For example, if the policy is intercepting SNMP traps that originate from other devices, you might want to set this variable to the name of the device where the trap originated. If the policy is monitoring a log file on a network share where applications on several nodes write messages, you could extract the name of the node from the error message, save it in a user-defined variable, and assign it to `MSG_NODE_NAME`.

`<$MSG_TEXT>`

Returns the full text of the event. In general, there are default texts for all editors derived from incoming event properties. Sample output: `SU 03/19 16:13 + ttyp7 bill-root`

3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure XML log file rules

Rules define what a monitor policy should do in response to a specific type of event. Each rule consists of a condition and of settings for the event generated by the policy. The condition is the part of a policy that describes the type of event in the source. The settings enable you to configure the event that BSM Integration Adapter sends to the Operations Management Event Browser.

An XML interceptor policy must contain at least one rule. If the policy contains multiple rules, it is important to remember that the rules are evaluated in a specific order, and that when one condition is matched, no additional rules will be evaluated.

The rule types are:

- **Event on matched condition**  
If matched, BSM Integration Adapter sends an event to the Operations Management Event Browser. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used.
- **Suppress on matched condition**  
If matched, BSM Integration Adapter stops processing and does not send an event to the Operations Management Event Browser.
- **Suppress on unmatched condition**  
If not matched, BSM Integration Adapter stops processing and does not send an event to the Operations Management Event Browser.

**Note:** In all cases, if a rule evaluates as true, no more rules are processed. It is important to pay attention to the [rule order](#).

The order in which rules are evaluated has a large effect on the type of messages you receive. It also affects the speed with which messages are sent and the amount of processor time that is required by the policy.

For example, you might have a policy that monitors CPU activity, containing these two rules:

1. If usage is greater than 80%,  
send a warning message and stop processing rules.
2. If usage is greater than 95%,  
send a critical message and stop processing rules.

If the rules were evaluated in the order shown, disk usage of 99% would only produce a warning message. If the order were reversed, however, a critical message would be sent. You could solve the problem by making the rules more specific, so that the order was not important:

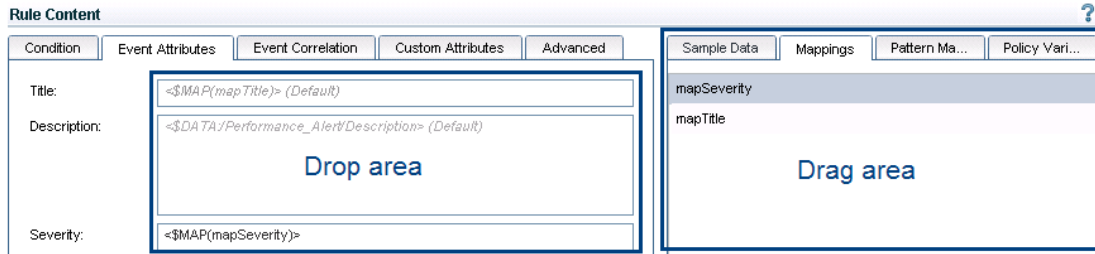
1. If usage is between 80% and 94%,  
send a warning message and stop processing rules.
2. If usage is greater than 95%,  
send a critical message and stop processing rules.

In the example above, disk usage of 99% produces a critical message regardless of which rule is evaluated first. However, if the rules are evaluated in the order shown, disk usage of 99% is evaluated by two rules. If the order were reversed, it would be evaluated only by the first rule, thereby sending the message more quickly and reducing processing time on the managed node.





**Tip:** The BSM Integration Adapter user interface enables you to drag data from the tabs on the right onto boxes on the left.

The following illustration shows a section of the rules page of XML interceptor policies. You can select data in the Sample Data, Mappings, Pattern Matching Variables, and Policy Variables tabs on the right and drag it to the Condition, Event Attributes, Event Correlation, Custom Attributes, and Advanced tabs on the left. BSM Integration Adapter inserts the data at the current cursor position.






### To configure rules in XML log file policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.  
Alternatively, double-click an existing XML log file policy to edit it.
2. Click **Rules**.
3. Click  in the toolbar and select the rule type. Then type a description for the rule. After a rule has been added, you can change the rule type by clicking the current rule type in the list of rules and selecting another rule type from the drop-down list.  
Alternatively, select an existing rule and click  to copy the rule. You can then rewrite the description of the copied rule and edit the rule.
4. Configure the following settings for the rule:
  - Configure conditions

The condition tab enables you to specify the XML properties and values that the policy searches for in the XML log file that the policy monitors. If the policy finds a match, it may or may not generate an event, depending on the rule type.

- i. Specify the XML element or attribute that the policy searches for.

If you are working with sample data, you can drag and drop the XML element or attribute from the XML Properties list to the Properties field. Alternatively, click  and type the XML property into the box. You must specify the XML path from the XML event tag to the property, separated by slash marks (/).


- ii. Select the operator. BSM Integration Adapter provides the following operators:

Operator	Description
==	Equal to
!=	Not equal to
<	Less than
<=	Less than or equal to
>	More than

Operator	Description
>=	More than or equal to
~=	Pattern operator

- iii. In the Operand field, type the value or pattern that you want the policy to compare with the XML log file line. If you are working with sample data, you can drag the value from the XML Values list and drop it on the operand box.

You can use standard BSM Integration Adapter pattern-matching rules when matching

values. Select the ~= pattern operator and click  to open the pattern matching expression toolbox. The toolbox also enables you to specify pattern matching options such as case sensitivity and field separators for the rule. If you do not specify pattern matching options for the rule, either the defaults (case sensitive; a blank and the tab character as separators) or the default options set for the policy will be used.

- **Configure event attributes**

The event attributes tab enables you to set the event attributes for a specific event. Except for the source event ID attribute, all attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events.

The source event ID attribute identifies the event in the source manager that provides the source event, for example Microsoft System Center Operations Manager (SCOM). BSM Integration Adapter must be able to identify the event to synchronize changes to the event with other servers, including the source management server, and to enable drilldown to a specific event in the source manager.

- **Title:** Brief description of the nature of the event.
- **Description:** Detailed description of the event.
- **Severity:** Severity assigned to the event.
- **Time Created:** Date and time when the event was created.

Use the following conventions when specifying the date and time attribute:

- **Integers.** XML interceptor policies interpret integers in XML files as seconds since 00:00:00 UTC on 1 January 1970 (Unix time). For example, 1276600333 is 15 June 2010, at 11:12:13.
- **Default time formats.** XML interceptor policies by default interpret the following time formats:
  - yyyy-mm-ddTHH:MM:SS (for example, 2010-06-15T11:12:13)
  - mm/dd/yyyy HH:MM:SS (for example, 06/15/2010 11:12:13)
- **Pattern matching.** You can use the function `<$DATETIME (FORMAT, VALUE) >` to specify a pattern (FORMAT) that matches the time string in a given XML property (VALUE). You can use standard BSM Integration Adapter pattern-matching rules

when matching values. By default, pattern matching for the time format is case sensitive. The default field separators are the space and the tab characters.

`FORMAT` must be enclosed in quotation marks ("`FORMAT`") and accepts the following variables:

`H` (hours), `M` (minutes), `S` (seconds). If `H`, `M`, or `S` is not set, the hour, minute, or second displays as zero.

`d` (day), `m` (month), `y` (year). If `d` or `m` is not set, the day or month display as one. If `y` is not set, the current year is assumed. If `y` is less than 100, the current millennium is assumed; for example, if `y` matches 10, the year displays as 2010. It is not possible to match a year earlier than 1970.

`p` (P.M.) If `p` is set, XML interceptor policies add 12 hours to the hours that precede the variable.

`VALUE` is the XML property or value to match.

XML properties use the following syntax: `<$DATA:/<XML_property>`

`<XML_property>` is the XML path, separated by slash marks (/), from the XML event tag to the XML element or attribute.

Examples:

To match the time format 06/15/2010 11:12:13 in the XML property

```
<$DATA:/SCOM_Alert/TimeRaised>, type  
<$DATETIME ("^<#.m>/<#.d>/<#.y>  
<#.H>:<#.M>:<#.S>$", <$DATA:/SCOM_Alert/TimeRaised>)>
```

To match the time format 11:12 15.06.2010 in the XML property

```
<$DATA:/SCOM_Alert/TimeRaised>, type  
<$DATETIME ("^<#.H>:<#.M> <#.d>.<#.m>.<#.y>$", <$DATA:/SCOM_  
Alert/TimeRaised>)>
```

To match the time format 06/15/2010 1:35 PM in the XML property

```
<$DATA:/SCOM_Alert/TimeRaised>, type  
<$DATETIME ("^<#.m>/<#.d>/<#.y> <#.H>:<#.M>  
<2*.p>$", <$DATA:/SCOM_Alert/TimeRaised>)>
```

If you leave the attribute empty or if none of the time formats above can be matched, then the date and time when the agent created the event displays in the Operations Management Event Browser. This time always displays using the time zone of the agent at creation time (for example, 11:30 (CET/winter). This means that this time always displays in this fixed time zone.

- **Category:** Name of the logical group to which the event belongs (for example, Database, Security, or Network). The event category is similar in concept to the HP Operations Manager message group.
- **Subcategory:** Name of the logical subgroup (category) to which the event belongs (for example, Oracle (database), Accounts (security), or Routers (network))
- **ETI:** Contains the event type indicator (ETI) resolution hint, which BSM uses to

associate the event with an ETI. Use the format `<ETI name>:<ETI value>`. Specify a namespace that matches the name of the indicator (for example, CPUload). Specify an instance that matches an indicator state (for example, High). When an event with an ETI resolution hint of CPUload:High is received, and ETI and values exist, the event attribute ETI is set. BSM uses ETIs to calculate the status reported by the event and the current value.

- **Node:** Contains the node hint, which BSM uses to find a node in the RTSM (Run-time Service Model). This is the host system where the event occurred.
- **Related CI:** Contains the related CI hint, which BSM uses to identify the CI related to the event (for example, oraclesid01@@node.example.com or C:@@server.example.com). Use the format `<hint 1>:<hint 2>:...:<hint n>@@<hostname>`.

Best practices for related CI hints

The related CI hint should have sufficient hints to find the corresponding CI.

It is necessary to differentiate between CIs that have a composition relationship to a host, and those that do not have such a relation:

- For “hosted on” CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>@@<hostname>
```

Typically, a “hosted on” CI is a sub-type of “software element”. For example, a CI of type `websphereas` has a container-link relation to the host.

Another example is the exchange server role CI type `exchangeclientaccessserver`. The root-container for this CI type is a software element, and for that CI type the root-container is host.

- For virtual CIs

```
<CI type name>:<key attribute 1>:<key attribute 2>:<key attribute n>
```

A virtual CI does not have a strong containment relation (container-link or root-container) to a host.

An example of a typical virtual CI type is `cluster`. This CI type does not have a strong containment relation to a host.

**Tip:** If you have problems resolving non-hosted CIs, provide the RTSM ID of the desired CI as a hint using the format `UCMDB:<ci_uid>`.

- **Source Manager:** Contains the source CI hint. In the context of BSM Integration Adapter, type the name and instance of the event and performance monitoring solution that provides events to BSM Integration Adapter (for example, NNMi:mgmt1.example.com or SCOM:mgmt2.example.com).
- **Source Event ID:** ID of the event in the source manager. This ID is required for synchronization of event changes with the source event. It also enables drilldown into

the source manager in the Operations Management Event Browser.

**Tip:** The monitored XML file usually contains the source event ID. If you are working with sample data, you can drag the source event ID from the Sample Data tab and add it to the source event ID field.

- **Send with closed status** Sets the event's lifecycle status to Closed before sending it to the Operations Management Event Browser.

For more information about CI resolution in BSM, see the *Using Operations Management* PDF or online help.

#### ■ Configure event correlation

Event correlation helps to prevent the Operations Management Event Browser from becoming cluttered by events that describe the same problem. When event correlation is enabled, you can set the type of duplicate event suppression and define the method used to suppress duplicate events.

- **Event Key:** An identifier used to identify duplicates and for Close Events with Key.
- **Close Events with Key:** If events with the event key that you type here exist in the Operations Management Event Browser when this event is received, these events are automatically closed. You can use pattern matching and variables to match multiple event keys. For example, consider the following pattern:

```
<$MSG_SEV>:<$MSG_NODE_NAME>:<5*>
```

This pattern is evaluated by first replacing the variables with the values that they resolve to, for example:

```
critical:cabbage.example.com:<5*>
```

This pattern is then compared using pattern matching rule against the event keys for all events in the Operations Management Event Browser. The pattern above would match the following event keys:

```
critical:cabbage.example.com:12345  
critical:cabbage.example.com:TEST1
```

- **Deduplication on Server:** Clear to disable deduplication on the server. Stops automatic discarding of new events that are duplicates of existing events.

#### Suppress events which are:

- **Generated by the same rule:** Select this option to suppress events that match the pattern specified for the selected rule. This is a more general setting for the suppression of duplicate events. For example, an XML log file entry policy might contain a rule with this match pattern: `Error Message<#>` The log file lines `Error Message10` and `Error Message20` are not identical, but would both match this rule.
- **Generated by the same input event:** Select this option to suppress events that were sent in response to two separate input events that are identical except for the date and time that the event was generated (for example, identical entries in an XML log file).
- **Identical relative to their attributes:** Select this option to suppress either events that

have the same event key or (if no event key is present) events that have identical event attributes (except for the date and time that the event was generated).

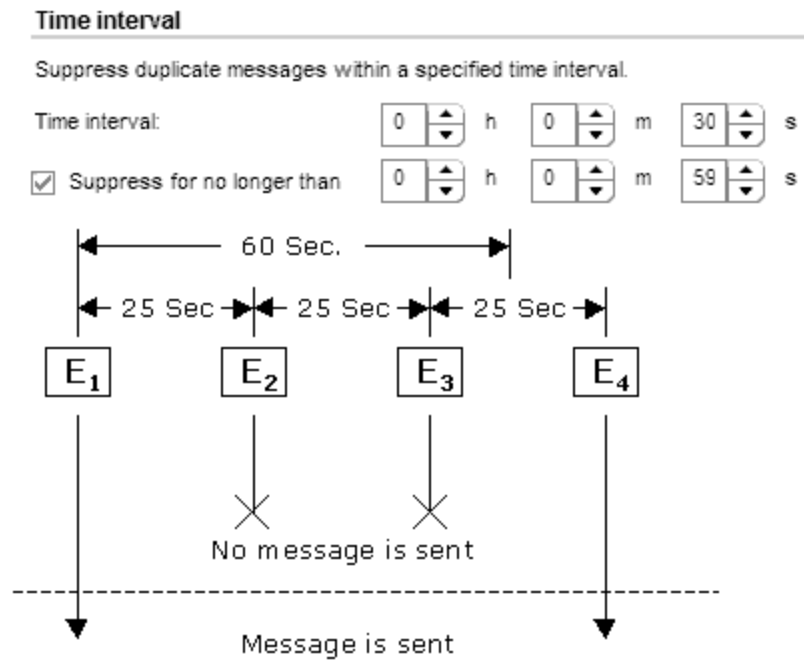
**Suppression Method**

For event correlation, you can define one of three correlation methods:

- **Time interval:** This correlation method lets you define an interval during which duplicate events will be ignored. For more information, read this [detailed example](#).

**Time interval correlation example**

In the illustration below, the interval is set to 30 seconds, but the suppression is limited to 60 seconds.

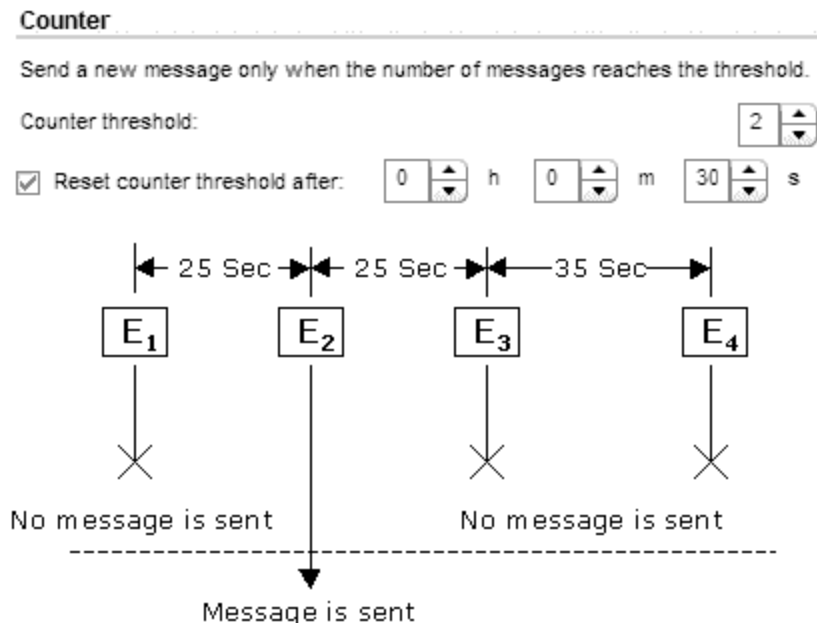


The **E<sub>x</sub>** represents events that are identical.

- The first input event (E1) matches a rule in the policy. The policy sends an event and starts timing.
- A second matching event (E2) occurs 25 seconds later. This event occurred *less than 30 seconds* after the first event, and is therefore suppressed.
- A third matching event (E3) occurs *less than 30 seconds after the second event*, and so is also suppressed.
- The next matching event (E4) occurs less than thirty seconds after the third event, but is also *more than 60 seconds after the first event*, and therefore the policy sends an event.
- **Counter:** This correlation method counts the number of matching input events and sends

an event only after the number of matching input events equals the counter threshold. The counter can also be reset to zero after a time period that you specify. For more information, read this [detailed example](#).

### Counter correlation example



The **E<sub>x</sub>** represent events that are identical.

- The first input event (E<sub>1</sub>) matches a rule in the policy, and the counter increments to one. No event is sent.
- A second matching event (E<sub>2</sub>) occurs, the counter increments to two, an event is sent, and the counter resets.
- A third matching event (E<sub>3</sub>), and the counter increments to one no event is sent.
- The next matching event (E<sub>4</sub>) occurs *more than thirty seconds* after the third event. Since at thirty seconds the counter was reset to zero, the counter now increments to one no event is sent.
- **Time interval/Counter** If you use the Time interval and Counter together, events are evaluated first by the timer. If an event passes the timer, it is then evaluated by the counter, which either suppresses it or sends an event to the Operations Management Event Browser.


**Note:** If you specify just time interval correlation or just counter-based correlation in an individual event, any event defaults for the other correlation method also apply. For example, if you specify time interval correlation for an event, and the event defaults specify counter-based correlation, the combined time interval and counter-based correlation applies to both new rules and existing rules.

You can change this default behavior, so that only the correlation method that you specify in the individual event applies. To change the default behavior, set the parameter `OPC_IGNORE_DEFAULT_MSG_CORRELATION=TRUE` in the `eaagt` namespace on the node. You can configure this parameter using `ovconfchg` or `ovconfpar` at a command prompt.

- **Configure custom attributes**

Custom attributes are additional attributes that contain any information that is meaningful to you. For example, you might add a company name, contact information, or a city location to an event. You can have more than one custom attribute attached to a single event. This attribute information displays in the Operations Management Event Browser in a column you have previously created to contain it.

To create a new custom attribute:

- Click  in the toolbar.
- Type the name of the custom attribute. The name is case-insensitive.

The following custom attribute names are reserved for use by HP:

```
Description
EtiHint
NodeHint
NoDuplicateSuppression
RelatedCiHint
SourceCiHint
SourcedFromExternalId
SourcedFromExternalUrl
SubCategory
```

- Type a value for the custom attribute.

- **Configure advanced attributes**

The advanced attributes tab enables you to configure event drilldown to the source manager that forwards the event, to specify additional HPOM-related attributes, and to configure the interface between messages and external programs on the HP Operations Agent.

- **Event drilldown**

Event drilldown information enables BSM users to launch the user interface of the source manager in the context of an event.

**Note:** The following event attribute can also be set by BSM based on connected server configuration. If a policy and a connected server configuration both set this attribute, the information in the policy takes precedence.



- **Event Drilldown URL:** URL of the event in the source manager. This is the complete path of the URL, and includes the FQDN (Fully Qualified Domain Name) of the computer that hosts the source manager, the communication port, and the root URL path (for example, `http://nnmi.example.com:8004/nnm/launch?cmd=showForm&objtype=Incident&objuuid=$OPC_CUSTOM[nnm.incident.uuid]&menus=true`).  
**Tip:** To drill down to a specific event in the source manager, add the source event ID to the URL. If you are working with sample data, you can drag the source event ID from the Sample Data tab and add it to the Event Drilldown URL field.
- **OM attributes**

HPOM-related attributes are visible in the Operations Management Event Browser and help the user to organize and evaluate the events. Some attributes are used by CI resolution to relate the event to the impaired CI.

  - **Application:** Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, Oracle and OS).
  - **Object:** Device such as a computer, printer, or modem. Unlike the Related CI attribute, which is a direct relationship to a CI in the the RTSM (Run-time Service Model), the application attribute is a simple string-type attribute (for example, C:, and /dev/spool).
  - **Type:** String used to organize different types of events within an event category or subcategory (for example, users or applications, accounts and security).  

BSM Integration Adapter sets this attribute automatically to `BSM_IA_Message`. You can delete the value but BSM Integration Adapter inserts it again when you save the policy.
  - **HPOM Service ID:** ID of the service associated the event. A service ID is a unique identifier for a service and can be used in BSM to identify the node and CI associated with the event.
- **Message stream interface**

The message stream interface allows external applications to interact with the internal message flow of HP Operations Agent. The external application can be a read-write application, for example, a message processing program that can read HP Operations messages, modify attributes, and generate new messages for retransmission to the server. The application could also read messages, or send its own messages.

When you enable the message stream interface, you can also allow external applications using the interface to set up automatic or operator-initiated commands.

Select **Agent message stream interface** to allow messages to be directed to the **message stream interface** on the node. When switched on, you can choose between the following options:

- Divert a message to the message stream interface instead of to the server when a message is requested by an external application.
- Send the message to the server, and a copy of the message to the message stream interface.

#### ■ Add XML sample data

If you are working with sample data, you can drag XML properties (XML elements and attributes) and values from the Sample Data tab and drop them onto the attribute boxes. Alternatively, you can type the path to the XML property or value directly into the attribute box.

XML properties use the following syntax: `<$DATA:/<XML_property>`

`<XML_property>` is the XML path, separated by slash marks (/), from the XML event tag to the XML element or attribute.


BSM Integration Adapter replaces the XML property at runtime with the value of the specified XML element or attribute. If you insert an XML value, the value will be used.

**Note:** The Sample Data tab is empty if no sample data has been loaded into the policy or if the sample data does not match any specified XML event tags.

The Sample Data tab shows the following information if sample data is available:



#### ○ XML Properties section

If sample data is available, then the XML Properties section of the Sample Data tab shows all XML elements and attributes that match an XML event tag. (You can identify attributes based on the preceding at sign (@).)

The XML Properties section by default shows the short path to the XML property or value. To view the full path, click . The full path begins with the XML event tag specified in the Source tab.

You can sort the information that appears in the XML Properties section so that data appears in either ascending or descending order, indicated by either an up or down arrow at the top of the list. The items in the XML Properties section are by default sorted alphabetically in ascending order. To change the sort order, click the arrow at the top of the list.

To search for an XML property or value, type the search string in the Search Properties box. The list changes as you type; only matching items appear.

- The Values section displays the values of an XML property selected in the XML Properties section. If a value appears more than once, click  to show or hide duplicate values. To find values that belong to more than one XML property, select the value and click . The XML Sample Data window opens and shows all XML properties that have the selected value.

#### ■ Add pattern matching variables

Pattern matching variables insert matched strings that have previously been assigned to variables. To insert a pattern matching variable, type the variable name enclosed in angle

brackets (for example, `<variablename>`) or drag and drop it from the Pattern Matching Variables list to the event attribute.

- Add mappings

Mappings are custom variables that you define in the mappings tab. To insert a custom variable, you can drag it from the Mappings list and drop it on the event attribute.

Alternatively, type the custom variable into the attribute box using the following syntax:

`<$MAP(<custom_variable>)>` where `<custom_variable>` is the map name of the variable (for example, `<$MAP(map@Severity)>`).

If the custom variable does not have an XML property assigned, use the following syntax:

`<$MAP(<custom_variable>,<<source_value>>)>` where `<source_value>` can be one of the following:

- XML path to the source value, for example `<$MAP(map@Severity, <$DATA/Performance_Alert/Severity>)>`
- The source value itself, for example `<$MAP(map@Severity, Warning)>`

- Add policy variables

You can use policy variables in event attributes. BSM Integration Adapter replaces the variables with the appropriate values in the generated event.

It is often useful to surround the variable with quotation marks, especially if it may return a value that contains spaces.

`<$LOGFILE>`

Returns the name of the log file that contains the input event. Sample output: `program_log.txt`

`<$LOGPATH>`

Returns the name and path of the log file that contains the input event. Sample output: `C:\temp\mylogfile\program_log.txt`

`<$MSG_NODE>`

Returns the IP address of the node on which the original event took place. Sample output: `192.168.1.123`


`<$MSG_NODE_NAME>`


Returns the name of the node on which the original event took place. This is the hostname that the agent resolves for the node. This variable is not fixed, however, and can be changed by a policy on a per-message basis. For example, if the policy is intercepting SNMP traps that originate from other devices, you might want to set this variable to the name of the device where the trap originated. If the policy is monitoring a log file on a network share where applications on several nodes write messages, you could extract the name of the node from the error message, save it in a user-defined variable, and assign it to `MSG_NODE_NAME`.

`<$MSG_TEXT>`

Returns the full text of the event. In general, there are default texts for all editors derived from incoming event properties. Sample output: `SU 03/19 16:13 + tty7 bill-root`

5. Click  in the toolbar to save the policy and close the editor.



**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

6. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Configure XML log file policy options

The options tab enables you to configure several policy behaviors.

### To configure options in XML log file policies

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click  **XML**. The XML interceptor policy editor opens.

Alternatively, double-click an existing XML log file policy to edit it.

2. Click **Options**. Options include:

- Log local events

BSM Integration Adapter allows you to define which events, if any, are logged on the node from which they originated. These events are logged on the local node in the log file:

```
<data_dir>\log\OpC\opcmsglg.
```

Three logging options are available.

- Log local events **that match a rule and trigger a message**. This selection logs any events in the event source that match the policy rules.
- Log local events **that match a rule and are ignored**. This selection logs any events in the event source that are suppressed (that is, they do not cause an event to be sent to the Operations Management Event Browser).
- Log local events **that don't match any rule**. This selection logs any events that do not match any of the rules in the policy.

- Capture unmatched events

You can configure a policy to send an event to the Operations Management Event Browser when an event does not match any rule in the policy because none of the conditions apply or because the policy does not contain any rules. This ensures that unexpected events that might be important do not go unreported. By default, unmatched events are ignored.

Each policy that sends unmatched events to the Operations Management Event Browser creates an event with the default values of the policy.

**Tip:** If you want a policy to send events only with the default values, omit all rules from the policy.

The following options are available:

- Unmatched events **are sent to the messages browser**
- Unmatched events **are sent to the acknowledged messages browser**
- Unmatched events **are ignored** (default)

If several policies forward unmatched events to the Operations Management Event Browser you could receive multiple events about a single input event.

- **Pattern matching options**

The following pattern matching options are available:

- **Case sensitivity**

You can choose whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the event. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the event and the pattern. This is the default setting.

- **Field separators**


You can indicate which characters should be considered to be field separators. Field separators are used in the pattern as separator characters for the rule condition. You can define up to seven separators, including these special characters:

- \n new line (NL)
- \r carriage return (CR)
- \t horizontal tab (HT)
- \f form feed (FF)
- \v vertical tab (VT)
- \a alert (BEL)
- \b backspace (BS)
- \\ backslash (\)


For example, if you wanted a backslash, an asterisk, and the letter A to define the fields in the event, you would type \\\*A (with no spaces separating the characters).


If you leave this box empty, the default separators (a blank and the tab character) are used by default.

If you change the pattern matching options, they apply to all new rules in a policy. Click **Apply to all** to apply them to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.

You can set case sensitivity and separator characters for individual rules in a policy by clicking the  button in the **Condition** tab of a rule.

3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* If the list of policies does not refresh automatically in the BSM Integration Adapter user interface, click  in the toolbar.

## Pattern matching

To make your policies as flexible as possible, you can use pattern-matching syntax. The pattern-matching syntax makes it possible to write rule conditions that match strings very specifically.

### Pattern-matching details

BSM Integration Adapter provides a powerful pattern-matching language that reduces the number of conditions you must use. Selected, dynamic parts of text-based events can be extracted, assigned to variables, and used as parameters to build the event description or to set other attributes.

The pattern-matching language enables you to very accurately specify the character string that you want a rule to match.

#### Matching special characters

Ordinary characters are expressions which represent themselves. Any character of the supported character set may be used. However, if any of the following special characters are used they must be prefaced with a backslash (\) that masks their usual function.

`\ [ ] < > | ^ $`

If ^ and \$ are not used as anchoring characters, that is, not as first or last characters, they are considered ordinary characters and do not need to be masked.

#### Matching characters at the beginning or end of a line

If the caret (^) is used as the first character of the pattern, only expressions discovered at the beginning of lines are matched. For example, "^ab" matches the string "ab" in the line "abcde", but not in the line "xabcde".

If the dollar sign is used as the last character of a pattern, only expressions at the end of lines are matched. For example, "de\$" matches "de" in the line "abcde", but not in the line "abcdex".

#### Matching multiple characters

Patterns used to match strings consisting of an arbitrary number of characters require one or more of the following expressions:

- <\*> matches any string of zero or more arbitrary characters (including separators)
- <n\*> matches a string of *n* arbitrary characters (including separators)
- <#> matches a sequence of one or more digits
- <n#> matches a number composed of *n* digits
- <\_> matches a sequence of one or more field separators
- <n\_> matches a string of *n* separators
- <@> matches any string that contains no separator characters, in other words, a sequence of one or more non-separators; this can be used for matching words
- </> matches one or more line breaks
- <n/> matches exactly *n* line breaks

Separator characters are configurable for each pattern. By default, separators are the space and the tab characters.

Matching two or more different expressions

Two expressions separated by the special character vertical bar (|) matches a string that is matched by either expression. For example, the pattern:

```
[ab|c]d
```

matches the string "abd" and the string "cd".

Matching text that does not contain an expression

The NOT **operator** (!) must be used with delimiting square brackets, for example:

```
<![WARNING]>
```

The pattern above matches all text which does not contain the string "WARNING".

The **NOT operator** may also be used with complex subpatterns:

```
SU <*> + <@.tty> <![root|[user[1|2]]].from>-<*.ot>
```

The above pattern makes it possible to generate a "switch user" event for anyone who is not user1, user2 or root. Therefore the following would be matched:

```
SU 03/25 08:14 + ttyp2 user11-root
```

However, this line would not be matched, because it contains an entry concerning "user2":

```
SU 03/25 08:14 + ttyp2 user2-root
```

Notice that if the subpattern including the **not operator** does not find a match, the **not operator** behaves like a <\*>: it matches zero or more arbitrary characters. For this reason, the pattern-matching expression: <![1|2|3]> matches any character or any number of characters, except 1, 2, or 3.

Mask (\) Operator

The backslash (\) is used to mask the special meaning of the characters:

```
[ ] < > | ^ $
```

A special character preceded by \ results in an expression that matches the special character itself.

Notice that because ^ and \$ only have special meaning when placed at the beginning and end of a pattern respectively, you do not need to mask them when they are used within the pattern (in other words, not at beginning or end).

The only exception to this rule is the tab character, which is specified by entering "\t" into the pattern string.

Bracket ([ and ]) Expressions

The brackets ([ and ]) are used as delimiters to group expressions. To increase performance, brackets should be avoided wherever they are unnecessary. In the pattern:

```
ab[cd[ef]gh]
```

all brackets are unnecessary--"abcdefgh" is equivalent.

Bracketed expressions are used frequently with the **OR operator**, the **NOT operator** and when using **subpatterns** to assign strings to variables.

Numeric range operators

BSM Integration Adapter provides six numeric range operators that can be used in pattern matching. The operators are used in this way:

Operator name	Syntax	Example/Explanation
Less than	<code>&lt;[<i>pattern</i>] -lt n</code> This is a match <i>pattern</i> you provide that returns the number to be compared] -lt n This is the value against which you want to test the number returned by the match pattern>	<code>&lt;[&lt;#&gt;] -lt 5&gt;</code> matches every number less than 5
Less than or equal to	<code>&lt;[<i>pattern</i>] -le n &gt;</code>	<code>&lt;[&lt;#&gt;] -le 5&gt;</code> matches 5 and every number less than 5
Greater than	<code>&lt;[<i>pattern</i>] -gt n &gt;</code>	<code>&lt;[&lt;#&gt;] -gt 5&gt;</code> matches every number greater than 5
Greater than or equal to	<code>&lt;[<i>pattern</i>] -ge n &gt;</code>	<code>&lt;[&lt;#&gt;] -ge 5&gt;</code> matches 5 and every number greater than 5
Equal to	<code>&lt;[<i>pattern</i>] -eq n &gt;</code>	<code>&lt;[&lt;#&gt;] -eq 5&gt;</code> matches 5 or 5.0
Not equal to	<code>&lt;[<i>pattern</i>] -ne n &gt;</code>	<code>&lt;[&lt;#&gt;] -ne 5&gt;</code> matches every number but 5 and 5.0
The operators can also be combined to produce matches according to ranges of numbers:		
Matches numbers that belong to the interval, excluding the limits	<code>&lt; n -lt [<i>pattern</i>] -lt n &gt;</code>	<code>&lt;5 -lt [&lt;#&gt;] -lt 10&gt;</code> matches every number between 5 and 10 ( but not 5 or 10)



Matches numbers that belong to the interval, including the limits	<code>&lt; n -le [pattern] -le n &gt;</code>	<code>&lt;5 -le [&lt;#&gt;] -le 10&gt;</code> matches every number between 5 and 10 (including 5 and 10)
Matches numbers that do not belong to the interval, excluding the limits	<code>&lt; n -gt [pattern] -gt n &gt;</code>	<code>&lt;10 -gt [&lt;#&gt;] -gt 5&gt;</code> matches every number between 5 and 10 ( but not 5 or 10)
Matches numbers that do not belong to the interval, including the limits	<code>&lt; n -ge [pattern] -ge n &gt;</code>	<code>&lt;10 -ge [&lt;#&gt;] -ge 5&gt;</code> matches every number between 5 and 10 (including 5 and 10)

## User-defined variables in patterns

Any matched string can be assigned to a variable, which can be used to compose events. To define a parameter, add ". parametername " before the closing bracket. The pattern:

```
^errno: <#.number> - <*.error_text>
```

matches an event such as:

```
errno: 125 - device does not exist
```

and assigns "125" to **number** and "device does not exist" to **error\_text**.

When using these variables, the syntax is `<variable_name>` (for example, `<number>`).

## Rules by which BSM Integration Adapter assigns strings to variables

In matching the pattern `<*.var1><*.var2>` against the string "abcdef", it is not immediately clear which substring of the input string will be assigned to each variable. For example, it is possible to assign an empty string to **var1** and the whole input string to **var2**, as well as assigning "a" to **var1** and "bcdef" to **var2**, and so forth.

The pattern matching algorithm always scans both the input line and the pattern definition (including alternative expressions) from left to right. <\*> expressions are assigned as few characters as possible. <#>, <@>, <S> expressions are assigned as many characters as possible. Therefore, **var1** will be assigned an empty string in the example above.

To match an input string such as:

```
this is error 100: big bug
```

use a pattern such as:

```
error<#.errnumber>:<*.errtext>
```

In which:

- "100" is assigned to **errnumber**
- "big bug" is assigned to **errtext**

For performance and pattern readability purposes, you can specify a delimiting substring between two expressions. In the above example, ":" is used to delimit <#> and <\*>.

Matching <@.word><#.num> against "abc123" assigns "abc12" to **word** and "3" to **num**, as digits are permitted for both <#> and <@>, and the left expression takes as many characters as possible.

Patterns without expression anchoring can match any substring within the input line. Therefore, patterns such as:

```
this is number<#.num>
```

are treated in the same way as:

```
<*>this is number<#.num><*>
```

## Using subpatterns to assign strings to variables

In addition to being able to use a single operator, such as \* or #, to assign a string to a variable, you can also build up a complex subpattern composed of a number of operators, according to the following pattern: <[ *subpattern* ].**var**>

For instance: <[<@>file.tmp].**fname**>

In the example above, the period ( . ) between "file" and "tmp" matches a similar dot character, while the dot between "]" and "**fname**" is necessary syntax. This pattern would match a string such as "Logfile.tmp" and assigns the complete string to **fname**.

Other examples of subpatterns are:

- <[Error|Warning].**sev**>
- <[Error[<#.n><\*.msg>]].**complete**>

In the first example above, any line with either the word "Error" or the word "Warning" is assigned to the variable, **sev**. In the second example, any line containing the word "Error" has the error number assigned to the variable, **n**, and any further text assigned to **msg**. Finally, both number and text are assigned to **complete**.

## Pattern matching for variables

BSM Integration Adapter enables you to test a string or variable against a pattern, and define an output string that is conditional on the result. You can do this using `$MATCH`, which has the following syntax:

```
$MATCH(string, pattern, true, [false])
```

Specify the parameters as follows:

`string`

Specify a literal string (for example, `TEST STRING`) or an BSM Integration Adapter variable (for example `<$LOGPATH>`).

`pattern`

Specify a pattern, using BSM Integration Adapter pattern matching syntax. You can create user-defined variables in the pattern to use in the parameters `true` and `false`. The pattern is case sensitive.

`true`

Specify a string to return if the string and pattern match. You can specify a literal string, or a user-defined variable, or an BSM Integration Adapter variable.

`false`

*Optional.* Specify a string to return if the string and pattern do not match. You can specify a literal string, or a user-defined variable, or an BSM Integration Adapter variable.

Separate each parameter with a comma (.). To specify a comma within a parameter, you must precede it with two backslashes (`\`).

You can use `$MATCH` within your policies in the following event attributes:

- Service ID
- Message type
- Message group
- Application
- Object
- Message text
- Automatic command
- Custom message attribute

**Note:** You can use `$MATCH` only once in each message attribute. You cannot use `$MATCH` recursively.

### Example

An XML logfile entry policy can monitor a number of log files. The name of path of the log file is available in the BSM Integration Adapter variable `<$LOGPATH>`. If part of the log file path corresponds to an application name, you can use `$MATCH` to set the application event attribute as follows:

```
$MATCH (<$LOGPATH>, <@.application>.log, <application>, Unknown)
```

## Examples of pattern matching in rule conditions

The following examples show some of the many ways in which the pattern-matching language can be used.

- `Error`  
Recognizes any event containing the keyword `Error` at any place in the event. (It is case sensitive by default.)
- `panic`  
Matches all events containing `panic`, `Panic`, `PANIC` anywhere in the text of the event, when case sensitive mode is switched off.
- `logon|logoff`  
Uses the **OR operator** to recognize any event containing the keyword `logon` or `logoff`.
- `^getty:<*.msg> errno<*><#.errnum>$`  
Recognizes any event such as: `getty: cannot open ttyxx errno : 6` or `getty: can't open ttyop3; errno 16`

In the example `getty: cannot open ttyxx errno : 6`, the string "cannot open ttyxx" is assigned to the variable **msg**. The digit 6 is assigned to the variable **errnum**. Note that the dollar sign (\$) is used as an anchoring symbol to specify that the digit 6 will only be matched if it is at the end of the line.

- `^errno[ |=]<#.errnum> <*.errtext>`  
Matches events such as: `errno 6 - no such device or address` or `errno=12 not enough core`.

Note the space before the **OR operator**. The expression in square brackets matches either this blank space, or the "equals" sign. The space between `<#.errnum>` and `<*.errtext>` is used as a delimiter. Although not strictly required for assignments to the variables shown here, this space serves to increase performance.

- `^hugo:<*>:<*.uid>:`  
Matches any `/etc/passwd` entry for user `hugo` and returns the user ID to variable **uid**. Notice that ":" in the middle of the pattern is used to delimit the string passed to **uid** from the preceding string. The colon ":" at the end of the pattern is used to delimit the string passed to **uid** from the succeeding group ID in the input pattern. Here, the colon is necessary not only as a speed enhancement, but also as a means of logical separation between strings.
- `^Warning:<*.text>on node<@.node>$`  
Matches any event such as: `Warning: too many users on node hpbbx` and assigns `too many users` to **text**, and `hpbbx` to **node**.
- `^<*.line1><1/><*.line2><1/><*.line3><1/><*.line4>$`

Matches four lines of text, for example:

```
Security ID:      S-1-5-21-3358208617-1210941181-189752109-500
Account Name:    Administrator
Account Domain:  EXAMPLE
Logon ID:        0x228a2
```

There is one line break between each line. The pattern assigns each line of text to a variable.

- <<#> -le 45>

This pattern matches all strings containing a number which is less than or equal to 45. For example, the event: *ATTENTION: Error 40 has occurred* would be matched.

Note that the number 45 in the pattern is a true numeric value and not a string. Numbers higher than 45, for instance, "4545" will not be matched even if they contain the combination, "45".

- <15 -lt <2#> -le 87>

This pattern matches any event in which the first two digits of a number are within the range 16-87. For instance, the event: *Error Message 3299* would be matched. The string: *Error Message 9932* would not be matched.

- ^ERROR\_<[<#.err>] -le 57>

This pattern matches any text starting with the string "ERROR\_" immediately followed by a number less than, or equal to, 57.

For example, the event: *ERROR\_34: processing stopped* would be matched and the string 34 would be assigned to the variable, *err*.

- <120 -gt [<#>1] -gt 20>

Matches all numbers between 21 and 119 which have 1 as their last digit. For instance, events containing the following numbers would be matched: 21, 31, 41... 101... 111 and so on.

- Temperature <\*> <@.plant>: <<#> -gt 100> F\$

This pattern matches strings such as: "Actual Temperature in Building A: 128 F". The letter "A" would be assigned to the variable, *plant*.

- Error <<#> -eq 1004>

This pattern matches any event containing the string "Error" followed by a space and the sequence of digits, "1004".

For example, *Warning: Error 1004 has occurred* would be matched by this pattern. However, *Error 10041* would not be matched by this pattern.

- WARNING <<#> -ne 107>

This pattern matches any event containing the string "WARNING" followed by a space and any sequence of one or more digits, except "107". For example, the event: *Application Enterprise (94/12/45 14:03): WARNING 3877* would be matched.

## Synchronizing events

BSM Integration Adapter enables you to monitor event sources, and, if certain conditions apply, to forward the detected events as HP Business Service Management (BSM) events to the Operations Management Event Browser. After Operations Management receives an event, you can keep it up to date on the event source by configuring BSM and BSM Integration Adapter to synchronize event changes back to the source manager that generated the original event. For example, if a BSM Operations Management operator closes an event, a notification can be automatically sent to NNMi.

Event changes that are synchronized back include lifecycle changes (the state is only updated when the state changes to closed).

**Tip:** Synchronized events have additional runtime parameters that can be inserted in URL tools. For more information about URL tools, see the Operations Management online help.

## To configure event synchronization

1. Configure the BSM Integration Adapter server as a connected server in Operations Management.

For more information, see "[Configure the HP BSM Integration Adapter server as a connected server](#)" (on page 119)

2. Configure policies to include the source event ID in the generated event.

For more information, see "[Configure policies for event synchronization](#)" (on page 121)

3. Write a Perl script that receives the event changes from BSM and forwards them to the source manager.

For more information, see "[Write Perl scripts for event synchronization](#)" (on page 122)

## Configure the HP BSM Integration Adapter server as a connected server


The first step to achieve event synchronization is to configure the BSM Integration Adapter server as a target connected server in the Connected Servers manager.

For full details about how to configure a connected server, see the Operations Management online help.

### To configure a target connected server

1. Navigate to the Connected Servers manager in the Operations Management user interface:

**Admin** → **Operations Management** → **Tune Operations Management** → **Connected Servers**

2. Click  to open the Create New Server Connection dialog box.
3. In the **Display Name** field, enter a name for the target connected server. The **Name** field is filled automatically. For example, if you enter `IA Manager Example` as the display name for the target BSM Integration Adapter server, `IA_Manager_Example` is automatically inserted in the Name field.

*Optional.* Enter a description for the new target server.

Select the **Active** checkbox to enable event synchronization. (You may clear the checkbox if you only want configure the BSM Integration Adapter server to launch the BSM Integration Adapter user interface or to launch the user interface of the source manager.)

**Note:** If you clear the **Active** checkbox, BSM deletes information about event changes and is therefore not able to update BSM Integration Adapter when the server is activated again. However, if the BSM Integration Adapter connected server is activated but temporarily unavailable, BSM buffers information about event changes, and tries to resend them when the server is available again.

Click **Next**.

4. Select **Integration Adapter**.

Click **Next**.

5. Enter the **Fully Qualified DNS Name** of the BSM Integration Adapter target server (for example, `ia_mgmt.example.com`).

*Optional.* 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.

Click **Next**.

6. Specify the communication port of the BSM Integration Adapter target server. By default, BSM and BSM Integration Adapter communicate using secure HTTPS at port 21350.
7. Click **Finish**.

The target `IA Manager Example` server appears in the list of Connected Servers.


The next step in configuring event synchronization is to insert the source event ID (that is, the ID under which the event is tracked in the source manager) in the generated events by adding it to the generating policies. See ["Configure policies for event synchronization" \(on page 121\)](#).



## Configure policies for event synchronization

The event that BSM Integration Adapter forwards to BSM Operations Management must include the original ID of the event in the source manager. Otherwise BSM and BSM Integration Adapter do not know which event to update in the source manager.

### To configure policies for event synchronization

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click **SNMP** or **XML**. The policy editor opens.

Alternatively, double-click an existing SNMP or XML interceptor policy to edit it.

2. Set the source event ID attribute in the event attributes tab:

- SNMP interceptor policies: Click **Rules**, then click **Event Attributes**.


**Note:** The source event ID attribute is not available for event defaults in SNMP interceptor policies.

- XML interceptor policies: Click **Event**, then click **Event Attributes**.

Alternatively, click **Rules**, then click **Event Attributes**.

**Tip:** The monitored XML file usually contains the source event ID. If you are working with sample data, you can drag the source event ID from the Sample Data tab and add it to the source event ID field.

3. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.

4. *Optional.* Activate the policy for your changes to take effect.

The next step in configuring event synchronization is to create a Perl script that receives the event changes and forwards them to the corresponding source manager. See ["Write Perl scripts for event synchronization" \(on page 122\)](#).

## Write Perl scripts for event synchronization

The `ombacksync` process on the BSM Integration Adapter server receives the event changes from the BSM data processing server. To forward these changes to the source manager, you must provide a Perl script that closes the event in the source manager.

The Perl script must call the subroutine `OMBackSync`, which supports the following parameters:

- `Operation` (`Init` or `Close`)
- `ID` (`Close` only)

When the `ombacksync` process starts, it processes your Perl script and calls the subroutine `OMBackSync` with the parameter `Init`. When the process receives an event with the status `closed`, `ombacksync` calls the subroutine `OMBackSync` with the parameters `Close` and `ID`.

BSM Integration Adapter provides an example Perl script that writes the time and date as well as the operation and ID to the file `OMBSOutput.txt`:

Windows: "%OvDataDir%\conf\backsync\OMBackSync.pl"

Linux: `/var/opt/OV/conf/backsync/OMBackSync.pl`

**Note:** If the `ombacksync` process encounters syntax errors in the Perl script, it generates an event describing the problem and stops. Correct the syntax and restart the `ombacksync` process.

## To forward event changes to the source manager

1. Write a Perl script that calls the subroutine `OMBackSync` with the parameters `Operation` and `ID`.
2. Name your Perl script `OMBackSync.pl` and place it in the following folder on the BSM Integration Adapter server:

Windows: "%OvDataDir%\conf\backsync\OMBackSync.pl"

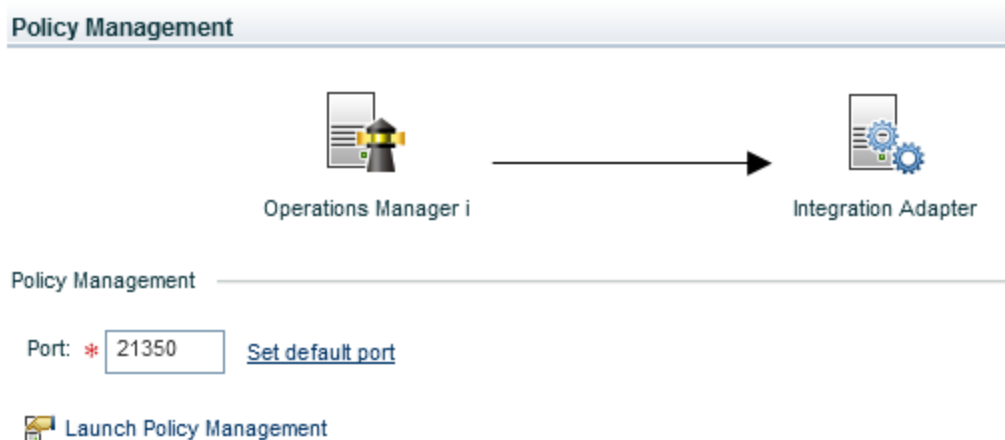
Linux: `/var/opt/OV/conf/backsync/OMBackSync.pl`

3. Restart the `ombacksync` process on the BSM Integration Adapter server:

```
ovc -restart ombacksync
```

## Configuring drilldown

You can integrate BSM Integration Adapter into Operations Management so that administrators can launch the BSM Integration Adapter user interface in the Connected Servers manager or in the context of an event. The following illustration shows the **Launch Policy Management** link in the Connected Servers manager.




For more information, see "[Configure launch of the HP BSM Integration Adapter user interface](#)" (on page 123).

BSM also enables operators to start the user interface of the source manager in the context of an event in the Operations Management Event Browser. For more information, see "[Configure drilldown into source managers](#)" (on page 124).

## Configure launch of the HP BSM Integration Adapter user interface

BSM enables you to start the BSM Integration Adapter user interface directly from within Operations Management. The following integrations are available if you configure your BSM Integration Adapter server as a connected server in Operations Management:

- BSM Operations Management Connected Servers manager

You can start the BSM Integration Adapter user interface by clicking the  icon in the connected server details pane.

- BSM Operations Management Event Browser

You can start the BSM Integration Adapter user interface by right-clicking the event in the Operations Management Event Browser and selecting **Configure** → **Integration Policies**.

After you start the BSM Integration Adapter user interface, depending on the security settings in your environment, you may have to log on. (See "[Log on to HP BSM Integration Adapter](#)" (on page 32).)

For more information about configuring a BSM Integration Adapter server as a connected server in Operations Management, see "[To configure a target connected server](#)" (on page 119).

## Configure drilldown into source managers

BSM enables operators to start the user interface of source managers in the context of an event in the Operations Management Event Browser. To launch the source manager's user interface, right-click the event in the Operations Management Event Browser and select **Show** → **Event in Source Manager**.

You can configure drilldown by adding the source server to the connected server configuration of the BSM Integration Adapter server in Operations Management, or by specifying this information in the policies that forward the source events to Operations Management. If a policy and a connected server configuration both contain information about the source manager, the information in the policy takes precedence.

**Tip:** Set up the source server as a connected server if you want to centrally configure drilldown to the source manager, as opposed to adding this information to individual policies.

Configure the source server as a connected server

For full details about how to configure a connected server, see the Operations Management online help.

1. Configure the BSM Integration Adapter server as a connected server in Operations Management. For more information, see ["To configure a target connected server" \(on page 119\)](#).
2. In the Event Drilldown tab, enter the **Fully Qualified DNS Name** of the computer that hosts the source manager (for example, `SCOM.mgmt2.example.com`).


Specify the communication port on the source manager.

Specify the **Root URL Path** of the event in the source manager. This is the base path of the URL, and does not include FQDN or port. To drill down to a specific event in the source manager, append the variable `${sourcedFrom.externalId}` to the URL. BSM replaces the variable at runtime if the event contains the source event ID. For more information about adding the source event ID to a policy, see ["Configure policies for event synchronization" \(on page 121\)](#).

Specify the communication protocol used by the source manager.

**Note:** You can also configure event drilldown information in policies. If a policy and a connected server configuration both contain event drilldown information, the information in the policy takes precedence.

Configure policies for event drilldown

1. In the BSM Integration Adapter user interface, click  in the toolbar, then click **SNMP** or **XML**. The policy editor opens.

Alternatively, double-click an existing SNMP or XML interceptor policy to edit it.

2. Set the event drilldown attribute in the advanced attributes tab:

- SNMP interceptor policies: Click **Rules**, then click **Advanced**.

**Note:** The event drilldown attribute is not available for event defaults in SNMP interceptor policies.

- XML interceptor policies: Click **Event**, then click **Advanced**.


Alternatively, click **Rules**, then click **Advanced**.


3. In the **Event Drilldown URL** field, type the URL of the event in the source manager. This is the complete path of the URL, and includes the FQDN (Fully Qualified Domain Name) of the computer that hosts the source manager, the communication port, and the root URL path.

Example:

```
http://nnmi.example.com:8004/nnm/launch?cmd=showForm
&objtype=Incident&objuuid=$OPC_CUSTOM[nnm.incident.uuid]
&menus=true
```

**Note:** This event attribute can also be set by BSM based on connected server configuration. If a policy and a connected server configuration both contain event drilldown information, the information in the policy takes precedence.

4. Click  in the toolbar to save the policy and close the editor.

**Note:** Do not leave the editor by closing the web browser window or tab (for example by clicking the Close button in the window's title bar or using a menu option). When you close the browser window or tab, the policy remains locked by you for editing. To close the policy editor without saving, click  in the toolbar.